AJSE–Mathematics
Volume 1, Number 1, June 2009, Pages 97–106

THE ARITHMETIC OF ELLIPTIC CURVES—AN UPDATE

BENEDICT H. GROSS

Abstract. We survey the progress that has been made on the arithmetic of elliptic curves in the past twenty-five years, with particular attention to the questions highlighted in Tate's 1974 Inventiones paper.

1. Introduction

In 1974, John Tate published "The arithmetic of elliptic curves" in Inventiones. In this paper [9], he surveyed the work that had been done on elliptic curves over finite fields and local fields and sketched the proof of the Mordell-Weil theorem for elliptic curves over $\mathbb{Q}$. He ended with a survey of several conjectures on elliptic curves over number fields, for which a considerable amount of theoretical and experimental evidence had already been accumulated.

Let E be an elliptic curve over a number field k, defined by a non-singular cubic equation in the projective plane over k. The solutions to this equation form an abelian group $E(k)$. This group is finitely generated, by the Mordell-Weil theorem, but it is difficult in practice to determine its rank. The first conjecture was in the direction of making this determination effective.

1) The Tate-Shafarevitch group $Ш(E/k)$, of principal homogeneous spaces for E over k which are trivial at all completions k_v, is finite.

The rest of the conjectures were all related to the L-function $L(E/k, s)$, which is defined by a convergent Euler product in the half-plane $\mathrm{Re}(s) > 3/2$. The product is taken over the non-zero prime ideals P of the ring of integers A of k, and the local term at P is determined by the number of points of E over the finite residue field A/P. The predictions related to the L-function were the following:

2) The local terms in the Euler product determine the elliptic curve E, up to isogeny over k.

3) The function $L(E/k, s)$ has an analytic continuation to the entire s-plane, and satisfies a functional equation relating its value at s to its value at $2 - s$.

4) The order of the analytic function $L(E/k, s)$ at $s = 1$ is equal to the rank of the finitely generated abelian group $E(k)$, and the leading term in its Taylor expansion at $s = 1$ is given by certain local and global arithmetic invariants of the curve E.

Since the publication of Tate's paper, substantial progress has been made on all four problems. Conjecture 2) was completely resolved in 1983 by Gerd Faltings [4], who proved a more general result for abelian varieties. Conjecture 3) was

Received November 26, 2007; Accepted March 15, 2009.
2000 *Mathematics Subject Classification.* 11G05.
Key words and phrases. Elliptic curve, L-function, Mordell-Weil group.

established for all elliptic curves over $\mathbb{Q}$ in 2001 [2], generalizing work done by Andrew Wiles and Richard Taylor in 1995 [11, 12], which settled the semi-stable case. Conjectures 1) and 4) are now known to be true for elliptic curves over $\mathbb{Q}$ whose L-function vanishes to order zero or one at the point $s = 1$ (except for a few loose ends on the leading term). This is a consequence of a limit formula that Don Zagier and I found in 1983 [6] and a cohomological method which Victor Kolyvagin introduced in 1986 [7].

In this paper, I will survey the progress that has been made on these questions. I will also describe the recent results of Richard Taylor on the conjecture of Sato-Tate, as well as some problems which remain open.

2. The L-function

We begin with the definition of the L-function, for an elliptic curve E defined over a number field k. Let A be the ring of integers of k, and let P be a non-zero prime ideal of A. If it is possible to find a model for E:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients a_i in A and discriminant $\Delta = \Delta(a_1, a_2, \ldots, a_6)$ non-zero (mod P), we say E has good reduction (mod P). In this case, let N_P denote the order of the finite group $E(A/P)$, and write

$$N_P = \mathbb{N}P + 1 - a_P,$$

where $\mathbb{N}P$ is the order of the finite field A/P.

It is known that

$$a_P^2 \leq 4.\mathbb{N}P$$

or equivalently, that the discriminant of the quadratic polynomial $x^2 - a_Px + \mathbb{N}P$ is ≤ 0.

If for every model of E over A we have $\Delta \equiv 0$ (mod P), we say E has bad reduction (mod P). In this case, we define $a_P = 1, -1, 0$ depending on the type of bad reduction: nodal with rational tangents, nodal with irrational tangents, or cuspidal.

