Mazur's work with the Eisenstein ideal: diophantine and non-diophantine perspectives

Loïc Merel

July 17, 2023

1 "By pure thought"

Mazur and Tate thus qualified their short proof that no elliptic curve over $\mathbf{Q}$ admits a rational point of order 13 [55]. Indeed, one can find in their work the central ideas that led Mazur to prove his torsion theorem in the Eisenstein ideal paper [48] of 1977, and its continuation, the isogeny paper [50], published the following year.

Theorem. (Torsion theorem) *Let E be an elliptic curve over $\mathbf{Q}$. The torsion part of $E(\mathbf{Q})$ is cyclic of order m, with $1 \leq m \leq 10$ or $m = 12$, or a product of a group of order 2 and of a cyclic group of even order ≤ 8.*

In the preface of his *Disquisitiones Arithmeticae*, Gauss proclaimed (or insisted) that diophantine questions do not constitute all of number theory [25]. A similar distinction seems appropriate when one contemplates the content and legacy of Mazur's Eisenstein ideal paper. Accordingly, the recurring and fecund theme of congruences between Eisenstein series and other modular forms will be considered first in the context of the torsion theorem, and then for other arithmetical, non-diophantine purposes.

2 From Levi to Ogg, Mazur and Tate

As Schappacher and Schoof realized around 1994 [74], Mazur's torsion theorem had been formulated as a conjecture in 1908 by Levi [44], in his address to the international congress of mathematicians, and seemingly forgotten in the course of the 20th century. It is difficult to trace exhaustively the history of this question. Levi had already noted that it amounts to prove that certain curves (the notation $X_1(N)$ was an anachronism in 1908) do not have rational points beside the obvious (cuspidal, in the modern jargon) ones. He established that no elliptic curve over $\mathbf{Q}$ admits a rational point of order 14, 16 or 20 [42, 43]. His proof was based on the method of descent, applied to curves of genus no larger than 1, the very technique dating back to Fermat and employed by many continuators of Levi, including, in a crowning achievement, by Mazur. Considering that the question was asked at the ICM, and that significant partial results were obtained, it is difficult to fault Levi for having failed to durably bring his conjecture to the attention of his contemporaries and successors, and therefore to deny him the priority for his prediction. Levi's work preceded Mordell's proof of the finite generation of (what we call nowadays) the Mordell-Weil group, published in 1922 [61].

Billing and Mahler [5] (in 1940), with an ulterior contribution of Nagell [64] (in 1952) proved, still by studying curves of genus 1, that no elliptic curve over $\mathbf{Q}$ possesses a point of order 11, 15 or 24. Levi seems to have been forgotten by 1949, at least by Nagell, who reaffirmed the torsion conjecture [63] without apparent awareness of Levi's work. In [66], Ogg ruled out 17 as a possible torsion prime. He proposed a geometric philosophy: $X_1(N)$ should have non-cuspidal $\mathbf{Q}$-rational points if and only if the genus of $X_1(N)$ is 0 (*i.e.* $N \leq 10$ or $N = 12$) [67]. This was known to be equivalent to the torsion conjecture. Thus the once forgotten torsion conjecture of Levi has sometimes been referred to as Ogg's conjecture.

All this was part of a wider background of results and conjectures of which here is a sample. In 1967, Cassels attributed to the folklore the belief that the order of torsion of an elliptic curve over a number field K is bounded in terms of K only [10]. Shafarevich had asked sometime before 1972 whether the bound in Cassels' folklore conjecture would depend only on the degree of K over $\mathbf{Q}$ [16]. Manin in 1967 proved that, for any prime number p and any number field K, the p-primary torsion of an elliptic curve over K is bounded in terms of p and K only [46]. Both Dem'janenko and Hellegouarch had noted an intriguing connection between hypothetical solutions of Fermat's equation for the prime exponent p and the p-torsion of what would be called later the Frey elliptic curve [28, 17]. Serre had proved his open image theorem in 1972 [75], in particular the following statement. Let E be an elliptic curve over a number field K without complex multiplications over $\bar{K}$. For l prime number, denote by E_l the group of l-division points of E. There exists a number N such that the representation $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E_l)$ is surjective for $l > N$. Serre asked about a uniform version [75]:

[...] peut-on prendre pour N un entier qui ne dépende que de E et pas de K?

3 The work of Mazur and Tate on 13-torsion

Here is the argument that Mazur and Tate employed to show that $X_1(13)$ has no $\mathbf{Q}$-rational points beside its cusps [55]. By "pure thought", the authors meant that, contra their predecessors, they had no use of any model for such a modular curve. They proceeded by embedding the curve $X_1(13)$ in its jacobian $J_1(13)$, and then studying the $\mathbf{Q}$-rational points of $J_1(13)$.

Such an approach had been familiar for a long time. In particular, Chabauty proved that, provided the rank r of Mordell-Weil group of the jacobian J of a curve X over $\mathbf{Q}$ is strictly smaller than the genus g of X, then $X(\mathbf{Q})$ is finite [11]. The condition $r < g$ is *Chabauty's condition*, a fundamental guiding principle to this day. But establishing finiteness differs significantly from providing the full list of rational points. Falting's theorem [21], proved in 1983 and famously ineffective, would have been of no help to Mazur and Tate. In the setting of modular curves, the latter authors and Ogg combined an understanding of the arithmetic of J with some knowledge of the geometry of the map $X \to J$. Their successors would follow variations of this basic plan (see program B below).

The key arithmetic argument is that the group $J_1(13)(\mathbf{Q})$ is cyclic of order 19 and *a fortiori* finite. The proof is summarized with admirable concision in the third paragraph of [55].

