BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 43, Number 3, July 2006, Pages 405–414
S 0273-0979(06)01121-9
Article electronically published on May 9, 2006

MR0220680 (36 #3732) 10.32

Baker, A.

Linear forms in the logarithms of algebraic numbers. I, II, III.

Mathematika **13** (1966), 204-216; *ibid.* **14** (1967), 102-107; *ibid.* **14** 1967 220–228.

This is a very interesting sequence of papers. We quote from the introduction: "In 1934 Gel′fond and Schneider proved, independently, that the logarithm of an algebraic number to an algebraic base, other than 0 or 1, is either rational or transcendental and thereby solved the famous seventh problem of Hilbert. Among the many subsequent developments, Gel′fond obtained... a positive lower bound for the absolute value of $\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2$, where β_1, β_2 denote algebraic numbers, not both 0, and α_1, α_2 denote algebraic numbers not 0 or 1, with $\log \alpha_1 / \log \alpha_2$ irrational. Of particular interest is the special case in which β_1, β_2 denote integers. In this case it is easy to obtain a trivial positive lower bound, and the existence of a non-trivial bound follows from the Thue-Siegel-Roth theorem. But Gel′fond's result improves substantially on the former, and, unlike the latter, it is derived by an effective method of proof. Gel′fond [*Transcendental and algebraic numbers* (Russian), GITTL, Moscow, 1952; MR0057921 (15,292e); English translation, p. 177, Dover, New York, 1960; MR0111736 (22 #2598)] remarked that an analogous theorem for linear forms in arbitrarily many logarithms of algebraic numbers would be of great value for the solution of some apparently very difficult problems of number theory. It is the object of this paper to establish such a result."

Define the height of an algebraic number to be the maximum of the absolute values of the relatively prime integer coefficients in its minimal defining polynomial.

The main result of Part I is Theorem 1.1: Let $\alpha_1, \cdots, \alpha_n$ $(n \geq 2)$ denote algebraic numbers, not 0 or 1, such that (for any fixed branch of the logarithm) $\log \alpha_1, \cdots, \log \alpha_n$ and $2\pi i$ are linearly independent over the rationals Q; suppose $k > n + 1$ and let d be any positive integer; then there is an effectively computable number $C = C(n, \alpha_1, \cdots, \alpha_n, k, d) > 0$ such that for all algebraic numbers $\beta_1, \cdots, \beta_n$, not all 0, with degree at most d, we have $(*)$ $|\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n| > Ce^{-(\log H)^k}$, where H denotes the maximum of the heights of $\beta_1, \cdots, \beta_n$. An immediate consequence is Corollary 1.1: If $\alpha_1, \cdots, \alpha_n$ denote non-zero algebraic numbers and $\log \alpha_1, \cdots, \log \alpha_n$, $2\pi i$ are linearly independent over Q, then $\log \alpha_1, \cdots, \log \alpha_n$ are linearly independent over the field A of all algebraic numbers. Starting with Corollary 1.1 for $n = 1$, complete induction gives Corollary 1.2: If $\alpha_1, \cdots, \alpha_n$ denote positive real algebraic numbers other than 1 and $\beta_1, \cdots, \beta_n$ denote real algebraic numbers with $1, \beta_1, \cdots, \beta_n$ linearly independent over Q, then ${\alpha_1}^{\beta_1} \cdots {\alpha_n}^{\beta_n}$ is transcendental. It is remarked that, according to Gel′fond and Linnik, Theorem 1.1 suffices, at least in principle, to settle a conjecture by C. F. Gauss [*Disquisitiones arithmeticae*, § 303, G. Fleischer, Leipzig, 1801; German translation, Springer, Berlin, 1889; reprinting of German translation, pp. 351–352, § 303, Chelsea, New York, 1965; MR0188045 (32 #5488); English translation, Yale Univ. Press, New Haven, Conn., 1966; MR0197380 (33 #5545)] that there are only nine imaginary quadratic fields with class number 1; H. Stark's different approach is mentioned. In order to prove Theorem 1.1, it is first shown that the following modified form of the theorem is sufficient. Theorem 1.1′: Under the hypothesis of Theorem 1.1 there is an effectively computable number C such that for all algebraic numbers $\beta_1, \cdots, \beta_{n-1}$ with degrees at most d, we have $|\beta_1 \log \alpha_1 + \cdots + \beta_{n-1} \log \alpha_{n-1} - \log \alpha_n| \geq e^{-(\log H)^k}$, where H denotes any number not less than C and the height of $\beta_1, \cdots, \beta_{n-1}$. The proof itself then depends on the construction of a function φ of $n-1$ variables; φ is a direct generalization of a function of one variable used in Gel′fond's work (cf. $R(x)$ in C. L. Siegel's *Transcendental numbers* [p. 81, Ann. of Math. Studies No. 16, Princeton Univ. Press, Princeton, N.J., 1949; MR0032684 (11,330c); German translation, Bibliograph. Inst. Mannheim, 1967; MR0209231 (35 #133)]) and has the form $\varphi(z_1, \cdots, z_{n-1}) = \sum_{\lambda_1=0}^{L} \cdots \sum_{\lambda_n=0}^{L} p(\lambda_1, \cdots, \lambda_n) {\alpha_1}^{\gamma_1 z_1} \cdots \alpha_{n-1}^{\gamma_{n-1} z_{n-1}}$ with integer coefficients and $\gamma_r = \lambda_r + \lambda_n \beta_r$ $(1 \leq r < n)$.