The L-function is defined by the Euler product

$$L(E/k, s) = \prod_{\text{bad } P} (1 - a_P\mathbb{N}P^{-s})^{-1} \prod_{\text{good } P} (1 - a_P\mathbb{N}P^{-s} + \mathbb{N}P^{1-2s})^{-1}.$$

Expanded out, this gives a Dirichlet series $\sum_{n\geq 1} b_n/n^s$ with integral coefficients b_n, which converges (and is non-zero) in the half-plane Re $(s) > 3/2$. If one includes the Euler factors at the infinite places of k, one gets the complete L-function

$$\Lambda(E/k, s) = (2\pi^{-s}\Gamma(s))^d \cdot L(E/k, s)$$

where $d \geq 1$ is the degree of k over $\mathbb{Q}$. The precise form of conjecture 3) is the statement that:

3*) $\Lambda(E/k, s)$ extends to an analytic function on the entire complex plane, and satisfies the functional equation

$$\Lambda(E/k, s) = \pm N^{1-s} \cdot \Lambda(E/k, 2 - s).$$

Informally, this states that the number of points (mod P) is not an arbitrary function of P. In 3*), N is a positive integer, divisible only by rational primes that ramify in k, or lie below primes of k where E has bad reduction. This was proved for $k = \mathbb{Q}$ in [2]; in this case the integer N is the conductor of E over $\mathbb{Q}$.

3. Modular forms

The key idea in the proof of 3*) for $k = \mathbb{Q}$ is to relate $L(E/\mathbb{Q}, s)$ to the L-function $L(f, s)$ of a holomorphic modular form. This insight goes back to Taniyama, and was developed and refined by Shimura and Weil. The precise formulation is already in Tate's paper: If $L(E/\mathbb{Q}, s) = \sum_{n\geq 1} b_n/n^s$, then the function

$$f(\tau) = \sum_{n\geq 1} b_n e^{2\pi i n\tau}$$

is the Fourier expansion of a modular form of weight 2 for the subgroup $\Gamma_0(N)$ of $SL_2(\mathbb{Z})$, which is a new form and an eigenform for the Hecke algebra. This implies that the Mellin transform of f:

$$\Lambda(E/\mathbb{Q}, s) = \int_0^\infty f(iy) y^s \frac{dy}{y}$$

has an analytic continuation, and satisfies the functional equation $\Lambda(E/\mathbb{Q}, s) = \pm N^{1-s}\Lambda(E/\mathbb{Q}, 2-s)$ with sign equal to the negative of the eigenvalue of the Fricke involution w_N on f [1].

We will sketch the proof that $f(\tau)$ is modular, following Taylor and Wiles, after introducing the ℓ-adic homology groups $T_\ell E$. Their methods have been extended to prove the functional equation of the L-series of some elliptic curves over totally real fields. However, for a general elliptic curve E over an imaginary quadratic field k, the L-function $L(E/k, s)$ is still not known to have an analytic continuation or satisfy a functional equation. The hope is to show that this is equal to the L-function of an automorphic form f on $GL_2(k)$, but the methods of Taylor and Wiles, which use the arithmetic of modular curves and their Hecke algebras, do not generalize to this case.

4. The ℓ-adic homology group

Let E be defined over the number field k, let $\bar{k}$ denote an algebraic closure of k and let $E[n]$ denote the n-torsion subgroup of $E(\bar{k})$. Then $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$ has an action of $\Gamma = \mathrm{Gal}(\bar{k}/k)$, preserving the group structure. Fix a prime ℓ, and define

$$T_\ell E = \varprojlim_{k} E[\ell^m],$$

where the transition map $E[\ell^{m+1}] \to E[\ell^m]$ is multiplication by ℓ. Then $T_\ell E \simeq \mathbb{Z}_\ell^2$ plays the role of the first ℓ-adic homology group of E, and has a $\mathbb{Z}_\ell$-linear action of Γ.

It is known that the Galois action on $T_\ell E$ is unramified at all good primes $P \subset A$ which are not of residual characteristic ℓ. At such a prime, a Frobenius element F_P in Γ, which on the residue field acts by $\alpha \mapsto \alpha^{\mathbb{N}P}$, has characteristic polynomial

$$x^2 - \alpha_P x + \mathbb{N}P \qquad \text{on} \quad T_\ell E.$$

These Frobenius classes are dense in Γ, so the knowledge of the L-function $L(E/k, s)$ as an Euler product determines the characteristic polynomials of all $\gamma \in \Gamma$ on $T_\ell E$. This information turns out to determine the $\mathbb{Z}_\ell[\Gamma]$ module $T_\ell E$, up to isogeny.