> *The possibility that this could be done occurred to us when Ogg passed through our town and mentioned that he had discovered a point of order 19 on the 2-dimensional abelian variety J. It seemed (to us and to Swinnerton-Dyer) that if such an abelian variety J, which has bad reduction at only one prime, and has a sizeable number of endomorphisms, has a point of order 19, it is not entitled to have any other points.*

Descent has been used by several predecessors of Mazur and Tate including Levi, but accomodating the "sizable number of endomorphisms" (*i.e.* the descent a with coefficients in a Hecke algebra) was a key innovation.

Thus the $\mathbf{Q}$-rational points of $X_1(13)$ are to be found among the 19 $\mathbf{Q}$-rational points of $J_1(13)$. It was known that only 6 of those points come from $X_1(13)$, and they all come from the cusps.

From then on, the torsion conjecture could be thought as a diophantine problem devoid of diophantine equations.

4 The Eisenstein ideal and torsion of prime order

We follow throughout Mazur's unusual choice of notation: let N be a prime number. The essential step to prove the torsion conjecture consists in proving that $X_1(N)$ has no rational points, beside its cusps, for $N = 11$ or $N > 13$ (call this *the prime torsion conjecture*). The additional arguments needed to obtain the full torsion conjecture have already been mentioned or reside in two articles of Ligozat [45] and Kubert [38].

But the Mazur–Tate argument can not work for any value of N since $J_1(N)(\mathbf{Q})$ was suspected (and Mazur confirmed this suspicion in [48], Theorem 3) to be infinite except for finitely many values of N. The modification introduced by Mazur consists in identifying a non-zero quotient abelian variety $\tilde{J}$ of $J_1(N)$ such that $\tilde{J}(\mathbf{Q})$ is finite or, more precisely, $\tilde{J}$ is the largest quotient of $J_0(N)$ for which the method of descent can be used to establish the finiteness of $\tilde{J}(\mathbf{Q})$.

For this, Mazur noted that the ring of endomorphisms (over $\mathbf{Q}$) of $J_0(N)$ identifies to the (commutative) Hecke algebra $\mathbf{T}$ (the subring of the endomorphisms of $J_0(N)$ generated by Hecke operators T_l for l prime number $l \neq N$, and by the Atkin-Lehner operator W_N). The *Eisenstein ideal* $\mathcal{I}$ of $\mathbf{T}$ is generated by the operators that would annihilate the single Eisenstein series of weight 2 for $\Gamma_0(N)$. In practice, it is spanned by the operators $T_l - (l + 1)$ for l prime number $l \neq N$, and by $1 + W_N$. Mazur established two basic properties: the quotient ring $\mathbf{T}/\mathcal{I}$ is isomorphic to $\mathbf{Z}/n\mathbf{Z}$, where n is the numerator of $(N - 1)/12$, reflecting the fact that $(N - 1)/24$ is the constant coefficient (essentially a Bernoulli number) of the Eisenstein series of weight 2 for $\Gamma_0(N)$. The second property lies deeper: $\mathcal{I}/\mathcal{I}^2$ is also a cyclic group of order n, but it identifies to the group $(\mathbf{Z}/N\mathbf{Z})^\times/\mu_{12}$ where μ_{12} is the group of 12th roots of unity. The latter identification is obtained by $T_l-(l+1) \mapsto$ class of $l^{(l-1)/2}$.

Denote by $\mathbf{T}_\mathcal{I}$ the $\mathcal{I}$-adic completion of $\mathbf{T}$. Then $\tilde{J}$ is the largest quotient of $J_0(N)$ on which $\mathbf{T}$ acts through $\mathbf{T} \to \mathbf{T}_\mathcal{I}$. Hence, $\tilde{J}$ is called the *Eisenstein quotient* of $J_0(N)$. The abelian variety $\tilde{J}$ is trivial if and only if $n = 1$, *i.e.* N is equal to 2, 3, 5, 7 or 13.

For $\mathcal{M}$ maximal ideal in the support of $\mathcal{I}$, Mazur considers the $\mathcal{M}$-adic completion of $\mathbf{T}$ and defines the $\mathcal{M}$-Eisenstein quotient $\tilde{J}_\mathcal{M}$ of $\tilde{J}$. The descent of Mazur-Tate can be adapted, delicately in terms of flat cohomology, to show the finiteness of $\tilde{J}_\mathcal{M}(\mathbf{Q})$, and deduce the finiteness of $\tilde{J}(\mathbf{Q})$. But Mazur is more precise: $\tilde{J}(\mathbf{Q})$ is cyclic of order n, and even isomorphic to $\mathbf{T}/\mathcal{I}$ as a $\mathbf{T}$-module. The descent provides in addition a proof of the triviality of the odd, $\mathcal{I}$-primary part of the Tate-Shafarevich group of $\tilde{J}$.

This enables to prove two properties of the whole of $J_0(N)$ conjectured by Ogg. First, the torsion part of $J_0(N)(\mathbf{Q})$ identifies to the cuspidal subgroup (and to $\tilde{J}(\mathbf{Q})$). The other property is of a dual nature: the maximal subgroup of $J_0(N)$ of μ-type (Cartier dual of a constant group-scheme) is the Shimura subgroup, defined as the kernel of the morphism $J_0(N) \to J_1(N)$ deduced from $X_1(N) \to X_0(N)$ by Picard functoriality.