In Part II it is shown that the number $2\pi i$ can be omitted in Corollary 1.1; this gives Corollary 2.1: Let $\alpha_1, \cdots, \alpha_n$ denote non-zero algebraic numbers; then $\log \alpha_1, \cdots, \log \alpha_n$ are linearly independent over Q if and only if they are linearly independent over A. Also Corollary 1.2 is sharpened to Corollary 2.2: If $\alpha_1, \cdots, \alpha_n$ denote algebraic numbers other than 0 or 1 and if $\beta_1, \cdots, \beta_n$ denote algebraic numbers with $1, \beta_1, \cdots, \beta_n$ linearly independent over Q, then ${\alpha_1}^{\beta_1} \cdots {\alpha_n}^{\beta_n}$ is transcendental. Both corollaries follow from Theorem 2.2: Let again $\alpha_1, \cdots, \alpha_n$ $(n \geq 2)$ denote non-zero algebraic numbers such that $\log \alpha_1, \cdots, \log \alpha_n$ are linearly independent over Q; suppose $k > 2n+1$ and let d be any positive integer; then there is an effectively computable number $C > 0$ such that for all algebraic numbers $\beta_1, \cdots, \beta_n$, not all 0, with degree at most d, we have $(*)$.

In Part III an inhomogeneous analogue is considered. Theorem 3.1: Let $\alpha_1, \cdots, \alpha_n$, $\beta_0, \beta_1, \cdots, \beta_n$ denote non-zero algebraic numbers; suppose $k > n+1$, and let d $[H]$ denote the maximum of the degrees [heights] of $\beta_0, \cdots, \beta_n$; then $|\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha| > Ce^{-(\log H)^k}$ for some effectively computable number $C = C(n, \alpha_1, \cdots, \alpha_n, k, d) > 0$. The method of proof can be adapted to $\beta_0 = 0$ and yields Theorem 3.2: Let $\alpha_1, \cdots, \alpha_n$, $\beta_1, \cdots, \beta_n$ denote non-zero algebraic numbers; suppose that either $\log \alpha_1, \cdots, \log \alpha_n$ or $\beta_1, \cdots, \beta_n$ are linearly independent over Q; suppose that $k > n$ and let d $[H]$ denote the maximum of the degrees [heights] of $\beta_1, \cdots, \beta_n$; then $(*)$ holds for some effectively computable number $C = C(n, \alpha_1, \cdots, \alpha_n, k, d) > 0$. Theorem 3.1 implies that $e^{\beta_0} {\alpha_1}^{\beta_1} \cdots {\alpha_n}^{\beta_n}$ is transcendental for any non-zero algebraic numbers $\alpha_1, \cdots, \alpha_n$, $\beta_0, \beta_1, \cdots, \beta_n$. Furthermore, $\pi + \log \alpha$ is transcendental for any algebraic number $\alpha \neq 0$ and also $e^{\alpha\pi + \beta}$ is transcendental for all algebraic numbers α, β with $\beta = 0$. It is conjectured that Theorems 3.1 and 3.2 essentially hold with $k = 1$. Further applications to binary forms and to Liouville's theorem of 1844 concerning the approximation of algebraic numbers by rational numbers are announced.

{See also MR0220694 (36 #3746).}
(From MathSciNet, May 2006)

G. J. Rieger

MR0718935 (85g:11026a) 11D41 11G30 14G25

Faltings, G.

Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. (German) [Finiteness theorems for abelian varieties over number fields]

Invent. Math. **73** (1983), *no.* 3, 349–366.

MR0732554 (85g:11026b) 11D41 11G30 14G25

Faltings, G.

Erratum: "Finiteness theorems for abelian varieties over number fields". (German)

Invent. Math. **75** (1984), *no.* 2, 381.

The most spectacular result proved in this paper is Mordell's famous 1922 conjecture: a nonsingular projective curve of genus at least two over a number field has only finitely many points with coordinates in the number field. This result is in fact obtained as a corollary of finiteness theorems concerning abelian varieties which are themselves of at least equal significance. We begin by stating them. Unless indicated otherwise, K will be a number field, Γ the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K, S a finite set of primes of K, and A an abelian variety over K. For a prime number l, T_lA will denote the Tate group of A (inverse limit of the groups of l^n-torsion points on A) and $V_lA = \mathbf{Q}_l \otimes_{\mathbf{Z}_l} T_lA$.