A more precise version of conjecture 2) is Tate's isogeny conjecture - that the map of $\mathbb{Z}_\ell$-modules:

$$\mathrm{Hom}_k(E, E') \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_\Gamma(T_\ell E, T_\ell E')$$

is an isomorphism, for any two elliptic curves E and E' over k. This was proved (for abelian varieties) over finite fields by Tate [8], and for abelian varieties over number fields by by Faltings [4]. A key idea introduced in the proof was the notion of the height of an elliptic curve (or a principally polarized abelian variety) with respect to the Hodge line bundle on the moduli space.

5. Modular Galois representations

We can read the Euler product defining the L-function $L(E/\mathbb{Q}, s) = \sum a_n/n^s$ from the ℓ-adic homology $T_\ell E$. Indeed, the local term at the prime p is given by the characteristic polynomial $x^2 - a_p x + p$ of the Frobenius element F_p. Hence, to show $\Lambda(E/\mathbb{Q}, s)$ is the Mellin transform of a modular form, it suffices to show that the Galois representation $T_\ell E$ is modular. By this we mean that there is a modular form f of weight 2 on $\Gamma_0(N)$, which is an eigenform for the Hecke algebra, whose integral eigenvalues a_p for the Hecke operators T_p give the characteristic polynomials of the Frobenius elements F_p on $T_\ell E$ as above, for all primes p not dividing $N\ell$.

The reduction of $T_\ell E$ (mod ℓ) is the Galois representation on $E[\ell]$, which is a vector space of dimension 2 over $\mathbb{Z}/\ell\mathbb{Z}$. We say $E[\ell]$ is modular if there is an eigenform f, with integral eigenvalues a_p, such that the characteristic polynomial of F_p is congruent (mod ℓ) to $x^2 - a_p x + p$.

If $T_\ell E$ is modular, then $E[\ell]$ is clearly modular. Wiles and Taylor established the converse, for primes $\ell \geq 3$, using techniques Mazur had developed for the study of deformations of Galois representations. At the time, little was known about the modularity of the representations $E[\ell]$. But when $\ell = 3$, so $\mathrm{Aut}(E[3]) = GL_2(3)$ is a *solvable* group, the modularity had been established by Langlands, using class field theory and the theory of cyclic base change. From this, Wiles and Taylor were able to conclude that $T_3 E$ was modular and hence prove the analytic continuation and functional equation of $L(E/\mathbb{Q}, s)$.

6. The Mordell-Weil theorem

Let E be an elliptic curve over the number field k. The theorem in the title of this section states that the abelian group $E(k)$ is finitely generated. The proof has two parts. The first is cohomological, and shows that the quotient group $E(k)/mE(k)$ is finite for any $m \geq 1$. In fact, one has an exact sequence

$$0 \to E(k)/mE(k) \to \mathrm{Sel}(E/k, m) \to Ш(E/k)[m] \to 0$$

where $\mathrm{Sel}(E/k, m)$ is a finite subgroup of the Galois cohomology group $H^1(\Gamma, E[m](\bar{k}))$ defined by local conditions. The proof that the Selmer group $\mathrm{Sel}(E/k, m)$ is finite requires all the classical results of number theory: that the class group $Pic(A)$ of the ring of integers A of k is finite and that the unit group A^* is finitely generated.

In the second part of the proof, one uses the positive definite symmetric bilinear form

$$\langle , \rangle \quad E(k) \times E(k) \to \mathbb{R}$$

associated to the canonical height. The canonical height

$$h(P) = \langle P, P \rangle$$

is the unique, real-valued, quadratic function on $E(k)$ such that the difference $h(P) - \log\left(\prod_v \max(|x(P)|_v, 1)\right)$ remains bounded as P runs through $E(k)$. Then $h(P) \geq 0$, with equality if and only if P is a torsion point in $E(k)$. If $\{P_1, ..., P_N\}$ represent the cosets of $mE(k)$ for $m \geq 2$ and $H = \max\{h(P_i)\}$, then $E(k)$ is shown to be generated by the finite number of points P with $h(P) \leq H$.

The non-effectivity of this proof in determining the rank of $E(k)$ is that we have no control over the cokernel of the map $E(k) \to \mathrm{Sel}(E/k, m)$. The conjecture that $\text{Ш}(E/k)$ is finite, so contains no infinitely divisible non-zero elements, is an attempt to rectify this. So far however, all proofs of the finiteness of $\text{Ш}(E/k)$ have depended on knowing the rank in advance.