The consideration of the finiteness of $\tilde{J}(\mathbf{Q})$ combined with the morphism $\phi : X_1(N) \to J_1(N) \to \tilde{J}$ directly implies the finiteness of $X_1(N)(\mathbf{Q})$ whenever $\tilde{J}$ is non-zero. An additional analysis of the geometry of ϕ is required to obtain the prime torsion conjecture. The reasoning of [48] will not be explained here. Indeed, to obtain this desired conclusion, Mazur provided a simpler and stronger argument in the isogeny paper [50].

5 Rational isogenies

The isogeny theorem, obtained by Mazur in 1978 in [50], is a substantial generalisation of the torsion theorem.

Theorem. (Isogeny theorem) *There exists an elliptic curve over* $\mathbf{Q}$ *with a cyclic isogeny of order* N *if and only if* $N \leq 19$ *or* N *belongs to the following list :* 21, 25, 27, 37, 43, 67, 163*.*

At the time of [50], it was not known whether the following numbers should be allowed: 39, 65, 91, 125, and 169. This issue was clarified by Kenku and Mestre [59, 32] soon afterwards, and might explain the presence of the restrictive qualifier *prime* in the title of [50].

It is unclear to me how precisely this statement had been expected among specialists. The finiteness of the list is not mentioned as a folklore conjecture in [10]. It is asked by Serre (see above) [75], who proposed a bound for non-CM curves. But Serre missed the exceptional prime number $N = 37$, which deserves a mention. Indeed, Mazur and Swinnerton-Dyer have discovered in 1974 that $X_0(37)$, of genus 2, admits a pair of non-CM, non-cuspidal, rational points [54]. Rational points of modular curves are often explained by "geometric reasons" (the relevant modular curve has genus 0, or genus 1, the point correspond to a CM-elliptic curve or a cusp). An ambitious project would seek to explain thus all algebraic points on modular curves, though the notion of geometric reason needs to be clarified. The finding of Mazur and Swinnerton-Dyer for $N = 37$ is the first significant hurdle in such a project. Since then, other notable exotic algebraic points have been discovered, *e.g.* a quadratic point on $X_0(311)$ by Galbraith [23] and a cubic point on $X_1(21)$ by Najman [65].

The proof of the isogeny theorem, and therefore of the torsion theorem, is based on a single result from [48]: the finiteness of $\tilde{J}(\mathbf{Q})$. Presciently, Mazur found useful to spell out in axiomatic form what is needed: when N is equal to 11 or > 13, there exists a non-trivial quotient abelian variety A of $J_0(N)$ such that $A(\mathbf{Q})$ is finite. Such a criterion amends Chabauty's condition: the rank of A is smaller than the dimension of A ($r < d$). It is harmless to suppose A optimal, *i.e.* the morphism $J_0(N) \to A$ has connected kernel. In effect, Mazur just considered $A = \tilde{J}$ (see below for the progress on program B with a different quotient A).

Mazur proceeded as follows. The essential question is to determine for which prime number N there exists an elliptic curve over $\mathbf{Q}$ admitting a $\mathbf{Q}$-rational subgroup C of order N. Let E be such an elliptic curve. Mazur proved that $j(E)$ is an integer away from 2. If not, an odd prime number p would divide the denominator of $j(E)$. Then (E, C) defines a $\mathbf{Q}$-rational point Q on $X_0(N)$. Extend $X_0(N)$ to a model $\mathcal{X}_0(N)$ over $\operatorname{Spec}\mathbf{Z}$, and the point Q to a section $\hat{Q} : \operatorname{Spec}\mathbf{Z} \to \mathcal{X}_0(N)$. Since $j(E)$ is not p-integral, $\hat{Q}$ coincides with a cusp $\hat{Q}_0$ in the fiber at p of $\mathcal{X}_0(N)$. Use $\hat{Q}_0$ as a base point to embed $X_0(N)$ in $J_0(N)$. Consider the morphism ϕ: $X_0(N) \to J_0(N) \to A$. Then $\phi(Q)$ is torsion since $A(\mathbf{Q})$ is finite. Denote by $\mathcal{A}$ the Néron model over $\operatorname{Spec}\mathbf{Z}$ of A. The morphism ϕ extends to the smooth locus $\mathcal{X}$ of $\mathcal{X}_0(N)$ as $\hat{\phi}$: $\mathcal{X} \to \mathcal{A}$. The section $\hat{Q}$ belongs to $\mathcal{X}$. Furthermore, the order of a $\mathbf{Q}$-rational torsion point in an abelian variety is determined in the special fiber at p (provided $p > 2$). Thus one gets that $\hat{\phi}(\hat{Q}) = \hat{\phi}(\hat{Q}_0)$ and $\hat{Q}$ coincides with $\hat{Q}_0$ in the fiber at p of A. Mazur noted that this implies that $\hat{Q} = \hat{Q}_0$ (a contradiction) provided $\hat{\phi}$ is a formal immersion at the cusp $\hat{Q}_0$ in characteristic p. After a delicate reinterpretation in terms of modular forms, this geometric condition turned out to be remarkably simple: $\hat{\phi}$ is a formal immersion at the cusp $\hat{Q}_0$ in characteristic p, at least if $p > 2$, whenever A is non-trivial. Thus either $\tilde{J}$ is trivial (and $N = 2$, 3, 5, 7, or 13) or $j(E)$ is integral away from 2. (A variant of this argument establishes that $N = 2$, 3, 5, 7, 13 or 17 or $j(E)$ is fully integral.)

One feels a kinship between Mazur's formal immersion argument and Chabauty's method, especially Coleman's explicit version via p-adic integration [13]. Indeed, Mazur's argument has been translated into Coleman's language by Baker [3].