The paper proves the following theorems. Theorem 3: The representation of Γ on V_lA is semisimple. Theorem 4: The canonical map $\mathrm{End}_K(A)\otimes_{\mathbf{Z}}\mathbf{Z}_l \to \mathrm{End}(T_lA)^\Gamma$ is an isomorphism. Theorem 5: For given S and g, there are only finitely many isogeny classes of abelian varieties over K with dimension g and good reduction outside S. Theorem 6: For given S, g, and d, there are only finitely many isomorphism classes of polarized abelian varieties over K with dimension g, degree (of the polarization) d, and good reduction outside S. Both Theorem 3 and Theorem 4 are special cases of conjectures concerning the étale cohomology of any smooth projective variety. The first is sometimes called the Grothendieck-Serre conjecture; the second is the Tate conjecture. Theorem 6 is usually called Shafarevich's conjecture because it is suggested by an analogous conjecture of his for curves (see below).

In proving these theorems, the author makes use of a new notion of the height $h(A)$ of an abelian variety: roughly, $h(A)$ is a measure of the volumes of the manifolds $A(\overline{K}_v)$, v an Archimedean prime of K, relative to a Néron differential on A. The paper proves Theorem 1: For given g and h, there exist only finitely many principally polarized abelian varieties over K with dimension g, height $\leq h$, and semistable reduction everywhere. Theorem 2: Let $A(\overline{K})(l)$ be the l-primary component of $A(\overline{K})$, some prime number l, and let G be an l-divisible subgroup of $A(\overline{K})(l)$ stable under Γ. Let G_n denote the set of elements of G killed by l^n. Then, for n sufficiently large, $h(A/G_n)$ is independent of n. Theorem $(*)$: Let A be an abelian variety over K with semistable reduction everywhere; then there is an N such that for every isogeny $A \to B$ of degree prime to N, $h(A) = h(B)$.

The proof of Theorem 4 is modelled on a proof of J. T. Tate for the case of a finite field K [same journal **2** (1966), 134–144; MR0206004 (34 #5829)]. There, Tate makes use of a (trivial) analogue of Theorem 6 for a finite field to show that a special element of $\mathrm{End}(T_lA)^\Gamma$ lies in the image of the map. At the same point in the proof, the author applies his Theorems 1 and 2. An argument of Yu. G. Zarkhin [Izv. Akad. Nauk SSSR Ser. Mat. **39** (1975), no. 2, 272–277; MR0371897 (51 #8114)] allows one to pass from the special elements to a general element. Theorem 3 is proved simultaneously with Theorem 4.

From Theorem 4 in the case of a finite field, it follows that the isogeny class of an abelian variety over a finite field is determined by the characteristic polynomial of the Frobenius element. By making an adroit application of the Chebotarev density theorem (and Theorems 3 and 4), the author shows the following: given S and g, there exists a finite set T of primes of K such that the isogeny class of an abelian variety over K of dimension g with good reduction outside S is determined by the characteristic polynomials of the Frobenius elements at the v in T. (This in fact seems to give an algorithm for deciding when two abelian varieties over a number field are isogenous.) Since the known properties of these polynomials (work of Weil) imply there are only finitely many possibilities for each prime, this proves Theorem 5.

In proving Theorem 6, only abelian varieties B isogenous to a fixed abelian variety A need be considered (because of Theorem 5), and, after K has been extended, A can be assumed to have semistable reduction everywhere. The definition of the height is such that $e(B/A) \overset{\text{df}}{=} \exp(2[K:\mathbf{Q}](h(B)-h(A)))$ is a rational number whose numerator and denominator are divisible only by primes dividing the degree of the isogeny between A and B. Therefore, $(*)$ shows there exists an integer N such that $e(B/A)$ involves only the primes dividing N. The isogenies whose degrees are divisible only by the primes dividing N correspond to Γ-stable sublattices of $\prod_{l|\mathbf{N}} T_l A$. From what has been shown about $T_l A$, there exist only finitely many isomorphism classes of such sublattices, and this shows that the set of possible values $h(B)$ is finite. Now Theorem 1 can be applied to prove Theorem 6.

The proof of Theorem 1 is the longest and most difficult part of the paper. The basic idea is to relate the theorem to the following elementary result: given h, there are only finitely many points in $\mathbf{P}^n(K)$ with height (in the usual sense) $\leq h$. The author's height defines a function on the moduli space M_g of principally polarized abelian varieties of dimension g. If M_g is embedded in $\mathbf{P}^n_K$ by means of modular forms rational over K, then the usual height function on $\mathbf{P}^n$ defines a second function on M_g. The two functions must be compared. Both are defined by Hermitian line bundles on M_g and the main points are to show (a) the Hermitian structure corresponding to the author's height does not increase too rapidly as one approaches the boundary of M_g (it has only logarithmic singularities) and (b) by studying the line bundles on compactifications of moduli schemes over $\mathbf{Z}$, one sees that the contributions to the two heights by the finite primes differ by only a bounded amount. This leads to a proof of Theorem 1. (P. Deligne has given a very concise, but clear, account of this part of the paper ["Preuve des conjectures de Tate et de Shafarevitch", Seminaire Bourbaki, Vol. 1983/84, Astérisque No. 121-122 (1985), 25–41; MR0768952 (87c:11026)].)

