BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 54, Number 4, October 2017, Pages 559–573
http://dx.doi.org/10.1090/bull/1576
Article electronically published on April 13, 2017

TATE'S WORK AND THE SERRE–TATE CORRESPONDENCE

PIERRE COLMEZ

Abstract. The Serre–Tate correspondence contains a lot of Tate's work in a casual form. We present some excerpts that show how some of Tate's best known contributions came into being.

Serre and Tate have been close friends for over 50 years and their correspondence, recently published as volumes 13 and 14 of the series "Documents mathématiques" of the Société mathématique de France ([4], [5]) reads like a diary of arithmetic geometry. It contains, in particular, a lot of Tate's work in a casual form. As Tate wrote to Serre on April 23, 1963, after a stream of cohomological letters:

> Excuse all these letters. I find that writing you is an excellent method of organizing my thoughts.

Some of this work was only published much later, some was never published. We give below some excerpts that show how some of Tate's best known contributions came into being. There are many other topics on which Tate worked that appear in the correspondence and that we will not consider, such as Galois cohomology, class field theory, p-adic Hodge theory, Honda–Tate theory, Serre–Tate theory, elliptic curves with everywhere good reduction, modular forms, Stark's conjectures....

1. The Tate curve

Elliptic curves over $\mathbf{C}$ are usually thought of as $\mathbf{C}$ modulo a lattice Λ. Now, two homothetic lattices give isomorphic elliptic curves, and so one can take the lattice Λ, corresponding to an elliptic curve E, of the form $2\pi i(\mathbf{Z}+\mathbf{Z}\tau)$, with $\operatorname{Im}\tau > 0$. Setting $q = e^{2i\pi\tau}$ and using the exponential map, one obtains an isomorphism $\mathrm{E}(\mathbf{C}) \cong \mathbf{C}^*/q^{\mathbf{Z}}$ of complex Lie groups. If the equation of the elliptic curve is $y^2 = x^3 - g_2x - g_3$, classical formulas express g_2, g_3 as power series in q and $x(w), y(w)$, if $w \in \mathbf{C}^*$, as series in q, w, and w^{-1}. These series have rational coefficients, and Tate had the amazing idea that they could be used to give a description of (special) elliptic curves over a p-adic field analogous to the above description over $\mathbf{C}$. This first shows up, in the correspondence, in a letter by Serre of July 31, 1959.

> Il paraît que vous faites des choses rupinantes avec les courbes elliptiques sur les p-adiques (j non entier), m'a raconté Lang; vous savez faire marcher ce que nos pères appelaient les "fonctions loxodromiques" sur les p-adiques. C'est bien sympathique, et j'aimerais beaucoup avoir des détails, si ça ne vous ennuie pas d'écrire.
>
> Si j'ai bien compris ce que me racontait Lang, votre théorie montre de façon amusante qu'une courbe elliptique à multiplication

Received by the editors March 25, 2017.
2010 *Mathematics Subject Classification.* Primary 01Axx, 10-03.

complexe a un invariant j entier algébrique. En effet, sinon, cet invariant aurait un pôle au moins pour un p. Par votre théorie, il s'ensuivrait que le module ℓ-adique associé ($\ell \neq p$) aurait un sous-module distingué de rang 1 (celui qui est formé des points rationnels sur la clôture non ramifiée du corps p-adique); l'anneau des endomorphismes serait bien obligé d'appliquer ce module dans lui-même, et ceci ayant lieu pour tout ℓ montre que cet anneau est réduit à $\mathbf{Z}$. D'accord?

Tate's answer, August 4, 1959.

I am happy to hear that you found the "fonctions loxodromiques" "bien sympathiques" because I like them, too—so much so that I am writing it up, believe it or not. Of course that goes very slowly, what with my writing neurosis, our new house, new child, etc. but still it goes. I am tout à fait d'accord with your remark that one gets a direct proof that $\mathrm{End}(\mathrm{A}) = \mathbf{Z}$ unless j is integral over the prime domain, and I appreciate the remark very much since it has forced me to start thinking about isogenies between these elliptic curves. Since I hope to have a manuscript to show you when we get to Princeton (first week of September for us) I will be very brief now about the details:

k complete with respect to $|\ |$,
$t \in k$, fixed, $0 < |t| < 1$,
w variable in k^*,

$$x(w) = \sum_{m=-\infty}^{\infty} \frac{t^m w}{(1-t^m w)^2} - 2\sum_{m=1}^{\infty} \frac{t^m}{(1-t^m)^2}$$

$$= \frac{w}{(1-w)^2} + \sum_{m=1}^{\infty} \left(\frac{t^m w}{(1-t^m w)^2} + \frac{t^m w^{-1}}{(1-t^m w^{-1})^2} - 2\frac{t^m}{(1-t^m)^2} \right)$$

$$= \frac{1}{w+w^{-1}-2} + \sum_{n=1}^{\infty} \frac{nt^n}{1-t^n}(w^n + w^{-n} - 2), \text{ this last for } |t| < |w| < |t|^{-1}.$$

$$x(w) = x(tw) = x(w^{-1}).$$

In the classical case ($k = \mathbf{C}$) we check that

$$\wp(u) = x(e^u) + \frac{1}{12}$$

by showing that the right hand side has the characterizing properties of $\wp(u; \omega_1, \omega_2)$, where $\omega_1 = 2i\pi$, $\omega_2 = \log t$. Carrying the expression of right hand-side at $u = 0$ out to the term in u^4 you find

$$g_2 = \frac{1}{12} + 20\sum_{n=1}^{\infty} \frac{n^3 t^n}{1-t^n}, \quad g_3 = -\frac{1}{216} + \frac{7}{3}\sum_{n=1}^{\infty} \frac{n^5 t^n}{1-t^n}$$

also you find by differentiation

$$\wp'(u) = x(w) + 2y(w),$$

where $w = e^u$ and where

$$y(w) = \sum_{m=-\infty}^{\infty} \frac{(t^m w)^2}{(1-t^m w)^3} + \sum_{m=1}^{\infty} \frac{t^m}{(1-t^m)^2},$$

$$y(w) = y(tw) \quad \text{and} \quad y(w^{-1}) + y(w) = -x(w).$$

Substituting $\wp = x + \frac{1}{12}$ and $\wp' = x + 2y$ in $\wp'^2 = \wp^3 - g_2\wp - g_3$, we find

$$(\star) \qquad y^2 + xy = x^3 - b_2 x - b_3,$$

where

$$(\star\star) \qquad \begin{cases} b_2 = \frac{1}{4}\big(g_2 - \frac{1}{12}\big) = 5\sum_{n=1}^{\infty} \frac{n^3 t^n}{1-t^n} = 5t + 45t^2 + 140t^3 + \cdots, \\ b_3 = \frac{1}{4}\big(g_3 + \frac{g_2}{12} - \frac{1}{432}\big) = \sum_{n=1}^{\infty} \big(\frac{7n^5 + 5n^3}{12}\big) \frac{t^n}{1-t^n} = t + 23t^2 + 154t^3 + \cdots \end{cases}$$

are power series in t with rational integral coefficients.