Mazur proved the isogeny theorem for elliptic curves with non-integral (away from 2) j-invariant by different means, without any use of $J_0(N)$. But the prime torsion theorem is easy in that case: Hasse's theorem implies that an elliptic curve with a torsion point of order N with potentially good reduction at p satisfies $N < (1+p^{1/2})^2$, which implies $N < 8$ for $p = 3$. To obtain the isogeny theorem, purely local arguments such as those do not suffice to supplement the integrality statement for $j(E)$. But they constrain N so much that either $N = 13$ or $\mathbf{Q}(\sqrt{-N})$ has class number 1 or $N = 37$. The Heegner-Baker-Stark theorem imposes that $N \leq 163$ [2, 77].

The proof of Fermat's Last Theorem, by Wiles and Taylor-Wiles [82, 79], relied crucially on the torsion theorem. Indeed, a hypothetical solution to Fermat's theorem, say $a^N + b^N = c^N$, gives rise to the Frey-Hellegouarch elliptic curve given by $y^2 = x(x - a^N)(x + b^N)$, which in turn produces a newform of weight 2, level 2, modulo N. Such a form is a cusp form, and therefore does not exist, provided the representation of the absolute Galois group on the N-division point on the Frey-Hellegouarch curve is irreducible, *i.e.* the curve does not admit a rational isogeny of degree N. Because of the semi-stability of the curve, the full strength of

Mazur's isogeny theorem is not required, but there is no known substitute to the torsion theorem to rule out the reducibility.

In [50], Mazur asked whether there exist two elliptic curves E, E' over $\mathbf{Q}$, non isogenous over $\mathbf{Q}$, and a prime number $N \geq 7$ such that $E[N]$ and $E'[N]$ are isomorphic as Galois module? It was given a positive answer by Kraus and Oesterlé [37]. The question developped into what is commonly called the Frey-Mazur conjecture: Fix E, does there exist N_E such that the answer negative for $N \geq N_E$? Here is a more ambitious request: Does there exists N_0 such that the answer is always negative for $N \geq N_0$? See [22] for the considerable consequences for variants of Fermat's Last Theorem, and beyond.

6 Program B, Question C and subsequent developments

Question C appeared in [49], and has been formulated again (in a stronger form) at the Durham conference of 1996 [52]. In the latter formulation, the answer is shown by Mazur to be positive if one accepts Lang's conjecture on rational points on varieties of general type.

Question. C *(1996 version) Does there exist universal number T such that for every number field K, the number of elliptic curve E over K, up to isomorphism, which are isogenous over K to more than T elliptic curves, up to isomorphism, is finite?*

The question seems as open in 2023 as it was in 1996. Program B precedes Question C in [49], was repeated verbatim in opening sentence of [48] and resonates with Serre's uniformity question (see above [75]).

Program. B *Given a number field K and a subgroup H of $\mathrm{GL}_2(\hat{\mathbf{Z}}) = \prod_p \mathrm{GL}_2(\mathbf{Z}_p)$ classify all elliptic curves E/K whose associated Galois representations on torsion points maps $\mathrm{Gal}(\bar{K}/K)$ into $H \subset \mathrm{GL}_2(\hat{\mathbf{Z}})$.*

Innumerable works on the torsion points of elliptic curves, and their Galois-theoretic properties have appeared in the 20th and 21st centuries. Most of them have been written after the Eisenstein ideal paper. Many have examined specific modular curves over specific number fields, have involved ingenious ideas and computer calculations. During the week September 18 to September 22 2023, two simultaneous conferences, one in Zagreb, one in Bangalore, will be devoted mostly to this topic, and chiefly to Mazur's program B [49].

The progresses belong to two general directions which were already recognized around 1970: $\mathbf{Q}$-rational points of other modular curves and algebraic points of $X_1(N)$.

For $K = \mathbf{Q}$, a positive answer to Serre's problem amounts to show that three families of modular curves have no non-CM, non-cuspidal $\mathbf{Q}$-rational points when their prime level is large enough. The three families are $X_0(N)$, $X^+_{\mathrm{split}}(N)$ and $X^+_{\mathrm{nonsplit}}(N)$. The curve $X_0(N)$ have been treated by Mazur in [50]. After additional work of Momose [60], Parent [69], and Rebolledo [71], a breakthrough happened in 2008 when Bilu and Parent proved that the curve $X^+_{\mathrm{split}}(N)$ has no non-CM, non cuspidal rational point for N large enough [6] (it was established later for all $N > 13$ with the help of Rebolledo [7]). These authors followed Mazur's method to treat elliptic curves with non integral j-invariant. They introduced two new arguments to study elliptic curves with integral j-invariant. Their first argument was borrowed from transcendental number theory, in particular the successive refinements of the isogeny theorems of Masser–Wüstholz [47]. Those refinement, due to David [15], Pellarin [70], and Gaudron–Rémond [24], provided a lower bound (in term of N) for the logarithm of the j-invariant. The other original argument of Bilu and Parent is an adaptation of Runge's method for integral points on curves. It provides an upper bound (in term of N) for the logarithm of the j-invariant, which contradicts the lower bound obtained by transcendence methods when N is large enough.