The proofs of Theorems 2 and $(*)$ are less difficult: they involve calculations which reduce the questions to formulas of M. Raynaud [Bull. Soc. Math. France **102** (1974), 241–280; MR0419467 (54 #7488)].

Torelli's theorem says that a curve is determined by its canonically polarized Jacobian. Thus Theorem 6 implies the (original) conjecture of Shafarevich: given S and g, there exist only finitely many nonsingular projective curves over K of genus g and good reduction outside S. An argument of A. N. Parshin [Izv. Akad. Nauk SSSR Ser. Mat. **32** (1968), 1191–1219; MR0257086 (41 #1740)] shows that Shafarevich's conjecture implies that of Mordell: to each rational point P on the curve X one associates a covering $\varphi_P : X_P \to X$ of X; the curve X_P has bounded genus and good reduction outside S; thus there are only finitely many possible curves X_P, and a classical theorem of de Franchis shows that for each X_P there are only finitely many possible φ_P; as the association $P \mapsto (X_P, \varphi_P)$ is one-to-one, this proves that there are only finitely many P.

Before this paper, it was known that Theorem 6 implies Theorems 3 and 4 (and Mordell's conjecture). One of the author's innovations was to see that by proving a weak form of Theorem 6 (namely Theorem 1) he could still prove Theorems 3 and 4 and then could go back to get Theorem 6.

Only one misprint is worth noting: the second incorrect reference in the proof of Theorems 3 and 4 should be to Zarkhin's 1975 paper [op. cit.], not his 1974 paper.

(From MathSciNet, May 2006)

James Milne

MR0735341 (85f:11048) 11J68 11D41

Evertse, J.-H.

On equations in S-units and the Thue-Mahler equation.

Invent. Math. **75** (1984), *no.* 3, 561–584.

Many finiteness results in the theory of Diophantine equations can be reduced to the assertion that for fixed λ and μ, the equation $\lambda u+\mu v = 1$ has only finitely many solutions (u, v) in S-units of a given number field. The author's main result gives an upper bound for the number of such solutions. The interest of this bound lies in its strong uniformity; it depends only on the degree of the number field and the number of primes in the set S. An estimate which depends also on the primes in S had previously been given by D. J. Lewis and K. Mahler [Acta Arith. 6 (1960/61), 333–363; MR0120195 (22 #10952)]. The author then applies his theorem to obtain uniform bounds for the number of solutions to Diophantine equations of Thue-Mahler and Ramanujan-Nagell type. The proof of the main theorem makes use of hypergeometric functions to investigate cubic irrationalities and their Diophantine approximations.

(From MathSciNet, May 2006)

Joseph H. Silverman

MR1333035 (96d:11071) 11G05 11D41 11F11 11F80 11G18

Wiles, Andrew

Modular elliptic curves and Fermat's last theorem.

Ann. of Math. (2) **141** (1995), *no.* 3, 443–551.

In June 1993 at the Isaac Newton Institute in Cambridge, England, Andrew Wiles announced in a series of lectures that he had proved Fermat's Last Theorem by proving a large part of the Taniyama-Shimura conjecture on the modularity of elliptic curves. Within a few months it turned out that the announcement was premature and the proof not complete. There had been many such claims before, beginning with Fermat's own 17th-century marginal note, which were never fulfilled. But Wiles persevered, and the last missing step was proved jointly by Richard Taylor and Wiles [Ann. of Math. (2) **141** (1995), no. 3, 553–572; MR1333036 (96d:11072)]. Published less than two years after the original announcement, Wiles' paper contains a proof very close to the original outline he described in his lectures. See the introduction for a very readable step-by-step account of the history of the Wiles and Taylor-Wiles papers. For expository articles about the proof of Fermat's Last Theorem, see papers by F. Q. Gouvêa [Amer. Math. Monthly **101** (1994), no. 3, 203–222; MR1264001 (94k:11033)], K. A. Ribet [Bull. Amer. Math. Soc. (N.S.) **32**

(1995), no. 4, 375–402; MR1322785 (96b:11073)], or K. C. Rubin and A. Silverberg [Bull. Amer. Math. Soc. (N.S.) **31** (1994), no. 1, 15–38; MR1256978 (94k:11062); erratum; Bull. Amer. Math. Soc. (N.S.) **32** (1995), no. 1, 170; MR1300061].

The Taniyama-Shimura conjecture is one of the most important outstanding problems concerning elliptic curves. As formulated by Shimura in the early 1960s, it asserts that every elliptic curve defined over the rational numbers is modular (see below). Wiles proved the modularity of a large class of elliptic curves, including all semistable ones. Although less than the full Taniyama-Shimura conjecture, this result still suffices to prove Fermat's Last Theorem.