Let A be the cubic curve $(\star)$ defined over k, where k is now arbitrary complete, no longer $\mathbf{C}$, and of any characteristic, using $(\star\star)$ as *definition* of coefficients. (Thus A is determined by one transcendental "module", t.) The discriminant of $(\star)$ is

$$\Delta = g_2^3 - 27g_3^2 = b_3 + b_2^2 + 72b_2b_3 - 432b_3^2 + 64b_2^3$$

$$= t - 24t^2 + 252t^3 + \cdots = t\prod(1-t^n)^{24}$$

and is not 0. Hence A is elliptic, with invariant

$$j = \frac{(12g_2)^3}{\Delta} = \frac{1}{t}(1 + 744t + 196884t^2 + \cdots)$$

just as in the classical case. But notice that in the non-archimedean case, the inverse series

$$t = \frac{1}{j} - 744\frac{1}{j^2} + \cdots$$

converges, so that t is *uniquely* determined by j—there is no modular group in that case. On the other hand of course, $|t| < 1 \implies |j| > 1$, i.e. j is not integral.

Let A_k denote the group of points on A with coordinates in k, and let $\langle t \rangle$ denote the subgroup of k^* generated by t.

Theorem. *The map $w \mapsto \varphi(w) = (x(w), y(w))$ is a homomorphism of k^* onto A_k with kernel $\langle t \rangle$.*

I leave the proof as an exercise, without hints, in the hope that you will find a better one than mine, which when written out in all detail, including some lemmas about power series in non-archimedean complete fields, takes 8 handwritten pages.

[. . .]

Finally, and most important, this last theorem and probably many other things that are hard to prove at present, would become

> obvious if one really had a theory of analytic + meromorphic functions in complete non-archimedean fields. Given such a field k, and given such a t with $0 < |t| < 1$, then it is clear from the above results that the "meromorphic" functions on the "manifold" $k^*/\langle t\rangle$ are just the rational functions of $x(w)$ and $y(w)$. But will you please define "meromorphic" and "manifold". How does one get around the total disconnectedness to get some kind of *global* theory? One really must try to make sense out of Krasner's stuff. I have not yet had the courage, however. But everything points to the existence of $\mathfrak{p}$-adic analytic continuation. D'accord? When it is understood, we can write a big addition to your Variétés rédaction.[1]

The content of this letter has had a deep influence on the field despite the fact that Tate did not publish it until 1995. Note that Grothendieck was not very receptive at first, as is shown by his letter to Serre of August 18, 1959 [3].

> Tate m'a écrit de son côté sur ses histoires de courbes elliptiques, et pour me demander si j'avais des idées sur une définition globale des variétés analytiques sur des corps valués complets. Je dois avouer que je n'ai pas du tout compris pourquoi ses résultats suggèreraient l'existence d'une telle définition, et suis encore sceptique. Je n'ai pas non plus l'impression d'avoir rien compris à son théorème, qui ne fait qu'exhiber par des formules brutales un certain isomorphisme de groupes analytiques ; on conçoit que d'autres formules tout aussi explicites en donneraient un autre pas plus mauvais (sauf preuve du contraire !).

2. Rigid analytic spaces

There is no trace in the correspondence of Tate thinking about the questions he raised in the last paragraph of the above letter before September 6, 1961. It could be that Grothendieck's presence at Harvard made him come back to the problem.

> A propos $\mathfrak{p}$-adic analysis, and θ-functions, I just began to think that one had better do some naive theory of divisors for specific "varieties" like affine n-space, the product of n multiplicative groups, the unit polycylinder $|x_i| \leqslant 1$, etc. For example, one should prove that in the corresponding rings (everywhere convergent Taylor series, "everywhere" convergent Laurent series, "Séries restreintes", etc.) two elements have a g.c.d. In other words, these rings should be factorial, except that in the first two cases, the factorization can be infinite, with some restrictions to be made precise, because of "non-compacity" of the varieties. Anyhow, I'm almost certain that in the case of Laurent series, the classical theory goes through and that the θ-functions (for a given "period lattice") just correspond to "periodic" divisors. Do you have any words of wisdom about the above underlined specific Conjecture? All I can get out of G is that the rings must have nilpotent elements, and certain morphisms must be explained to be covering morphisms, in order that one can think more clearly.

[1]Serre was writing the "fascicule de résultats sur les variétés" for Bourbaki.

After that, things went quite fast as Serre wrote, on October 2, 1961:

> Que deviens-tu? Lang m'a dit que tu[2] savais (presque?) définir les "vraies" variétés analytiques p-adiques. Est-ce vrai? Si oui, envoie des détails.

Tate, October 16, 1961:

> I enclose five pages, in "canonical style" which constitute the first installment of the "details" concerning rigid p-adic analytic spaces (with nilpotent elements, of course) which you asked for. I have had the very devil of a time organizing the sorites concerning the category $\mathscr{C}^*$, and the full subcategory $\mathscr{A}$ of algebras of the type $K\{t_1, \ldots, t_r\}$ which will be the "affine" algebras of the theory, to my satisfaction. For example, it took me over a week to extend results which I had in the case of a discrete valuation to the general case. Each time I started to write you an account (twice), I tore it up and started over. But now you have a beginning, and I'm pretty sure that the next installments will be easier to write (and more interesting!). Of course you and Borel will incorporate all this in the fascicule on varieties (heh, heh!). It will be clear without saying that I have been helped enormously by Grothendieck, and by § 7 of Ch 0 of the Elements. Actually, what I send is just the very beginning, but Theorems 4.4 and 4.5 are certainly of interest. Do you see any simpler way to show $K\{T_1, \ldots, T_r\}$ is noetherian? This is almost trivial if the valuation is discrete, for then $V\{T_1, \ldots, T_r\}$ is noetherian because the corresponding graded ring is. Do you see any way for example to prove that $A\{X\}$ is noetherian if A is? I have no idea whether that statement is true. I still do not yet see how to prove $K\{T_1, \ldots, T_r\}$ is factorial when V is non-noetherian, whereas if V is noetherian, the result is about trivial as Grothendieck told me : Because then $V\{T_1, \ldots, T_r\}$ is regular, and when divided by x (prime element of V) it is a polynomial ring, and a projective of rank 1 is free there, so also over $V\{T_1, \ldots, T_r\}$, so that is factorial, so also is $K\{T_1, \ldots, T_r\} = (V\{T_1, \ldots, T_r\})_x$. Just so you have some idea of what is to follow, I give a few remarks. Of course the fact that for $A \in \mathscr{A}$ the maximal ideals are "points" (thm 4.5) is the key to practically everything. What I *think* I can do (though I have not written the details), is prove that for any finite covering of the maximal ideal spectrum of A by open sets of the special form $U = \{y \mid |f_i(y)| \leqslant 1, |g_j(y)| \geqslant 1\}$, where f_i and g_j are finite families of elements of A, gives rise to the trivial Čech cohomology for any sheaf of the form $\widetilde{M}$, where M is a finite type A-module. With this result I hope to be able to patch together rigid analytic spaces. It is certainly enough to get the ones I know about (toruses, elliptic curves, etc).