Thus, the non-CM, non-cuspidal rational points of $X^+_{\mathrm{split}}(N)$ for all prime numbers N could be determined, except for $N = 13$. This particular level escaped Mazur's approach, as the jacobian of $X^+_{\mathrm{split}}(13)$ does not possess a non-zero quotient with finitely many rational points. The absence of any non-trivial rank 0 quotient is the key aspect of the jacobians of $X^+_{\mathrm{nonsplit}}(N)$ which prevents the study the rational points of $X^+_{\mathrm{nonsplit}}(N)$ by Mazur's method. Indeed, even the amended version of Chabauty's condition fails, as no quotient of the jacobian satisfies $r < d$. Despite this inauspicious situation, the inexistence of non-CM, non-cuspidal rational point on $X^+_{\mathrm{split}}(13)$ and $X^+_{\mathrm{nonsplit}}(13)$ has been established by way of involved and promising techniques, adapted from Kim's generalisation of Chabauty's methods, especially when $r = g$, by Balakrishnan, Dogra, Müller, Tuitman and Vonk [4]. One would hope that history repeats itself, and that the breakthrough at level 13 would be followed by a general result. However, contra Mazur and Tate for $X_1(13)$, [4] relies on handling specific models of those modular curves of genus 3. Further efforts along those general lines [20] so far do not provide yet complete lists of points on $X^+_{\mathrm{nonsplit}}(N)$, which is the main problem left for $K = \mathbf{Q}$.

Suppose now that K is any number field. Cassel's "folklore conjecture", often called the *uniform boundedness conjecture*, amounts to the inexistence of non-cuspidal K-rational point on $X_1(N)$ when N is large enough (depending on K only). The strengthening suggested by Shafarevich, accordingly called the *strong uniform boundedness conjecture*, would make the 'large enough" depend on $d = [K : \mathbf{Q}]$, asserting thus the non-existence of non-cuspidal $\mathbf{Q}$-rational points on the d-th symmetric power $X_1(N)^{(d)}$ of $X_1(N)$ for N large enough.

Kamienny extended Mazur's approach explained above in the following manner. Consider the map ϕ_d: $X_0(N)^{(d)} \to A$ obtained by composing the canonical maps $X_0(N)^{(d)} \to J_0(N)$ and $J_0(N) \to A$. It can be extended to a morphism $\hat{\phi}_d$: $\mathcal{X}^{(d)} \to \mathcal{A}$. Mazur's argument in the isogeny theorem applies without much modification provided $\hat{\phi}_d$ is a formal immersion in some characteristic p, for p prime $p > 2$. Generalizing Mazur's criterion for $d = 1$, Kamienny showed that the latter condition is satisfied when the first d Hecke operators are $\mathbf{F}_p$-linearly independent as endomorphisms of $\tilde{A}$. When $A = \tilde{J}$, this means linear independence in $\mathbf{T}/(p\mathbf{T} + I)$, where I is the kernel of $\mathbf{T} \to \mathbf{T}_{\mathcal{I}}$ [30]. Kamienny proved this to be satisfied when $d = 2$ and $N > 71$ [29] and then, with Mazur, when $2 < d \leq 8$, for N large enough [31]. Abramovich introduced a variant of this argument and showed that, when $d \leq 14$, $X_1(N)^{(d)}$ has non-cuspidal rational points for only finitely many values of N [1]. As for an analogue of the torsion theorem for quadratic fields, Kamienny determined a complete list of the prime numbers that could divide the order of torsion subgroups of elliptic curves over quadratic fields. The list of possible torsion subgroups for quadratic fields could be obtained with the help of Kenku and Momose [33].

All this was still based on $A = \tilde{J}$ and the finiteness of $\tilde{J}(\mathbf{Q})$. One hardly imagines how Mazur could have devised the winding homomorphism in [48] without being aware that the finiteness of $\tilde{J}(\mathbf{Q})$ follows from the Birch and Swinnerton-Dyer conjecture. However, the latter conjecture was *Terra Incognita* in 1977.

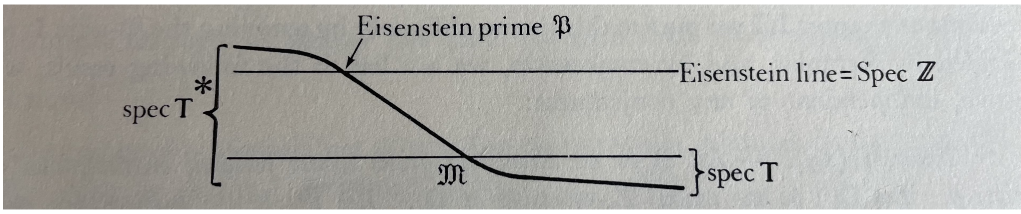
Consider the maximal quotient J_e (the *winding quotient*, following the term introduced by Mazur and Swinnerton-Dyer) of $J_0(N)$ whose L-function does not vanish at 1. By 1994, it followed from the work of Gross–Zagier [26] and Kolyvagin [36] complemented by important non-vanishing results due to Bump–Friedberg–Hoffstein [8] and Murty–Murty [62] that $J_e(\mathbf{Q})$ is finite. In J_e, a more general replacement for the Eisenstein quotient has emerged [57]. The approach of Kamienny–Mazur applies with $\tilde{J}$ replaced by J_e and, *mutatis mutandis*, given any d, the required linear independence has been established for N large enough, proving thus the strong uniform boundedness conjecture [57]. The method has been improved by Oesterlé and Parent [68] and others to progress within program B. *E.g.* Derickx, Etropolski, van Hoeij, Morrow and Zureick-Brown [18] listed completely the possible torsion subgroups of elliptic curves over cubic fields.

Despite occasional ulterior occurrences [39], the Eisenstein quotient ceased thus to be an indispensable tool for further study of diophantine questions.

7 The Eisenstein line and the concept of fusion

Gauss' pronouncement that not all number theory is diophantine finds an echo in the fact that the Eisenstein ideal is, more than ever, an invaluable concept for algebraic number theory. One might see in Ramanujan's famous congruence between Δ and E_{12} modulo 691, which predates by far Mazur's work, an early manifestation of this notion. It is beyond the scope of this account to review all subsequent developments (*e.g.* the proofs of the converse Herbrand theorem by Ribet [73] and of Iwasawa's main conjecture by Mazur and Wiles [56]).