Fermat's Last Theorem asserts that there are no positive integers a, b, c, and n, with $n > 2$, such that $a^n + b^n = c^n$. To a hypothetical solution of this equation one can associate an elliptic curve

$$E_{a^n,b^n}\colon y^2 = x(x - a^n)(x + b^n).$$

This connection was first noticed and used in the late 1960s by Hellegouarch. In the mid-1980s Frey described how to use this construction to connect Fermat's Last Theorem to the Taniyama-Shimura conjecture. Ribet [Invent. Math. **100** (1990), no. 2, 431–476; MR1047143 (91g:11066)] was able to prove what Frey suspected: if $a^p + b^p = c^p$ and p is a prime greater than 3, then $E_{a^p b^p}$ is not modular. In other words, the Taniyama-Shimura conjecture implies Fermat's Last Theorem.

Fix an elliptic curve E and a prime p. The Galois group $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on the group $E(\overline{\mathbf{Q}})$ of points of E with coordinates in $\overline{\mathbf{Q}}$, and the action on the p-power torsion points $E(\overline{\mathbf{Q}})_{p^\infty} \cong (\mathbf{Q}_p/\mathbf{Z}_p)^2$ gives rise to a representation $\rho_{E,p}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_p)$. On the other hand, if $f(z) = e^{2\pi iz} + \sum_{n>1} a_n e^{2\pi inz}$ is a cusp form of weight two for some $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbf{Z})$, f is an eigenfunction of all Hecke operators, and λ is a prime above p of the ring of integers $\mathcal{O}_f$ of the number field $\mathbf{Q}(a_2, a_3, \cdots)$, then Eichler and Shimura associated to f a representation $\rho_{f,\lambda}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_\lambda)$, where $\mathcal{O}_\lambda$ is the completion of $\mathcal{O}_f$ at λ. One says E is modular if $\rho_{E,p}$ "comes from a modular form", i.e., if there exist such a form f and prime ideal λ with $\rho_{E,p} \cong \rho_{f,\lambda}$. This definition does not depend on the choice of p.

Write $\overline{\rho}_{E,p}$ and $\overline{\rho}_{f,\lambda}$ for the representations into $\mathrm{GL}_2(\overline{\mathbf{F}}_p)$ obtained from $\rho_{E,p}$ and $\rho_{f,\lambda}$ by reduction modulo p and λ, respectively. Wiles' approach is to prove E is modular in two steps: (1) show that there are f and λ such that $\overline{\rho}_{E,p} \cong \overline{\rho}_{f,\lambda}$, (2) show that for *every* representation $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_\lambda)$ satisfying certain natural properties, and such that the reduction of ρ modulo λ is isomorphic to $\overline{\rho}_{f,\lambda}$ (so in particular for $\rho = \rho_{E,p}$), there are f' and λ' such that $\rho \cong \rho_{f',\lambda'}$.

Although little is known in general about step (1), it is known in the case in which $p = 3$ and $\overline{\rho}_{E,3}$ is irreducible by work of R. P. Langlands [*Base change for* GL(2), Ann. of Math. Stud., 96, Princeton Univ. Press, Princeton, NJ, 1980; MR0574808 (82a:10032)] and of J. Tunnell [Bull. Amer. Math. Soc. (N.S.) **5** (1981), no. 2, 173–175; MR0621884 (82j:12015)]. (The irreducibility condition turns out not to be a serious problem: when $\overline{\rho}_{E,3}$ is reducible, Wiles makes very clever use of the irreducible case for $p = 3$ to prove step (1) for $p = 5$.) The heart of Wiles' proof is his proof of step (2) under certain weak assumptions.

Very briefly, the proof goes as follows. Suppose E is semistable at p, $\overline{\rho}_{E,p}$ is irreducible, and f and λ are given by step (1). Write $\mathcal{O}$ for $\mathcal{O}_\lambda$ and let k be its residue field. B. Mazur's deformation theory of Galois representations [in *Galois groups over* **Q** *(Berkeley, CA, 1987)*, 385–437, Springer, New York, 1989; MR1012172 (90k:11057)], with one important case due to R. Ramakrishna [Compositio Math.

87 (1993), no. 3, 269–286; MR1227448 (94h:11054)], gives a complete local Noetherian $\mathcal{O}$-algebra R with residue field k and a representation $\rho_R\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(R)$ whose reduction is $\overline{\rho}_{f,\lambda}$, such that for every complete local Noetherian $\mathcal{O}$-algebra A with residue field k, every representation $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(A)$ with prescribed ramification properties and whose reduction is $\overline{\rho}_{f,\lambda}$ factors through $\mathrm{GL}_2(R)$ by a unique map from R to A. In other words, the "universal deformation ring" R parametrizes all "liftings" of $\overline{\rho}_{f,\lambda}$ with prescribed ramification properties. On the other hand, Wiles constructs a completed Hecke algebra $\mathbf{T}$ which parametrizes all liftings of $\overline{\rho}_{f,\lambda}$ with the same prescribed ramification properties which come from modular forms. The universal property gives a surjective map $\varphi\colon R \to \mathbf{T}$, and to verify step (2) it suffices to show that φ is an isomorphism.