[2]Note that the casual "tu" replaced the formal "vous": one reason is that Tate had participated in his first "congrès" Bourbaki.

This time Grothendieck was much more enthusiastic. Here is what he writes to Serre, on the first of October of 1961.

> L'atmosphère mathématique à Harvard est tout à fait rupinante, un vrai souffle d'air frais en comparaison de Paris, chaque année plus morne. Il y a ici bon nombre d'étudiants intelligents, qui commencent à être familiers avec le langage des schémas et ne demandent qu'à travailler sur des problèmes intéressants, qui évidemment ne manquent pas. Je vends même des faisceaux de Weil et cohomologie de Weil (si peu que j'en sache) avec la plus grande facilité, y compris à Tate qui vient de démarrer sérieusement les structures analytiques "globales" qui le tracassaient depuis deux années, et qui semblent s'exprimer le plus aisément en termes "d'espaces annelés de Weil". Il me semble de plus en plus évident à ce propos qu'il faudra reprendre complètement le concept de schéma formel en même temps que celui d'espace analytique (ou "rigide-analytique" comme Tate et moi disons pour ses structures "globales"), pour les mettre dans un chapeau commun, qu'il reste à trouver.

Tate's notes were distributed by IHES under the title "Rigid analytic spaces, Private notes of J. Tate, reproduced with(out) his permission by IHES", and finally published in *Inventiones* (thanks to Serre's insistance) in 1971.

3. The Néron–Tate height pairing

The Néron–Tate height pairing is a fundamental tool for studying rational points on abelian varieties, for example it appears in the precise form of the Birch and Swinnerton-Dyer conjecture. It is a positive quadratic form on the group of $\overline{\mathbf{Q}}$-points of an abelian variety defined over a number field, and Tate, in a letter of October 24, 1962, gives an incredibly simple construction of this quadratic form (thanks to Lemma 1 below, now known as *Tate's trick*).

> Has Néron mentioned to you the quadratic form business? I wrote him a few days ago a proof of his Edinburgh conjectures which is so trivial I can hardly believe it:
>
> **Lemma 1.** *Let* A *be an abelian group and* $h : \mathrm{A} \to \mathbf{R}$ *a real valued function on* A *such that the function*
>
> $$d(\mathrm{P}, \mathrm{Q}) = h(\mathrm{P} + \mathrm{Q}) + h(\mathrm{P} - \mathrm{Q}) - 2h(\mathrm{P}) - 2h(\mathrm{Q})$$
>
> *is bounded on* $\mathrm{A} \times \mathrm{A}$*. Then there exists a unique biadditive symmetric map* $b : \mathrm{A} \times \mathrm{A} \to \mathbf{R}$ *such that* $h(\mathrm{P}) - b(\mathrm{P}, \mathrm{P})$ *is bounded on* A*.*
>
> This is a nice exercise. (When the "bounded's" are replaced by "zero's", then the thing is essentially the well known criterion for a Banach space to be a Hilbert space.)
>
> **Lemma 2.** *Let* A *be an abelian variety, let* p_1 *and* p_2 *denote the two projections of* $\mathrm{A} \times \mathrm{A}$ *onto* A*, and for each invertible sheaf* L *on* A*, put*
>
> $$a(\mathrm{L}) = (p_1 + p_2)^*\mathrm{L} + (p_1 - p_2)^*\mathrm{L} - 2p_1^*\mathrm{L} - 2p_2^*\mathrm{L},$$

an invertible sheaf on $\mathrm{A}\times\mathrm{A}$. *Then if* $\mathrm{L}=\mathrm{M}\otimes\mathrm{M}^{-}$ (*and probably also if we just assume* $\mathrm{L}=\mathrm{L}^{-}$, *where* L^{-} *is the image of* L *under* $\mathrm{P}\rightsquigarrow -\mathrm{P}$) *we have* $a(\mathrm{L})$ *trivial, i.e.* $a(\mathrm{L})\approx\mathscr{O}_{\mathrm{A}\times\mathrm{A}}$.

(Also an exercise.)

Putting the two lemmas together with the "functorial" properties of the logarithmic height h (cf. Néron–Lang) we get:

Theorem. *If* A *is an abelian variety defined over a product formula field* k, *and* L *an invertible sheaf on* A *such that* $\mathrm{L}=\mathrm{L}^{-}$, *then there exists a unique bilinear map* $b_{\mathrm{L}}:\mathrm{A}_{\overline{k}}\times\mathrm{A}_{\overline{k}}\to\mathbf{R}$ *such that* $h_{\mathrm{L}}(\mathrm{P})-b_{\mathrm{L}}(\mathrm{P},\mathrm{P})$ *is bounded on* $\mathrm{A}_{\overline{k}}$.

(Here h_{L} is the logarithm of Northcott's "uniform height" on all algebraic extensions of k, which is determined by L up to a bounded term). Of course Néron's Edinburgh conjecture is a corollary. Also Northcott's theorem that $h_{\mathrm{L}}(\mathrm{P})$ is bounded on the division points is now obvious.

Néron and Tate's pairing is a sum of local terms for all places of the number field of definition, and Tate gave a very concrete description of these local contributions in the case of elliptic curves, in a letter dated June 21, 1968, continued on October 1, 1979, with an algorithmic description (and the code of a program for HP25 that computes these local terms).

4. The Sato–Tate conjecture

The Sato–Tate conjecture is now viewed as an equidistribution statement for Frobenius elements inside some motivic Galois groups (a wild generalization of the theorem of Tchebotarev). This point of view was put forward by Serre in a letter to Borel, dated May 18, 1966. Tate's original[3] point of view was a bit different and appears in a fantastic letter dated August 5, 1963.

I have been in a very optimistic mood recently, with the result that I have some conjectures.