7. The conjecture of Birch and Swinnerton-Dyer

We return to the study of the L-function of E over k, and give a more precise statement of conjecture 4).

Let $n \geq 0$ be the rank of $E(k)$, and let $\mathbb{Z}P_1 + \mathbb{Z}P_2 + \cdots + \mathbb{Z}P_n$ be a free subgroup of finite index t in $E(k)$. We use the positive definite height pairing $\langle , \rangle$ on $E(k)$ to define the positive real number

$$R(E/k) = \det\ (\langle P_i, P_j \rangle)/t^2.$$

Then $R(E/k)$ is an invariant of $E(k)$, which is independent of the basis, or of the free subgroup chosen.

Let ω be a non-zero invariant differential on $E(k)$. Using the canonical local valuation $||_v$ at each place v of k, and a local decomposition of Haar measure of k, $dx = \otimes dx_v$ on the adeles $\mathbb{A}$ of k giving the quotient group $\mathbb{A}/k$ volume 1, we may define for each place v a measure $|\omega|_v$ on the group $E(k_v)$.

For each infinite place v of k, we define

$$c_v(\omega) = \int_{E(k_v)} |\omega|_v.$$

For each finite place $v = v_P$ of k, we define

$$c_v(\omega) = c_P(\omega) = \int_{E(k_v)} |\omega|_v \cdot L(E/k_v, 1).$$

Here $L(E/k_v, 1)$ is the valve at $s = 1$ of the P-th term in the Euler product for $L(E/k, s)$.

When E has good reduction (mod P), we have

$$L(E/k_v, 1) = (1 - a_P \mathbb{N}P^{-1} + \mathbb{N}P^{-1})^{-1} = \mathbb{N}P/\#E(A/P).$$

If furthermore, we assume that

$$\begin{cases} \int_{A_P} dx_P = 1 \\ \omega \text{ is integral at P and } \omega \not\equiv 0 \pmod{P} \end{cases}$$

then $c_P(\omega) = 1$. Since this is true for almost all primes P, the product $\prod c_v(\omega)$ over all valuations is well-defined. It is independent of the choice of ω, by the product formula.

The refined version of 4) is the conjecture of Birch and Swinnerton-Dyer:

$$\lim_{s\to 1} L(E/k,s)/(s-1)^n = \prod c_v(\omega)\cdot R(E/k)\cdot \#\text{Ш}(E/k).$$

If ω is a global Néron differential, then

$$\prod c_v(\omega) = \prod_{v \text{ infinite}} c_v(\omega)\cdot \prod_{\substack{P \\ \text{with bad reduction}}} (E(k_P):E^0(k_P))\cdot\ |D|^{-1/2},$$

where D is the discriminant of k over $\mathbb{Q}$.

For example, assume that $E(k)$ has rank $n=1$, and let P be a point of infinite order. Let t be the index of the subgroup $\mathbb{Z}P$ in $E(k)$. Then the conjecture of Birch and Swinnerton-Dyer predicts that

$$L(E/k,1)=0$$

$$L'(E/k,1) = \prod c_v(\omega)\cdot\langle P,P\rangle\cdot\#\text{Ш}(E/k)/t^2.$$

8. Heegner points on the curve $X_0(N)$

The combination of the results of Faltings and Taylor-Wiles suggest the following attack on the conjecture of Birch and Swinnerton-Dyer, when $k=\mathbb{Q}$.

Let $f=\sum_{n\geq 1} a_n q^n$ be the eigenform of weight 2 on $\Gamma_0(N)$ associated to the L-function

$$L(E/\mathbb{Q},s)=\sum_{n\geq 1} a_n n^{-s}.$$

Then

$$\omega_f = f(q)\frac{dq}{q} = 2\pi i f(\tau)\, d\tau$$

is a regular differential on the modular curve $X_0(N)$ over $\mathbb{Q}$. Indeed, the non-cuspidal complex points of the curve $X_0(N)$ have the form $H/\Gamma_0(N)$, where H is the upper half-plane, and one can check that the differential ω_f on H is invariant under $\Gamma_0(N)$. Shimura showed that ω_f had only two independent complex periods, so corresponds to an elliptic curve factor E^* of the Jacobian of $X_0(N)$. Moreover, $L(E^*/\mathbb{Q},s)=L(f,s)=L(E/\mathbb{Q},s)$, so by Faltings' isogeny theorem, E^* is isogenous to E over $\mathbb{Q}$.