Let $\pi\colon \mathbf{T} \to \mathrm{End}(f\mathcal{O}) \cong \mathcal{O}$ be the map giving the action of $\mathbf{T}$ on the modular form f, let $\mathfrak{p}_{\mathbf{T}} = \ker(\pi)$, and let $\mathfrak{p}_R = \ker(\pi \circ \varphi)$. Using commutative algebra and algebraic properties of the Hecke algebra $\mathbf{T}$, Wiles shows that the injectivity of φ follows from the inequality $\#(\mathfrak{p}_R/{\mathfrak{p}_R}^2) \leq \#(\mathfrak{p}_{\mathbf{T}}/\mathfrak{p}_{\mathbf{T}}^2)$. (This inequality can be viewed as an analogue of the analytic class number formula for cyclotomic fields, which played a major role in earlier work on Fermat's Last Theorem.) Under certain mild conditions on $\overline{\rho}_{E,p}$, Wiles reduces the verification of this inequality to the "minimal" case, where the prescribed ramification conditions are as strict as possible. (In this reduction, results and methods of Ribet [in *Motives (Seattle, WA, 1991)*, 639–676, Proc. Sympos. Pure Math., 55, Part 2, Amer. Math. Soc., Providence, RI, 1994; MR1265566 (95d:11056)] and others developed to attack J.-P. Serre's conjectures [Duke Math. J. **54** (1987), no. 1, 179–230; MR0885783 (88g:11022)] play a crucial role.) Wiles then proves the desired equality in the minimal case under the assumption that $\mathbf{T}$ is a complete intersection. The verification that $\mathbf{T}$ is a complete intersection is proved in the Taylor-Wiles paper [op.cit.].

(From MathSciNet, May 2006)

Karl Rubin

MR1333036 (96d:11072) 11G18 11D41 11F1 11R34 13C40

Taylor, Richard; Wiles, Andrew

Ring-theoretic properties of certain Hecke algebras.

Ann. of Math. (2) **141** (1995), *no.* 3, 553–572.

This paper provides the proof of an important step needed for Wiles' work [Ann. of Math. (2) **141** (1995), no. 3, 443–551; MR1333035 (96d:11071)] on Fermat's Last Theorem and the Taniyama-Shimura conjecture.

Given a finite field k of odd characteristic p and a representation $\overline{\rho}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(k)$ satisfying certain local conditions and an irreducibility condition, the authors define a congruence subgroup Γ of $\mathrm{SL}_2(\mathbf{Z})$ and a completion $\mathbf{T}$ of the Hecke algebra of cusp forms on Γ, with scalars extended to the ring of integers $\mathcal{O}$ of a sufficiently large finite extension of $\mathbf{Q}_p$. The main result of this paper is that $\mathbf{T}$ is a complete intersection ring.

The proof uses a new kind of Iwasawa theory argument. For finite sets Q of primes, the authors study enlarged Hecke rings $\mathbf{T}_Q$ formed by replacing Γ by a subgroup Γ_Q of Γ containing $\Gamma \cap \Gamma_1(\prod_{q\in Q} q)$. Let Δ_Q be the p-Sylow subgroup of $\prod_{q\in Q}(\mathbf{Z}/q\mathbf{Z})^\times$. Subject to some conditions on the primes in Q, the authors prove (using methods of E. de Shalit [Compositio Math. **95** (1995), no. 1, 69–100; MR1314697 (96i:11063)]) that $\mathbf{T}_Q$ is a free $\mathcal{O}[\Delta_Q]$-module of rank equal to $\mathrm{rank}_{\mathcal{O}}(\mathbf{T})$.

Next, for an appropriate integer r, the authors carefully choose sets Q_n, $n \geq 1$, such that for every n, $\#(Q_n) = r$ and all primes in Q_n are congruent to 1 modulo p^n. In particular each Δ_{Q_n} has a quotient isomorphic to $(\mathbf{Z}/p^n\mathbf{Z})^r$. Using a compactness argument the authors artificially patch together finite quotients of a subsequence of the $\mathbf{T}_{Q_n}$ to construct an "inverse limit" $\mathbf{T}_\infty$ of the $\mathbf{T}_{Q_n}$ such that $\mathbf{T}_\infty$ is a free module over a power series ring $\mathcal{O}[\![X_1, \cdots, X_r]\!]$, $\mathbf{T}_\infty/(X_1, \cdots, X_r)\mathbf{T}_\infty \cong \mathbf{T}$, and $\mathbf{T}_\infty$ is generated as an $\mathcal{O}$-algebra by r elements. From this it follows that $\mathbf{T}$ is a quotient of a power series ring in r variables by r relations, and hence is a complete intersection.