Let $f:\mathrm{X}\longrightarrow\mathrm{Y}$ be a morphism of schemes of finite type over $\mathbf{Z}$. Suppose Y irreducible, and f projective, simple, with $f_*\mathscr{O}_{\mathrm{X}}=\mathscr{O}_{\mathrm{Y}}$. Let $d=\dim\mathrm{X}-\dim\mathrm{Y}$ be the fiber dimension,

$$\zeta_{\mathrm{X}}(s)=\prod_{y\in\mathrm{Skel}\mathrm{Y}}\zeta_{\mathrm{X}_y}(s);\qquad \zeta_{\mathrm{X}_y}(s)=\frac{\mathrm{P}_{y,1}(\mathrm{N}y^{-s})\cdots}{\mathrm{P}_{y,0}(\mathrm{N}y^{-s})\cdots\mathrm{P}_{y,2d}(\mathrm{N}y^{-s})}.$$

Thus

$$\zeta_{\mathrm{X}}(s)=\frac{\Phi_0(s)\Phi_2(s)\cdots\Phi_{2d}(s)}{\Phi_1(s)\cdots\Phi_{2d-1}(s)},$$

with

$$\Phi_i(s)=\prod_y\frac{1}{\mathrm{P}_{y,i}(\mathrm{N}y^{-s})},\quad \Re(s)>\dim\mathrm{Y}+\frac{i}{2}\ \text{(assuming Riemann Hypothesis)}.$$

By Poincaré duality we have $\Phi_{2d-i}(s)=\Phi_i(s-d+i)$.

[3]The interested reader will find in the Serre–Tate correspondence a very interesting series of e-mails, at the beginning of March 2008, concerning the history of the Sato–Tate conjecture.

Conjectures. *Let* X_* *be the general fiber of* f*, a variety over* K=R(Y).

(a) *The order of the zero of* $\Phi_1(s)$ *at* $s = \dim Y$ *is the rank of the group of* K*-rational points on the Picard variety of* X_*/K.

(b_i) *The order of the pole of* $\Phi_{2i}(s)$ *at* $s = (\dim Y + i)$ *is equal to the rank of the image of the group of algebraic* $(d-i)$*-cycles on* X_* *which are rational over* K *in the homology group* $H_{2d-2i}(\overline{X_*})$ *of the geometric general fiber* $\overline{X_*}$ (whatever this all means).

(c_i) $\Phi_{2i+1}(s)$ *is regular and non-zero at* $s = \dim Y + \frac{2i+1}{2}$.

Notice that (b_i) and (c_i) can be expressed in weaker form without assuming analytic continuation, because the location of the pole in question is on the line of convergence of the product (assuming Riemann Hypothesis).

Notice that all conjectures are unchanged if we replace Y by a non empty open subscheme, so they really are conjectures about the variety X_*/K.

Notice that (a) for all varieties over K is equivalent to (a) for abelian varieties over K, K being a given field of finite type over the prime field.

I have especial confidence in (a) and (b_1). The (b_i) for $i > 1$ and (c_i) are a result of pure optimism, no thought whatsoever.

Exercise. Let K be a number field, let E be an elliptic curve over K, and apply (b_1) to $X_* = E \times E$ over K. Show that (b_1) is true (by Deuring) in case E has complex multiplication. Show that if E has non complex multiplication, then Conjecture (b_1) implies something about the distribution of the angle $\theta(\mathfrak{p})$ of the $\alpha_{\mathfrak{p}}$ such that $\zeta_{E_{\mathfrak{p}}}(s) = \frac{(1-\alpha_{\mathfrak{p}} N\mathfrak{p}^{-s})(1-\overline{\alpha_{\mathfrak{p}}} N\mathfrak{p}^{-s})}{(1-N\mathfrak{p}^{-s})(1-N\mathfrak{p}^{1-s})}$, namely that if you assume a distribution function $f(\theta) = \sum_{\nu=0}^{\infty} a_\nu \cos \nu\theta$ for $0 \leqslant \theta \leqslant \pi$, then you should get $\int_0^\pi (1 + 2\cos 2\theta) f(\theta) d\theta = 0$, *i.e.* $a_2 = -a_0$. Thus the simplest possible function $f(\theta)$ which should occur is

$$f(\theta) = a - a\cos 2\theta = 2a \sin^2 \theta.$$

Mumford tells me that Sato has found $f(\theta) = c \sin^2 \theta$ experimentally by machine on one curve with thousands of p—many more p than your computation. Did you ever have your distribution analyzed, and do they all look like $\sin^2 \theta$????

Question. Does one know enough about algebraic cycles of intermediate dimension on $E^r = E \times E \times \cdots \times E/K$ to be able to test the conjectures (b_i) and (c_i) via Deuring for E^r with E with complex multiplication, and to see whether the (b_i) and (c_i) are compatible with, or perhaps predict, the $\sin^2 \theta$ in the other case? (Incidentally I just wrote Mumford asking him the same question.)

The "exercise" is the famous Sato–Tate conjecture. It only recently [2] became a theorem for elliptic curves over **Q** or, more generally, over a totally real field [1], but the general case is still wide open.

Serre was busy with a paper for *Izvestia*, and did not reply immediately, which prompted Tate to write on August 28, 1963:

> I got your "petit mot" of 18 August yesterday, and conclude from it that you did not get my letter of August 5 which I sent to Villa Chantaco, Pyla. Tant pis. But you will not escape so easily—I will now repeat what I previously wrote.

Which he did, with quite a lot of extra details. In particular, Conjecture (b_i) was extended from even i's to all i's.

> **Conjecture** (b_i) (for $0 \leqslant i \leqslant 2d$)**.** *The order of the pole of* $\Phi_i(s)$ *at* $s = \dim \mathrm{Y} + \frac{i}{2}$ *is equal to the rank of the group* $\mathrm{H}^i_{\mathrm{alg}}(\mathrm{X}_*/\mathrm{K})$.
>
> Here I must explain that I don't know what I mean by $\mathrm{H}^i_{\mathrm{alg}}(\mathrm{X}_*/\mathrm{K})$ for *odd* i, i.e. (b_i) is at present meaningless for odd i, but for *even* $i = 2j$, I mean the dimension over $\mathbf{Q}_\ell$ of the subspace of $\mathrm{H}^i_{\mathrm{alg}}(\overline{\mathrm{X}}_*, \mathbf{Q}_\ell)$ which is spanned by the images of the algebraic cycles on X_* of codimension j which are "defined over K" (hopefully this is independent of ℓ; if $\mathrm{K} \subset \mathbf{C}$, then I can be more precise, and use the classical cohomology $\mathrm{H}^i(\mathrm{X}_* \times_{\mathrm{K}} \mathbf{C}, \mathbf{Q})$).