Mazur introduced vividly the Eisenstein quotient by a scheme-theoretic picture [48]:



He seems to be first to have examined $\mathbf{T}$, or rather Spec $\mathbf{T}$, with the eye of a geometer. The geometric view of the Hecke algebra foreshadowed the eigencurve introduced in 1996 by Coleman and Mazur [12]. Already in [48], Mazur found worthwhile to prove that Spec $\mathbf{T}$ is connected, even if it is useless for the torsion theorem.

To accomplish the Eisenstein descent, it was important to establish that the completion of $\mathbf{T}$ at a maximal ideal $\mathcal{M}$ is a Gorenstein ring, whenever $\mathcal{M}$ is either of odd residual characteristic or Eisenstein. (Instances of failure of the Gorenstein property were found by Kilford in characteristic 2 [34], and theoretically justified by Kilford and Wiese [35].) This can be reformulated as a "multiplicity two theorem": the $\mathcal{M}$-adic Tate module of $J_0(N)$ is free of rank 2 over $\mathbf{T}_{\mathcal{M}}$. Subsequently, the Gorenstein property was proved for other Hecke algebras [53], with the purpose of understanding Serre's conjecture. It played an important part to prove many modularity theorems [72, 82, 79, 19]. An addendum by Mazur to the original proof can be found in [80].

Whereas newforms and Galois representations used to be thought with coefficients in (completed) algebraic number fields, or their rings of integers, Mazur brought to the fore the usefulness and the necessity to allow coefficients in Hecke rings, whose subtleties, consequently, need to be studied.

Indeed, further down in the introduction of [48], one finds this prophetic gem:

> *One may think of the "geometric descent" argument [...] as a technique of passing from the knowledge of the arithmetic of the Eisenstein line (i.e. of Eisenstein series, and of $\mathbf{G}_{\mathrm{m}}$) to the knowledge of the arithmetic of irreducible components meeting the Eisenstein line (i.e. of $\tilde{J}$) by a "descent" performed at a common prime ideal. One might hope that for other prime ideal common to distinct irreducible components (primes of* fusion*) one might make analogous passages [...].*

Under all appearances, Mazur had here in mind the question of understanding Selmer groups. However the philosophy of propagation along the connected components of $\operatorname{Spec}\mathbf{T}$ was destined to become a central idea for automorphic forms, in particular for many modularity theorems obtained so far in the Langlands program.

Mazur gave an application of the principle of propagation in a subsequent work: If a newform f corresponds to a irreducible line that meets the Eisenstein line, the L-value of f at 1 is in agreement with the Birch and Swinnerton-Dyer formula (and various twisted formulas) for this modular form at this Eisenstein prime [51]. This line of inquiry was pursued further by Stevens [78].

In a similar vein, Cremona and Mazur have shown that fusion between two cusp forms (especially of inequal Mordell-Weil ranks) produces certain elements in Tate-Shafarevich groups, that they call *visible* [14]. If one of the modular forms is attached to an elliptic curve E over $\mathbf{Q}$, an examination of a large set of examples indicates that the Tate-Shafarevich group of E is surprisingly often made of visible elements.

The Eisenstein ideal theory makes a crucial appearance in the conjectures of Harris and Venkatesh concerning modular forms of weight 1 [27]. Let f be a new form of weight 1 for $\Gamma_1(M)$, for M integer prime to N. Harris and Venkatesh consider the modular form $F_N(z) = \operatorname{Tr}_{\Gamma_0(N)}^{\Gamma_1(M)\cap\Gamma_0(N)}(f(z)f(Nz))$, which is a cusp form of weight 2 for $\Gamma_0(N)$. The monodromy of the Shimura covering $X_1(N) \to X_0(N)$ applied to F_N produces an element of $(\mathbf{Z}/N\mathbf{Z})^\times/\mu_{12}$ (which identifies to the Galois group of the maximal unramified covering intermediate to the Shimura covering). This element is a pseudo-eigenvalue of what Venkatesh calls the derived Hecke operator at N applied to f, as one of the first interesting special cases of his general theory. In concrete terms, Harris and Venkatesh project F_N on the Eisenstein eigenspace and the pseudo-eigenvalue turns out to be the coefficient of proportionality of F_N with the Eisenstein series.

8 The dual quest to understand the Eisenstein completion of T

Despite all of Mazur's efforts, the Eisenstein ideal still holds intrinsic mysteries. The ring $\mathbf{T}_{\mathcal{I}}$ is isomorphic to $\prod_{p|n}\mathbf{T}_{\mathcal{P}}$, where $\mathcal{P} = p\mathbf{T} + \mathcal{I}$ is the maximal ideal of residual characteristic p in the support of the Eisenstein ideal. For p Eisenstein prime number, Mazur asked about the value r_p of the rank of $\mathbf{T}_{\mathcal{P}}$ over $\mathbf{Z}_p$, [48], page 140, (see also *What is this element u ?* page 103). The investigation of this problem has followed two distinct lines of inquiry, which led to answers of a different nature that can fruitfully be compared. This situation recalls the classical dualism between the "algebraic" and "analytic" sides for the special values of L-functions.

Assume that p is not one of the unruly primes 2 and 3. Whenever r_p has small value can be expressed in terms of values modulo N of certain analogues of the zeta function and its derivatives (hence "analytic"). In concrete terms, r_p is > 1 if and only if $\prod_{k=1}^{(N-1)/2} k^k$ is a p-th power modulo N or, alternately, in terms of supersingular elliptic curves, if and only if the discriminant of the Hasse polynomial in characteristic N is a p-th power) [58, 40].