The paper has an appendix explaining a simplification suggested by Faltings to some of the arguments of Chapter 3 of Wiles' paper [op. cit.] and to §3 of this paper.

(From MathSciNet, May 2006)

Karl Rubin

MR2076124 (2005f:11051) 11D61 11R18 11R27

Mihăilescu, Preda

Primary cyclotomic units and a proof of Catalan's conjecture. (English. English summary)

J. Reine Angew. Math. **572** (2004), 167–195.

In 1844, in a letter to the editor of Crelle's Journal, Eugène Catalan formulated his famous conjecture that two consecutive natural numbers other than 8 and 9 cannot be proper powers. In other words, he conjectured that the only nontrivial solution to the Diophantine equation $x^p - y^q = 1$ is given by $3^2 - 2^3 = 1$. Catalan's short note appeared in volume 27 of Crelle's journal. 160 years later Mihăilescu's ingenious proof appears in volume 572 of the same journal.

A brief outline of the proof of Catalan's conjecture runs as follows. It suffices to give a proof for prime exponents. In view of earlier work, we may even assume $p, q > 3$. There is a symmetry: if (x, y, p, q) is a solution to Catalan's equation, so is $(-y, -x, q, p)$. Suppose that we have a nonzero solution to Catalan's equation $x^p - y^q = 1$. Since we have $p \neq q$, the symmetry allows us to assume $p > q$. In the paper under review Mihăilescu shows that one necessarily has $p \equiv 1 \pmod{q}$. In 2000 Mihăilescu had already established his "double Wieferich criterion" [J. Number Theory **99** (2003), no. 2, 225–231; MR1968450 (2004b:11040)]. It says that one has $p^{q-1} \equiv 1 \pmod{q^2}$ as well as $q^{p-1} \equiv 1 \pmod{p^2}$. Combining this with the result in the paper under review, we find that the existence of a nonzero solution to Catalan's equation $x^p - y^q = 1$ implies $p \equiv 1 \pmod{q^2}$. Since $p = 1 + kq^2$ is not prime for $k = 1, 2, 3$, it follows that we have $p > 4q^2$. In other words, p is much larger than q. In this situation, the techniques from the theory of linear forms in logarithms are particularly effective. In appendix B of the paper, it is shown that the inequality implies $q < 25000$. A short computer calculation then completes the proof. Since the present paper was written, Mihăilescu has proved a third result. This enabled him to replace the argument involving linear forms in logarithms and the computer calculation by a purely algebraic proof that exploits the theory of cyclotomic fields [“On the relative class group of cyclotomic extensions in presence of a solution to Catalan’s equation”, J. Number Theory, to appear].

In order to describe the proof of the main result of the paper under review, we assume $p > q$ as well as $p \not\equiv 1 \pmod{q}$ and we explain how Mihăilescu deduces a contradiction. A standard descent argument applied to a nonzero solution of the equation $x^p - y^q = 1$ shows that the ideal generated by $x - \zeta_p$ in the ring $\mathbb{Z}[\zeta_p, \frac{1}{p}]$ is the q-th power of an ideal. Here ζ_p denotes a primitive p-th root of unity. In addition, it follows from Mihăilescu’s double Wieferich criterion that $x - \zeta_p$ is a q-adic q-th power, i.e. it is a q-th power in the completions at all primes lying over q. Therefore it is convenient to proceed as follows. Let H be the subgroup of elements $a \in \mathbb{Q}(\zeta_p)^*$ that are q-adic q-th powers and for which the principal ideal (a) is a q-th power. Then the ‘Selmer group’ $S = H/\mathbb{Q}(\zeta_p)^{*q}$ is a finite obstruction group containing $x - \zeta_p$. There is an exact sequence of $\mathbb{Z}/q\mathbb{Z}$-vector spaces

$$0 \longrightarrow E_q/E^q \longrightarrow S \longrightarrow \mathrm{Cl}[q].$$

Here E and Cl denote the unit group and ideal class group of $\mathbb{Z}[\zeta_p, \frac{1}{p}]$ respectively. By $\mathrm{Cl}[q]$ we denote the q-torsion subgroup of Cl and by E_q the subgroup of E that consists of q-adic q-th powers. All these groups as well as the obstruction group S itself are $\mathbb{Z}/q\mathbb{Z}[G]$-modules for $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Any such module is a direct product of its plus and minus parts, i.e. of the subspaces that are invariant and anti-invariant respectively under the action of complex conjugation $\iota \in G$. The plus part is a module over the group ring $\mathbb{Z}/q\mathbb{Z}[G^+]$, where G^+ denotes the quotient group $G/\langle\iota\rangle$.