And the "exercise" expanded, with hints for a solution.

> But what excites me even more at present than the Fermat–Weil case, is the case of a product of an abelian curve with itself. I will give the results in form of exercices:
>
> Let E be an abelian curve defined over a number field K. For each $\mathfrak{p}$ (with non degenerate reduction) let
>
> $$\zeta(s, \mathrm{E}_\mathfrak{p}) = \frac{(1 - \alpha_\mathfrak{p} \mathrm{N}\mathfrak{p}^{-s})(1 - \overline{\alpha_\mathfrak{p}} \mathrm{N}\mathfrak{p}^{-s})}{(1 - \mathrm{N}\mathfrak{p}^{-s})(1 - \mathrm{N}\mathfrak{p}^{1-s})} \ , \ \alpha_\mathfrak{p} = \varepsilon_\mathfrak{p} \sqrt{\mathrm{N}\mathfrak{p}} \ , \ \varepsilon_\mathfrak{p} = e^{i\theta(\mathfrak{p})}.$$
>
> Put
>
> $$\mathrm{L}_0(s) = \prod_\mathfrak{p} \frac{1}{1 - \mathrm{N}\mathfrak{p}^{-s}} \ , \text{ and } \mathrm{L}_\nu(s) = \prod_\mathfrak{p} \frac{1}{(1 - \varepsilon_\mathfrak{p}^\nu \mathrm{N}\mathfrak{p}^{-s})(1 - \overline{\varepsilon_\mathfrak{p}}^\nu \mathrm{N}\mathfrak{p}^{-s})} \ , \text{ for } \nu > 0 \ .$$
>
> 1. Show that for $\mathrm{X}_* = \mathrm{E}^m = \mathrm{E} \times \mathrm{E} \times \cdots \times \mathrm{E}$ (m times), we have
>
> $$\Phi_j(s, \mathrm{E}^m/\mathrm{K}) = \prod_{\nu+\mu=j} \frac{1}{(1 - \alpha_\mathfrak{p}^\nu \overline{\alpha_\mathfrak{p}}^\mu \mathrm{N}\mathfrak{p}^{-s})^{\binom{m}{\nu}\binom{m}{\mu}}} = \prod_{0 \leqslant \nu \leqslant \frac{j}{2}} \big(\mathrm{L}_{j-2\nu}(s - \frac{j}{2})\big)^{\binom{m}{\nu}\binom{m}{j-\nu}} \ .$$
>
> 2. Suppose there exist real numbers $c_0 = 1, c_1, c_2, \ldots$ such that for each $\nu \geqslant 0$, $\lim_{s \to 1}\{(s-1)^{c_\nu} \mathrm{L}_\nu(s)\}$ exists * Suppose also that there is a distribution function $\mathrm{F}(t)$ on $[0, \pi]$ such that, for $0 \leqslant a \leqslant b \leqslant \pi$, the set of primes $\mathfrak{p}$ such that $|\theta(\mathfrak{p})| \in [a, b]$ has Dirichlet density $\int_a^b d\mathrm{F}(t)$. Show (at least formally—I haven't studied the analytic subtleties if any) that
>
> $$d\mathrm{F}(t) = \frac{1}{\pi} \sum_{\nu=0}^{\infty} c_\nu \cos \nu t \, dt \ .$$
>
> 3. Let (as usual) τ denote the period ratio of the curve E; $\mathrm{Im}(\tau) > 0$. Show that there exists $x, y \in \mathrm{H}^1(\mathrm{E}_\mathbf{C}, \mathbf{C})$ such that $\mathrm{H}^{1,0}(\mathrm{E}_\mathbf{C}) = \mathbf{C}x$, $\mathrm{H}^{0,1}(\mathrm{E}_\mathbf{C}) = \mathbf{C}y$, and such that $\mathrm{H}^1(\mathrm{E}_\mathbf{C}, \mathbf{Q}) = \mathbf{Q}u + \mathbf{Q}v$, where $u = x + y$ and $v = \overline{\tau}x + \tau y$ (perhaps $v = \tau x + \overline{\tau}y$, I forgot).

Show then that $\mathrm{H}^\bullet(\mathrm{E}^m_{\mathbf{C}}, \mathbf{C}) = \mathbf{C}[x_1, \dots, x_m; y_1, \dots, y_m]$ (exterior algebra on $2m$ letters of degree 1), with $\mathrm{H}^{p,q}(\mathrm{E}^m_{\mathbf{C}})$ being spanned by the $\binom{m}{p}\binom{m}{q}$ monomials $x_{i_1} \cdots x_{i_p} y_{j_1} \cdots y_{j_q}$, and with $\mathrm{H}^\bullet(\mathrm{E}^m_{\mathbf{C}}, \mathbf{Q}) = \mathbf{Q}[u_1, \dots, u_m; v_1, \dots, v_m]$, where $u_i = x_i + y_i$ and $v_i = \tau x_i + \overline{\tau} y_i$.

a) Show that if $\mathrm{E}_{\mathbf{C}}$ has complex multiplication (i.e. $[\mathbf{Q}[\tau] : \mathbf{Q}] = 2$), then $\mathrm{H}^{1,1}(\mathrm{E}^m_{\mathbf{C}}) = \mathrm{H}^2(\mathrm{E}^m_{\mathbf{C}}, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C}$. Conclude from this that the ring $\mathrm{H}^{2\bullet}_{\mathrm{alg}}(\mathrm{E}^m_{\mathbf{C}}/\mathbf{C}) = \mathbf{C}[\mathrm{H}^2_{\mathrm{alg}}(\mathrm{E}^m_{\mathbf{C}})]$ (i.e. all algebraic cycles are homologous to intersections of divisors if you allow rational coefficients), and that $\dim_{\mathbf{Q}} \mathrm{H}^{2\nu}_{\mathrm{alg}} = \binom{m}{\nu}^2$. Show, using Deuring, that conjecture $(\mathrm{b}_{2\nu})$ is true for E^m/K.