It follows that there is a dominant morphism of algebraic curves over $\mathbb{Q}$

$$\varphi : X_0(N)\to E$$

taking the cusp $i\infty$ of $X_0(N)$ to the origin of E. If we insist that φ be of minimal degree, it is well-defined up to sign. This suggests using arithmetic information on the curve $X_0(N)$ to study the arithmetic of the curve E — an idea first investigated by Bryan Birch.

A point x on the curve $X_0(N)$ has a modular description — it corresponds to a pair of elliptic curves $(\epsilon \underset{f}{\rightarrow} \epsilon')$ related by an isogeny f whose kernel is cyclic of order N. This allows us to construct, via the theory of complex multiplication, a collection of points — called Heegner points — on $X_0(N)$ over number fields of small degree.

Let k be an imaginary quadratic field where all primes p dividing N are split. Let A be the ring of integers of k and let $n\subset A$ be an ideal with $n\cdot\overline{n}=(N)$, $\gcd(n,\overline{n})=1$. Then the complex elliptic curves $\epsilon=\mathbb{C}/A$ and $\epsilon'=\mathbb{C}/n^{-1}$ are related by an isogeny f with kernel (n^{-1}/A) cyclic of order N. The corresponding point $x = (\epsilon \underset{f}{\rightarrow} \epsilon')$ on $X_0(N)$ is defined over H, the Hilbert class field of k.

Let $P = \mathrm{Tr}_{H/k}(\varphi(x))$ in $E(k)$, where the trace is taken by adding the conjugates of $\varphi(x)$ in $E(H)$. Birch asked the question of when P had infinite order, and conjectured that it was related to the non-vanishing of the first derivative of $L(E/k, s)$ at $s = 1$. Zagier and I answered this in 1983, by proving the following limit formula. Let ω be the invariant differential on E over $\mathbb{Q}$ with $\varphi^*(\omega) = \omega_f$. Then

$$L(E/k, 1) = 0$$

$$L'(E/k, 1) = \int_{E(\mathbb{C})} |\omega| \cdot \ |D|^{-1/2} \cdot \langle P, P\rangle.$$

This implies that P has infinite order if and only if $L'(E/k, 1) \neq 0$.

9. Heegner points and the Selmer group

We continue with the notation of the previous section, and assume that P has infinite order in $E(k)$. Write $\omega_0 = c\omega$, where ω_0 is a Néron differential on E over $\mathbb{Q}$. It is known that c is an integer. For each prime p dividing N, let m_p be the order of $(E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p))$.

If we compare the limit formula with the conjecture of Birch and Swinnerton-Dyer for E over k, we are led to predict that

(1) the group $E(k)$ has rank $n = 1$, so contains the subgroup $\mathbb{Z}P$ with finite index t
(2) the group $\text{Ш}(E/k)$ is finite, of order $(t/c \cdot \Pi m_p)^2$.

Victor Kolyvagin was able to prove 1) and most of 2) in 1986, by studying the relationship between Heegner points and the Selmer groups of E over k.

An example of what Kolyvagin established is the following [5]. Let ℓ be an odd prime where the Galois action on $E[\ell]$ has image $GL_2(\mathbb{Z}/\ell\mathbb{Z})$ and which does *not* divide the point P in the finitely generated group $E(k)$. Then $\mathrm{Sel}(E/k, \ell)$ has dimension 1 over $\mathbb{Z}/\ell\mathbb{Z}$. Since this contains the subgroup $E(k)/\ell E(k)$ where P is nontrivial, this implies that

(1) the rank of $E(k)$ is equal to 1,
(2) the group of ℓ-torsion $\text{Ш}(E/k)[\ell]$ is zero.

Both are consistent with the predictions above, as the hypotheses on ℓ imply that ℓ does not divide t.

These hypotheses hold for almost all primes ℓ, when E does not have complex multiplication. With more work at the remaining primes, Kolyvagin was able to establish the finiteness of $\text{Ш}(E/k)$, under the hypothesis that $L'(E/k, 1) \neq 0$. Combining this with some non-vanishing results, this yields the finiteness of $\text{Ш}(E/\mathbb{Q})$ for all elliptic curves E over $\mathbb{Q}$ whose L-function vanishes to order ≤ 1 at $s = 1$.