Mihăilescu first shows that the element $(x - \zeta_p)^{1+\iota}$ generates a free $\mathbb{Z}/q\mathbb{Z}[G^+]$-module inside S^+. Indeed, if $\theta \in \mathbb{Z}[G^+]$ has the property that $(x - \zeta_p)^{(1+\iota)\theta} = a^q$ for some $a \in \mathbb{Q}(\zeta_p)^*$, then there is also such an element θ for which the group ring element

$$(1 + \iota)\theta = \sum_{\sigma \in G} n_\sigma \sigma$$

has small non-negative coefficients. Inspection of the p-adic valuation of $x - \zeta_p$ shows that $\sum_{\sigma \in G} n_\sigma = mq$ for some integer $m \geq 0$. Therefore we have

$$(x - \zeta_p)^{(1+\iota)\theta} = \prod_{\sigma \in G} (x - \sigma(\zeta_p))^{n_\sigma} = x^{mq} + (\text{lower degree terms}),$$

and we are led to the equation

$$x^{mq} + (\text{lower degree terms}) = a^q.$$

This is a Diophantine equation with coefficients in the ring of integers of the totally real number field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Mihăilescu solves it by what can be viewed as an application of C. Runge’s method [J. Reine Angew. Math. **100** (1887), 425–435; JFM 19.0076.03]. He shows that there are no solutions $x \in \mathbb{Z}$ unless we have $\theta = 0$. For Mihăilescu’s proof to work, it is important to know that x and y cannot be small. This follows from an old result of J. W. S. Cassels [Proc. Cambridge Philos. Soc. **56** (1960), 97–103; MR0114791 (22 #5610)], which says that any nonzero solution to the Catalan equation $x^p - y^q = 1$ has the property that p divides y and q divides x. This is easily seen to imply that both integers x, y are necessarily very large. It follows that the $\mathbb{Z}/q\mathbb{Z}[G^+]$-annihilator of $(x - \zeta_p)^{1+\iota}$ in S is zero, as required.

In order to obtain a contradiction, Mihăilescu considers the following filtration of the $\mathbb{Z}/q\mathbb{Z}[G^+]$-module E/E^q of p-units modulo q-th powers:

$$0 \subset C_q E^q/E^q \subset CE^q/E^q \subset E/E^q.$$

Here C is the multiplicative group of cyclotomic p-units. It is generated by $1-\zeta_p$ and its conjugates. We put $C_q = C \cap E_q$. By the assumption $p \not\equiv 1 \pmod{q}$, the ring $\mathbb{Z}/q\mathbb{Z}[G^+]$ is semi-simple. Since exact sequences of $\mathbb{Z}/q\mathbb{Z}[G^+]$-modules are automatically split, E/E^q is isomorphic to the direct product of the subquotients $E_1 = C_qE^q/E^q$, $E_2 = CE^q/C_qE^q$ and $E_3 = E/CE^q$ of the filtration above. Similarly, it follows easily from the exactness of the sequence $0 \to E_1 \to E_q/E^q \to E_3$ that the Selmer group S is isomorphic to a submodule of $E_1 \times E_3 \times \mathrm{Cl}[q]$. Since E/E^q is invariant under complex conjugation, we therefore have $S^+ \subset E_1 \times E_3 \times \mathrm{Cl}[q]^+$.

By F. Thaine's Theorem [Ann. of Math. (2) **128** (1988), no. 1, 1–18; MR0951505 (89m:11099)], the $\mathbb{Z}/q\mathbb{Z}[G^+]$-annihilator of E_3 automatically annihilates the plus part of $\mathrm{Cl}[q]$ as well. It follows that the $\mathbb{Z}/q\mathbb{Z}[G^+]$-annihilator of $E_1 \times E_3$ annihilates S^+. However, we saw above that S^+ contains the free $\mathbb{Z}/q\mathbb{Z}[G^+]$-module generated by $(x-\zeta_p)^{1+\iota}$. Therefore its annihilator is zero. As a consequence, so is the annihilator of $E_1 \times E_3$. Since $E/E^q \cong E_1 \times E_2 \times E_3$ is a free $\mathbb{Z}/q\mathbb{Z}[G^+]$-module of rank 1, it follows that the annihilator of E_2 is the unit ideal, so that the subquotient $E_2 = CE^q/C_qE^q$ is trivial. In other words, every cyclotomic p-unit is a q-adic q-th power. However, this conclusion is absurd. Indeed, we have $(\zeta_p - 1)^q \equiv \zeta_p^q - 1 \pmod{q}$. If the cyclotomic p-unit $\zeta_p^q - 1$ is a q-th power, then this congruence actually holds modulo q^2. This implies that every p-th root of unity is a zero of the polynomial

$$W(T) = \frac{(T-1)^q - T^q + 1}{qT} \in \mathbb{Z}/q\mathbb{Z}[T].$$

But this is impossible since the degree of the cyclotomic polynomial is $p-1$, and by our assumption $p > q$, this exceeds the degree of $W(T)$, which is $q-2$.

This contradiction proves Mihăilescu's Theorem.

(From MathSciNet, May 2006)

René Schoof