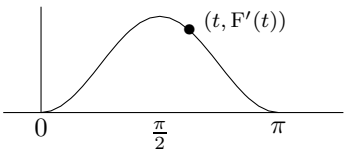
b) (This is the point which really excites me.) Suppose no complex multiplication. Show that $\mathrm{H}^{2\bullet}_{\mathrm{alg}}(\mathrm{E}^m_{\mathbf{C}}) = \mathbf{Q}[u_i v_j + u_j v_i]_{1 \leqslant i,j \leqslant m}$ and hence that $\dim_{\mathbf{Q}} \mathrm{H}^{2\nu}_{\mathrm{alg}} = \binom{m}{\nu}^2 - \binom{m}{\nu-1}\binom{m}{\nu+1}$ in this case. [This took me several days to prove, and at present I need to use $j(\tau)$ algebraic $\Rightarrow$ τ transcendental if no complex multiplication (result of Schneider); however that result is presumably not essential—otherwise one could make a counterexample to Hodge's conjecture.] Anyway, now conclude that for the Fourier coefficients c_ν we get

$$c_0 = 1\ ,\ c_2 = -1\ ,\ \text{and } c_{2\nu} = 0 \text{ for } \nu > 1\ ,$$

if and only if conjecture $(\mathrm{b}_{2\nu})$ holds.

Assuming conjecture $(\mathrm{b}_{2\nu+1})$ holds with $\dim \mathrm{H}^{2\nu+1}_{\mathrm{alg}} \overset{\mathrm{def}}{=} 0$ (this is true for the Fermat–Weil hypersurfaces over number fields and also for E^m where E has complex multiplication), then we conclude that

$d\mathrm{F}(t) = \frac{1}{\pi}(1 - \cos 2t)\, dt = \frac{2}{\pi} \sin^2 t\, dt.$



End of exercise.

5. The Lubin–Tate formal groups

Class field theory gives a description of the Galois group of the maximal abelian extension of number fields or local fields, but does not produce actual elements of these abelian extensions. If the base field is $\mathbf{Q}$, the famous Kronecker–Weber theorem states that all abelian extensions are contained in the field obtained by adjoining all roots of unity. If the base field K is a quadratic imaginary field, then the theory of complex multiplication produces abelian extensions from the torsion points of elliptic curves with complex multiplication by K, but for an arbitrary number field we still do not know how to do that: this was Hilbert's 12-th problem and it is still wide open. For local fields the situation is now completely satisfactory thanks to Lubin and Tate's theory, which gives a beautifully constructive description of abelian extensions of local fields. The first mention of it is a note in the margin at the beginning of a letter dated January 10, 1964,

③ "Complex multiplication" should give all class fields locally

referring to the last paragraph of the letter.

One more thing before I mail this: I think that Lubin's business in his thesis will give *the* "explicit reciprocity law" in local class field theory; it was your remarks on commuting algebras which made me see it:

Let $h = [\mathrm{K} : \mathbf{Q}_p] < \infty$. Let $\mathscr{O}$ be the ring of integers in K, and let $\mathscr{O}_u$ and K_u be the things in the maximal unramified extension. Then, in the paper he submitted to the *Annals*, Lubin has shown the existence of a formal group F over $\mathscr{O}$ such that $\mathrm{End}_{\mathscr{O}}(\mathrm{F}) \xrightarrow{\sim} \mathscr{O}$ and such that its reduction $\widetilde{\mathrm{F}}$ is of height $h = [\mathrm{K} : \mathbf{Q}_p]$. Moreover, F is unique (up to non-unique isomorphism) over $\mathscr{O}_u$, i.e., $\mathrm{F} \times_{\mathscr{O}} \mathscr{O}_u$ is unique, a fact which you will see is perfectly in accord with what I am about to say. Namely, in the usual way we can embed $\mathrm{K} \simeq \mathrm{End}_{\mathscr{O}}(\mathrm{F}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ into $\mathrm{End}_{\mathbf{Q}_p}(\mathrm{T}_p(\mathrm{F})) = (h \times h)$-matrices over $\mathbf{Q}_p$. Now the image of the Galois group G_{K} in $\mathrm{End}_{\mathbf{Q}_p}(\mathrm{T}_p(\mathrm{F}))$ commutes with K *and is therefore in* K, since $[\mathrm{K} : \mathbf{Q}_p] = h$. Thus we get a homomorphism $\mathrm{G}_{\mathrm{K}} \to \mathrm{U}_{\mathrm{K}} =$ units in K. Restricting this to the inertia group $\mathrm{G}_{\mathrm{K}_u}$ we get a homomorphism $\mathrm{G}_{\mathrm{K}_u} \to \mathrm{U}_{\mathrm{K}}$, which is probably canonical by the unicity remarks above, and which it is impossible to doubt is in fact the *reciprocity law isomorphism* (or its negative!). For example, if $\mathrm{K} = \mathbf{Q}_p, h = 1$, then F is the multiplicative group and you get the explicit law for cyclotomic extensions proved by Dwork *locally.* For $h = 2$ this should all fit with the classical theory of complex multiplication. The miracle seems to be that once one abandons algebraic groups and goes to formal groups, the theory of complex multiplication applies *universally* (locally) and indeed the "full" groups on *one*-parameter already just suffice, one for each ground field! I have no idea for a proof at present. I told Lubin to study Dwork's proof for $h = 1$. The thing is the other side of the coin from the question of $\mathfrak{g} \approx \mathfrak{gl}(h, \mathbf{Q}_p)$ when $\mathrm{End}(\mathrm{F}) = \mathbf{Z}_p$.

This was followed, on March 3, 1964, by a letter beginning with:

Lubin and I recently proved the following results, which I would write in French if I were Bott.[4]

Let k be complete with respect to a discrete valuation with finite residue class field with q elements. Let A be the ring of integers in k and let π be a prime element in A. Let $f(\mathrm{X}) = \mathrm{X}^q + \cdots + \pi\mathrm{X}$ be a polynomial of degree q with coefficients in A, highest coefficient 1, such that $f(\mathrm{X}) \equiv \mathrm{X}^q \pmod{\pi}$, $f(0) = 0$, and $f'(0) = \pi$; for example, we might take $f(\mathrm{X}) = \mathrm{X}^q + \pi\mathrm{X}$ simply, (although if $\mathrm{A} = \mathbf{Z}_p, \pi = p$, we might want to take $f(\mathrm{X}) = (1 + \mathrm{X})^p - 1$). For each integer $m \geqslant 1$, let

$$f^{\circ m}(\mathrm{X}) = \mathrm{X}^{q^m} + \cdots + \pi^m\mathrm{X} = f(f(\cdots(f(\mathrm{X}))\cdots)) \quad (m\text{-th iterate of } f).$$

Let W_f be the set of elements $\lambda \in \bar{k}$ such that $f^{\circ m}(\lambda) = 0$ for some m, and let $\mathrm{K}_\pi = k(\mathrm{W}_f)$ be the field generated over k by these elements (it does in fact depend only on the choice of π, not on the choice of f).

[4] A reference to the letter Bott wrote to Serre to announce his famous periodicity theorem.