Lecouturier introduced a higher Eisenstein theory to further study r_p and gave various elementary criterias for $r_p > 2$ [40]. The most interesting development on the "analytic side" involved Sharifi's conjectures, and their variants. The latter conjectures relate p-adic modular symbols to the second K-group of the cyclotomic ring $\mathbf{Z}[\mu_N, 1/Np]$ [76]. Lecouturier and Wang deduced an isomorphism (explicitly expressed in terms of Steinberg symbols) between $\mathcal{I}^2/\mathcal{I}^3 \otimes \mathbf{Z}_p$ and $JK_2(\mathbf{Z}[\mu_N, 1/Np]/J^2K_2(\mathbf{Z}[\mu_N, 1/Np]) \otimes \mathbf{Z}_p$, where J is the augmentation ideal of $\mathbf{Z}[\mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q})]$, which acts on $K_2(\mathbf{Z}[\mu_N, 1/Np])$ [41]. They derived conditional criterias for $r_p > 3$. It seems that Sharifi and Venkatesh have gone a long way to prove Sharifi's conjecture. But no criterion for $r_p > 4$ has been given on the analytic side so far.

On the "algebraic side", Calegari and Emerton adopted a different perspective [9]. They defined and studied a ring from the theory of deformation of (two-dimensional, reducible) Galois representations without invoking modular forms. By way of an $R = T$ theorem, they proved that the ring they have introduced is isomorphic to $\mathbf{T}_{\mathcal{I}}$. They recovered directly the properties established by Mazur: structure of $\mathbf{T}/\mathcal{I}$, of $\mathcal{I}/\mathcal{I}^2$. To illustrate the relevance to algebraic number theory, Calegari and Emerton have shown that $r_p > 1$ if the p-rank of the class group of $\mathbf{Q}(N^{1/p})$ is > 1, which, in turn, could be compared to the analytic criterion above. Wake and Wang-Ericksson, with a different approach of deformation theory, and a different $R = T$ theorem, proceeded further, and expressed r_p purely in terms of Galois cohomology using Massey products [81]. About the analogy between relating the dual approaches of r_p to a conjecture about L-values, they asked:

> *[Wake and Wang-Ericksson's theorem relates r_p] to an "algebraic side" (vanishing of Massey products). It is natural to ask whether there is a corresponding object on the analytic side – is there a zeta element $\tilde{\zeta}$ such that* $\operatorname{ord}(\tilde{\zeta}) = r_p$*?.*

References

[1] Dan Abramovich. Formal finiteness and the torsion conjecture on elliptic curves. A footnote to a paper: “Rational torsion of prime order in elliptic curves over number fields” [Astérisque No. 228 (1995), 3, 81–100; MR1330929 (96c:11058)] by S. Kamienny and B. Mazur. Number 228, pages 3, 5–17. 1995. Columbia University Number Theory Seminar (New York, 1992).

[2] A. Baker. Imaginary quadratic fields with class number 2. *Ann. of Math. (2)*, 94:139–152, 1971.

[3] Matthew H. Baker. Kamienny’s criterion and the method of Coleman and Chabauty. *Proc. Amer. Math. Soc.*, 127(10):2851–2856, 1999.

[4] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[5] G. Billing and K. Mahler. On exceptional points on cubic curves. *J. London Math. Soc.*, 15:32–43, 1940.

[6] Yuri Bilu and Pierre Parent. Serre’s uniformity problem in the split Cartan case. *Ann. of Math. (2)*, 173(1):569–584, 2011.

[7] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.

[8] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein. Nonvanishing theorems for L-functions of modular forms and their derivatives. *Invent. Math.*, 102(3):543–618, 1990.

[9] Frank Calegari and Matthew Emerton. On the ramification of Hecke algebras at Eisenstein primes. *Invent. Math.*, 160(1):97–144, 2005.

[10] J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.

[11] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l’unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

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

[13] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[14] John E. Cremona and Barry Mazur. Visualizing elements in the Shafarevich-Tate group. *Experiment. Math.*, 9(1):13–28, 2000.

[15] Sinnou David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, (62):iv+143, 1995.

[16] V. A. Dem’ janenko. The uniform boundedness of the torsion of elliptic curves over algebraic number fields. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:484–496, 1972.

[17] V. A. Dem’janenko. The torsion points of elliptic curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 34:757–774, 1970.

[18] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown. Sporadic cubic torsion. *Algebra Number Theory*, 15(7):1837–1864, 2021.

[19] Fred Diamond. The Taylor-Wiles construction and multiplicity one. *Invent. Math.*, 128(2):379–391, 1997.

[20] Netan Dogra and Samuel Le Fourn. Quadratic Chabauty for modular curves and modular forms of rank one. *Math. Ann.*, 380(1-2):393–448, 2021.

[21] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[22] Gerhard Frey. Links between solutions of $A - B = C$ and elliptic curves. In *Number theory (Ulm, 1987)*, volume 1380 of *Lecture Notes in Math.*, pages 31–62. Springer, New York, 1989.

[23] Steven D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311–318, 1999.

[24] Éric Gaudron and Gaël Rémond. Théorème des périodes et degrés minimaux d'isogénies. *Comment. Math. Helv.*, 89(2):343–403, 2014.

[25] D. Carolo Friderico Gauss. *Disquisitiones Arithmeticae.* 1801.

[26] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[27] Michael Harris and Akshay Venkatesh. Derived Hecke algebra for weight one forms. *Exp. Math.*, 28(3):342–361, 2019.