10. On the distribution of Frobenius classes

Another question on the L-function where there has been recent progress is the distribution of Frobenius conjugacy classes, as the prime P varies. Assume that E over k has good reduction at P, and recall that the characteristic polynomial of $\mathrm{Frob}(P)$ on the ℓ-adic homology $T_\ell E$ is equal to

$$x^2 - a_P x + \mathbb{N}P.$$

Let $t_P = a_P/(\mathbb{N}P)^{1/2}$ in $\mathbb{R}$. By the inequality $a_P^2 \leq 4\mathbb{N}P$ we have $-2 \leq t_P \leq 2$. In other words, the polynomial

$$x^2 - t_P x + 1$$

is the characteristic polynomial of a conjugacy class $\{\gamma_P\}$ in the compact group SU_2. Richard Taylor [10] has recently proved the Sato-Tate conjecture — that these classes are equidistributed with respect to the push forward of Haar measure under the map $\mathrm{SU}_2 \to \mathrm{SU}_2/\text{conjugacy} = [-2, 2]$, at least when k is totally real and E has a prime of multiplicative reduction.

Another result on distribution was obtained by Noam Elkies [3] in his thesis. Assuming that k has a real completion, the value $a_P = 0$ occurs for infinitely many primes P.

11. Speculations on curves of higher rank

Some of the main questions remaining open concern curves of rank $n \geq 2$. Assume, for simplicity, that the curve E is defined over $\mathbb{Q}$. We still do not know if the rank of the group $E(\mathbb{Q})$ can be arbitrarily large, although examples of all ranks $n \leq 19$ have been found on the computer. Elkies recently found a curve over $\mathbb{Q}$ whose rank is at least 28.

Another open question is the variation of the rank in families of curves with the same j-invariant. If E is defined by the equation

$$y^2 = f(x),$$

and d is a fundamental discriminant, let $E(d)$ be the curve defined by the equation

$$dy^2 = f(x).$$

Then $E(d)$ becomes isomorphic to E over the quadratic extension $k = \mathbb{Q}(\sqrt{d})$, but is not isomorphic to E over $\mathbb{Q}$. In particular, the ranks of $E(d)(\mathbb{Q})$ and $E(\mathbb{Q})$ may differ.

Let $F(x)$ be the number of fundamental discriminants d with $|d| \leq x$, where the rank $n(d)$ of $E(d)(\mathbb{Q})$ is at least 2. Theoretical results of Katz and Sarnak lead one to guess that $F(x)$ grows like a constant times $x^{3/4}(\log x)^a$. Since the number of discriminants d with $|d| \leq x$ grows like a constant times x, this suggests that curves of rank $n \geq 2$ are rare.

References

[1] B. Birch and H. Swinnerton-Dyer, Elliptic curves and modular functions, Modular functions of one variable IV, Springer Lecture Notes in Mathematics, 476, 1975.

[2] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over Q: wild 3-adic exercises, J. Amer. Math. Soc. 14 (2001), 843–939.

[3] N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, Invent. Math. 89 (1987), 561–568.

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

[5] B. Gross, Kolyvagin's work on modular elliptic curves, L-functions and arithmetic, 235–256, London Math. Soc. Lecture Series, 153, 1989.

[6] B. Gross and D. Zagier, Heegner points and derivatives of L-series, Invent. Math. 84 (1986), 225–320.

[7] V. Kolyvagin, Finiteness of E(Q) and Ш(E/Q) for a class of Weil curves, Izv. Akad. Nauk. SSSR 52, 1988.

[8] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966) 134–144.

[9] J. Tate, The arithmetic of elliptic curves, Invent. Math. 23 (1974), 179–206.

[10] R. Taylor, Automorphy for some l-adic lifts of (mod l) representations II, Publ. Math IHES 108 (2008), 183–239.
[11] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, Ann. of Math. 141 (1995), 553–572.
[12] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, Ann. of Math. 141 (1995), 443–551.

Mathematics Department, Harvard University, 1 Oxford St., Cambridge, MA 02138-2901
E-mail address: gross@math.harvard.edu

THE ARITHMETIC OF ELLIPTIC CURVES—AN UPDATE

BENEDICT H. GROSS

الخلاصة (Abstract). نستطلع التقدم الذي حصل في حساب المنحنيات الإهليليجية في السنوات الخمس والعشرين الماضية، مع تركيز خاص على المسائل التي أبرزت في ورقة تيت في مجلة Inventiones عام ١٩٧٤.