Theorem. K_π *is the maximal abelian extension of* k *such that* π *is a norm from every finite subfield, and for each unit* u *in* k*, and each* $\lambda \in \mathrm{W}_f$ *we have* $(u, \mathrm{K}_\pi/k)(\lambda) = \underline{u}_f^{-1}(\lambda)$*, where* $\underline{u}_f(\mathrm{X}) \in \mathrm{A}[[\mathrm{X}]]$ *is the unique formal series such that* $\underline{u}_f(\mathrm{X}) \equiv u\mathrm{X} \pmod{\deg 2}$ *and* $\underline{u}_f(f(\mathrm{X})) = f(\underline{u}_f(\mathrm{X}))$.

The existence and uniqueness of such a series (for any $u \in \mathrm{A}$, not only for units) is a trivial exercise; you construct it stepwise, coefficient by coefficient, and observe at each step that the n-th coefficient is in A because, for *any* series $\mathrm{G}(\mathrm{X}) \in \mathrm{A}[[\mathrm{X}]]$ the coefficients of $\mathrm{G}(\mathrm{X}^q) - (\mathrm{G}(\mathrm{X}))^q$ are divisible by $\pi + \pi^r$ (for $r \geqslant 2$).

I am of course deliberately obscuring the issue. The point is that in the same way, you show that there is a unique $\mathrm{F}_f(\mathrm{X}, \mathrm{Y}) \in \mathrm{A}[[\mathrm{X}, \mathrm{Y}]]$ such that $\mathrm{F}_f(\mathrm{X}, \mathrm{Y}) \equiv \mathrm{X} + \mathrm{Y} \pmod{\deg 2}$ and

$$f(\mathrm{F}_f(\mathrm{X}, \mathrm{Y})) = \mathrm{F}_f(f(\mathrm{X}), f(\mathrm{Y})),$$

and you verify (by the unicity statement in the general lemma you are now mentally formulating) that

$$\mathrm{F}_f(\mathrm{F}_f(\mathrm{X}, \mathrm{Y}), \mathrm{Z}) = \mathrm{F}_f(\mathrm{X}, \mathrm{F}_f(\mathrm{Y}, \mathrm{Z}))$$

because both are $\equiv \mathrm{X} + \mathrm{Y} + \mathrm{Z} \pmod{\deg 2}$ and both "commute" with f. Moreover you check that F_f is not only a formal group, but a formal A-module over A, via the series $\underline{u}_f$. Moreover any two, say F_f and F_g (here I mean to imply that $f'(0) = \pi = g'(0)$) are canonically isomorphic over A by means of a series $\mathbf{1}_{fg}(\mathrm{X}) \equiv \mathrm{X} \pmod{\deg 2}$ and $f(\mathbf{1}_{fg}(\mathrm{X})) = \mathbf{1}_{fg}(g(\mathrm{X}))$, whose existence and unicity follows from the same lemma—there was no need to have the same f on both sides! (Also incidentally f can be a series, not a polynomial: What is needed is only $f(0) = 0, f'(0) = \pi$ and $f(\mathrm{X}) \equiv \mathrm{X}^q \pmod{\pi}$.) Now one shows easily that the torsion points over $\bar{k}$ on the formal A-module F_f constitute an A-module isomorphic to k/A. Hence there is an injection $\mathrm{G}(\mathrm{K}_\pi/\mathrm{K}) \hookrightarrow \mathrm{U} =$ units in A. It is a surjection, because the Eisenstein polynomials $f^{\circ m}(\mathrm{X})/f^{\circ(m-1)}(\mathrm{X}) = \mathrm{X}^{q^m - q^{m-1}} + \cdots + \pi$ are irreducible in k. These same polynomials show that π is a universal norm from K_π. Now you can believe that one can check that the isom $\lambda \mapsto \underline{u}_f^{-1}$ is the reciprocity law; one uses the fact that any two of our formal groups F_f and $\mathrm{F}_{f'}$ (for different π and π') are isomorphic over the completion $\hat{\mathrm{B}}$ of the ring of integers in the maximal unramified extension T of k. This follows from Lubin's thesis in case k is of characteristic 0, but we now have a short proof for the existence of a series $\varphi(\mathrm{X}) \in \hat{\mathrm{B}}[[\mathrm{X}]]$ such that it begins with $\varepsilon\mathrm{X}$, ε a unit, and such that:

$$\begin{cases} \varphi^\sigma(\mathrm{X}) = \varphi(\underline{u}_f(\mathrm{X})) \quad (\text{where } u = \pi'/\pi) \text{ (and } \sigma = \text{Frobenius}) \\ \mathrm{F}_f^\varphi = \mathrm{F}_{f'} \text{ and } \underline{a}_f^\varphi = \underline{a}_{f'} \text{ for all } a \in \mathrm{A} \end{cases}$$

Using these identities, you show, first, that $\mathrm{K}_\pi\mathrm{T}$ is independent of π and then that the map $\theta_\pi : k^* \to \mathrm{G}(\mathrm{K}_\pi\mathrm{T}/k)$ which is defined

by

$$\theta_\pi(\pi) = (\text{identity on } \mathrm{K}_\pi, \text{ Frobenius on T})$$
$$\theta_\pi(u) = (\lambda \mapsto \underline{u}_f^{-1}(\lambda) \text{ for } \lambda \in \mathrm{W}_f, \text{ identity on T}) \qquad (u \in \mathrm{U})$$

is independent of π. Since by construction we have

$$\theta_\pi(\pi) = (\pi, \mathrm{K}_\pi\mathrm{T}/k)$$

it now follows that the map $\theta = \theta_\pi$ for all π is the reciprocity law map, because the π's generate k^*. Notice that we have constructed the canonical homomorphism $\theta : k^* \to \mathrm{G}(\mathrm{K}_\pi\mathrm{T}/k)$ without using any class field theory at all; using class field theory we see that $\theta =$ reciprocity law, and hence, since θ is injective, $\mathrm{K}_\pi\mathrm{T}$ is the maximal abelian extension of k. Probably one could prove that directly, too, using ramification theory.

There are still many problems: For example can one give an "explicit" proof of the "translation theorem" relating two ground fields $k \subset k'$. In particular, when k'/k is unramified, we should then be able to pass over to your geometric pro-algebraic theory and look at things up there.

Finally, note that in case of characteristic $p > 0$ one has some pure algebra, which is new, at least to me, namely: Suppose $\mathbf{F}_q \subset k$. Let $\mathrm{A} = \mathbf{F}_q[\mathrm{T}]$ (polynomial ring—A has now no longer anything to do with k). Then for each element $c \neq 0$ in k, the additive group $\mathbf{G}_a$ becomes an A-module via $a \cdot x = ax$ for $a \in \mathbf{F}_q$, and $\mathrm{T} \cdot x = x^q + cx = f(x)$. The torsion submodule (over $\bar{k}$), consisting of the elements λ such that $f^{\circ m}(\lambda) = 0$ for some m, is again an injective hull of the A-module $\mathbf{F}_q = \mathrm{A}/\mathrm{TA}$, and these points are separable over k because $c \neq 0$. Thus they generate an abelian extension whose Galois group is included in the units of $\hat{\mathrm{A}} = \mathbf{F}_q[[\mathrm{T}]]$.