[28] Y. Hellegouarch. Étude des points d'ordre fini des variétés abéliennes de dimension un définies sur un anneau principal. *J. Reine Angew. Math.*, 244:20–36, 1970.

[29] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[30] S. Kamienny. Torsion points on elliptic curves over fields of higher degree. *Internat. Math. Res. Notices*, (6):129–133, 1992.

[31] S. Kamienny and B. Mazur. Rational torsion of prime order in elliptic curves over number fields. Number 228, pages 3, 81–100. 1995. With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992).

[32] M. A. Kenku. On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$. *J. London Math. Soc. (2)*, 23(3):415–427, 1981.

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

[34] L. J. P. Kilford. Some non-Gorenstein Hecke algebras attached to spaces of modular forms. *J. Number Theory*, 97(1):157–164, 2002.

[35] L. J. P. Kilford and Gabor Wiese. On the failure of the Gorenstein property for Hecke algebras of prime weight. *Experiment. Math.*, 17(1):37–52, 2008.

[36] V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[37] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[38] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[39] Samuel Le Fourn and Pedro Lemos. Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan. *Algebra Number Theory*, 15(3):747–771, 2021.

[40] Emmanuel Lecouturier. Higher Eisenstein elements, higher Eichler formulas and rank of Hecke algebras. *Invent. Math.*, 223(2):485–595, 2021.

[41] Emmanuel Lecouturier and Jun Wang. On a conjecture of Sharifi and Mazur's Eisenstein ideal. *Int. Math. Res. Not. IMRN*, (1):391–421, 2022.

[42] B. Levi. Saggio per una teoria aritmetica delle forme cubiche ternarie. *Atti della Reale Acc. Sci. di Torino*, 42:739–754, 1906.

[43] B. Levi. Saggio per una teoria aritmetica delle forme cubiche ternarie. *Atti della Reale Acc. Sci. di Torino*, 43:99–120, 413–434, 672–681, 1908.

[44] B. Levi. Sull'equazione indeterminata del 3o ordine. Number 2, pages 175–177. 1909.

[45] Gérard Ligozat. *Courbes modulaires de genre* 1. Bull. Soc. Math. France Mém., No. 43. Société Mathématique de France, Paris, 1975. Supplément au Bull. Soc. Math. France, Tome 103, no. 3.

[46] Ju. I. Manin. The p-torsion of elliptic curves is uniformly bounded. *Izv. Akad. Nauk SSSR Ser. Mat.*, 33:459–465, 1969.

[47] D. W. Masser and G. Wüstholz. Estimating isogenies on elliptic curves. *Invent. Math.*, 100(1):1–24, 1990.

[48] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. With an appendix by Mazur and M. Rapoport.

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

[50] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[51] B. Mazur. On the arithmetic of special values of L functions. *Invent. Math.*, 55(3):207–240, 1979.

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

[53] B. Mazur and K. A. Ribet. Two-dimensional representations in the arithmetic of modular curves. Number 196-197, pages 6, 215–255 (1992). 1991. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

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

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

[56] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[57] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[58] Loïc Merel. L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. *J. Reine Angew. Math.*, 477:71–115, 1996.

[59] Jean-François Mestre. Points rationnels de la courbe modulaire $X_0(169)$. *Ann. Inst. Fourier (Grenoble)*, 30(2):v, 17–27, 1980.

[60] Fumiyuki Momose. Rational points on the modular curves $X_{\text{split}}(p)$. *Compositio Math.*, 52(1):115–137, 1984.

[61] L.J. Mordell. "on the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, 21:179–192, 1922.

[62] M. Ram Murty and V. Kumar Murty. Mean values of derivatives of modular L-series. *Ann. of Math. (2)*, 133(3):447–475, 1991.

[63] Trygve Nagell. Problems in the theory of exceptional points on plane cubics of genus one. In *Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949*, pages 71–76. Johan Grundt Tanums Forlag, Oslo, 1952.

[64] Trygve Nagell. Recherches sur l'arithmétique des cubiques planes du premier genre dans un domaine de rationalité quelconque. *Nova Acta Soc. Sci. Upsaliensis (4)*, 15(6):66, 1952.

[65] Filip Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. *Math. Res. Lett.*, 23(1):245–272, 2016.

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

[67] A. P. Ogg. Diophantine equations and modular forms. *Bull. Amer. Math. Soc.*, 81:14–27, 1975.

[68] Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.

[69] Pierre J. R. Parent. Towards the triviality of $X_0^+(p^r)(\mathbf{Q})$ for $r > 1$. *Compos. Math.*, 141(3):561–572, 2005.

[70] Federico Pellarin. Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques. *Acta Arith.*, 100(3):203–243, 2001.

[71] Marusia Rebolledo. Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires. *Pacific J. Math.*, 234(1):167–184, 2008.

[72] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[73] Kenneth A. Ribet. A modular construction of unramified p-extensions of $Q(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[74] Norbert Schappacher and René Schoof. Beppo Levi and the arithmetic of elliptic curves. *Math. Intelligencer*, 18(1):57–69, 1996.

[75] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[76] Romyar Sharifi. A reciprocity map and the two-variable p-adic L-function. *Ann. of Math. (2)*, 173(1):251–300, 2011.

[77] H. M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[78] Glenn Stevens. *Arithmetic on modular curves*, volume 20 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1982.

[79] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[80] Jacques Tilouine. Hecke algebras and the Gorenstein property. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 327–342. Springer, New York, 1997.

[81] Preston Wake and Carl Wang-Erickson. The rank of Mazur's Eisenstein ideal. *Duke Math. J.*, 169(1):31–115, 2020.

[82] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.