6. Tate's report on elliptic curves

Tate published in *Inventiones*, in 1974, a very nice survey paper on elliptic curves. The correspondence gives a detailed account of the genesis of the paper.

Tate, July 11, 1972.

> Poor me—I am suffering because I agreed to give one of the series of Colloquium Lectures at the Summer Meeting of the AMS, four talks on "The Arithmetic of Elliptic Curves". It's only at the end of August, but they want a manuscript to deliver in advance. Anyway, it's a beautiful subject.

Tate, August 25, 1972.

> Thanks for the letter which I found waiting on return from vacation. The week before leaving on that vacation I spent writing notes to be distributed at my talks on elliptic curves next week. Each day I wrote, and each evening I took the day's production to Laura who typed it immediately. The method produced over-rapid convergence to a most uneven and disorganized 40+ pages.

Serre, some time in the fall of 1972.

> J'ai reçu ce matin ton rapport elliptique. C'est très joli! A l'impression comme dit Lang. A propos, où est-ce que ça va paraître? Est-ce que l'AMS le publie? Sinon il faudrait trouver un journal qui le prenne; ça rendrait service aux gens.

Serre, April 19, 1973.

> Je reviens à la charge au sujet de tes Colloquium lectures "The arithmetic of elliptic curves". Elles seraient très utiles à des tas de gens, il faut vraiment que tu les publies. Je te propose[5] de le faire dans *Inventiones*, ou *Annales ENS*; il y aurait de très petites choses à changer par ci par là: je te propose de préparer moi-même ces changements, et je t'en enverrais la liste pour que tu l'approuves; tu n'aurais donc à t'occuper de rien! J'irais même jusqu'à corriger les épreuves s'il le faut...

Tate, April 24, 1973.

> Thank you for your offer to publish my Dartmouth lectures on elliptic curves, and to do all the work involved. I gratefully accept, partially, as follows. You send me your list of "little changes". Then let me ponder about the whole thing and possibly make a couple of medium changes in it, but with a *deadline*, say July 1 (1973!). If I've done nothing by then, you can go ahead—otherwise I'll send you a revised edition then, or a few days later if I am actively working on it at the time. O.K.? I prefer *Inventiones* to *Annales ENS* (because of the appearance, not because of the speed—I'm not in a hurry).

Tate, July 2, 1973

> Please give me a little more time (i.e. beyond 10 July) on the elliptic curve report. I *have* started on it, but have been distracted by various things, in particular, your conjectures[6] on $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_{\ell^a})$. I think I can prove the conjecture for $\ell = 2$, by brilliantly observing that $2^{\frac{5}{2}} < \pi e^2/4$ (see enclosed sheets, which I offer as payment for the extended deadline).

Tate, July 27, 1973.

> Your solution to the problem of a deadline for my Dartmouth notes is perfect: I hereby authorize you, if you have not received a revised version of them from me before Oct 1, 1973, to proceed with their publication, editing them as you wish. The authorization cannot be vetoed by me... (signed) J. Tate.

[5]Those were the blessed times when the role of journals was still to disseminate ideas, and not to rank papers, and editors were actually encouraging you to submit results they found interesting rather than trying to find a pretext to refuse your papers...

[6]This is an allusion to Serre's conjecture on the modularity of mod p 2-dimensional representations of the absolute Galois group of $\mathbf{Q}$, which he formulated in a letter to Tate, on May 1, 1973, but published only in 1987 (in an extended and more precise form which made it possible to deduce Fermat's last theorem from the Taniyama–Weil conjecture). This conjecture is now a theorem [6], and Tate's result is the starting point for a complicated induction over the set of prime numbers.

Finally, after several extended deadlines, Serre, November 2, 1973.

> Your survey is gone to *Inventiones*. [...]

Serre, April 9, 1974.

> Reçu hier le dernier n° d'*Inventiones*. Ton papier elliptique est dedans, très bien imprimé (y compris la jolie courbe avec N = 37) et je n'ai pas vu de "misprint". Je suis vraiment très content qu'*Inventiones* ait publié ça; on manque de "surveys" : il est très difficile de trouver des gens qui veuillent bien en rédiger.
>
> [...]
>
> J'espère que tu as eu la bonne idée de commander 50 ou 100 tirages à part supplémentaires : tu risques d'en avoir besoin.

Tate, June 21, 1974.

> The reprints of my survey article on elliptic curves just arrived. I'm sending them out now, and am astonished at the number of requests I've got already—you were right.

Indeed! Ten years later, when I started studying elliptic curves, one of the first things I did was to photocopy that survey paper of Tate!

About the author

Pierre Colmez is Director of Research at CNRS, working at Université de Pierre et Marie Curie, Paris. He works in number theory with a special emphasis on p-adic topics. He was director of the series Documents mathématiques of the Société mathématique de France for which he coedited, with J.-P. Serre, the Grothendieck–Serre and the Serre–Tate correspondences.

References

[1] T. Barnet-Lamb, T. Gee, and D. Geraghty, *The Sato–Tate conjecture for Hilbert modular forms*, Jour. Amer. Math. Soc. **24** (2011), 411–469. MR2748398

[2] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, Publ. Res. Inst. Math. Sci. **47** (2011), 29–98. MR2827723

[3] P. Colmez and J.-P. Serre, editors, *Correspondance Grothendieck–Serre* (French). Documents Mathématiques (Paris), 2. Société Mathématique de France, Paris, 2001. MR1942134

[4] P. Colmez and J.-P. Serre, editors, *Correspondance Serre–Tate. Vol. I* (French). Documents Mathématiques (Paris), 13. Société Mathématique de France, Paris, 2015. MR3379329

[5] P. Colmez and J.-P. Serre, editors, *Correspondance Serre–Tate. Vol. II* (French). Documents Mathématiques (Paris), 14. Société Mathématique de France, Paris, 2015. MR3379330

[6] C. Khare and J.-P. Wintenberger, *Jean-Pierre Serre's modularity conjecture*, Invent. Math. **178** (2009), 485-504 and 505–586. MR2551763; MR 2551764

CNRS, IMJ-PRG, Université Pierre et Marie Curie, 4 place Jussieu, 75005 Paris, France

E-mail address: pierre.colmez@imj-prg.fr