# LINKS BETWEEN STABLE ELLIPTIC CURVES AND CERTAIN DIOPHANTINE EQUATIONS

By

Gerhard Frey

I. Introduction. The most popular diophantine equation is perhaps the equation

$$C_{F_n} : Z_1^n - Z_2^n = Z_3^n$$

where n is a natural number.

A (non trivial) solution of $C_{F_n}$ is a triple $(z_1, z_2, z_3) \in Z^3$ with $z_1 \cdot z_2 \cdot z_3 \neq 0$ and $\gcd(z_1, z_2, z_3) = 1$ and satisfying $C_{F_n}$. It is well known that for $n = 1, 2$ there are infinitely many solutions of $C_{F_n}$, for $n = 3$ (and many other exponents) there are no solutions, and due to Falting's theorem and the fact that the genus of the curve defined by $C_{F_n}$ is larger than 1 for $n > 3$ it follows that there are only finitely many solutions for $n > 3$.

The famous conjecture denoted as "Fermat's last theorem" is

CONJECTURE $F_n$. For $n \geq 3$ there are no solutions of $C_{F_n}$.

It is easily seen that the essential case is that $n = p$ is a prime.

If one tries to prove $F_p$ it soon becomes obvious that the arithmetic of the cyclotomic field $\mathbb{Q}(\zeta_p)$ where $\zeta_p$ is a primitive p-th root of unity plays an important role. This observation first made by Kummer was a great stimulus for the development of algebraic number theory and especially of class field theory: One studies unramified abelian extensions of $\mathbb{Q}(\zeta_p)$ whose degree is a p-power, and in the "regular case" where no such extensions exist, it follows that $F_p$ is true (cf. [1]). In other words: The non-existence of 1-dimensional unramified representations of the absolute Galois group $G_{\mathbb{Q}(\zeta_p)}$ of $\mathbb{Q}(\zeta_p)$ in $Gl_1(\mathbb{C})_p$ implies $F_p$.

So it seems to be natural to look for higher dimensional representations $\rho$ of $G_{\mathbb{Q}(\zeta_p)}$ with only small ramification, and the first case to test is: $\rho$ has dimension 2 and is induced by the action of $G_{\mathbb{Q}(\zeta_p)}$ on the points of order p of an elliptic curve E defined over $\mathbb{Q}$.

There is our motivation to relate an elliptic curve E with remarkable arithmetical properties to any solution of equations of "Fermat type" (see II). Especially E is stable over $\mathbb{Q}$ (cf. [2]). In the case of the original Fermat equation the properties of E are so excellent that one suspects that such a curve cannot exist (cf. the Theorem on p. 15).

Now one has to attack those elliptic curves, and here the conjecture of Taniyama and Shimura enters: Each elliptic curve E over $\mathbb{Q}$ should be a quotient of the Jacobian of an appropriate modular curve $X_o(N)$. The resulting parametrization

$$\varphi: X_o(N) \longrightarrow E$$

carries all essential arithmetical data of E: If we choose N to be minimal with respect to E then N is the geometric conductor of E.

If $\omega$ is a holomorphic differential on E then $\varphi^*\omega$ corresponds to a modular form f of weight 2 on $X_o(N)$, and this form f determines the representations of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ induced by the action of $G_{\mathbb{Q}}$ on the torsion points of E, and the third essential data for us turns out to be the degree of $\varphi$.

In III. we describe those facts in more detail and we state two types of conjectures that would imply Fermat's last theorem. The first type is due to Serre and is in the spirit of the representation-theoretical point of view we described above; it emphasizes the special role of the equation $C_{F_p}$ amongst all other equations of this type. The second type of conjectures states that the degree of $\varphi: X_o(N) \longrightarrow E$ should have a polynomial bound in N; it is due to Szpiro and supported by the "function field case". If this conjecture would be true it would

have consequences for all equations of "Fermat type" at least for large exponents.

Both types of conjectures have links to so called "congruence primes" (cf. [6]), and we give results about these primes in IV. using results of Deligne, Rapoport and Mazur about the Néron model of $J_0(N)$ over $\mathbb{Z}$ in the case that N is square free.

## II. Construction of stable elliptic curves

1. Arithmetic of elliptic curves. In the following we list some notions and properties concerning elliptic curves over $\mathbb{Q}$ that are relevant for us. For a systematic study of elliptic curves over global fields we refer to [9].

An elliptic curve $E/\mathbb{Q}$ is a projective irreducible curve of genus 1 with (at least) one $\mathbb{Q}$-rational point $P_\infty$. The theorem of Riemann-Roch implies that one can find plane projective curves of degree 3 which are models for E such that $P_\infty$ is the only "infinite" point of E. The equations for these models can be chosen in normal forms whose affine versions we write down:

The generalized Weierstraß normal form:

E is given by

$$N_E: Y^2+\lambda XY+\mu Y = X^3+\alpha X^2+\beta X+\gamma$$

with $\alpha,\beta,\gamma,\lambda,\mu \in \mathbb{Z}$ such that $N_E$ has no singular points. There is a biregular transformation defined over $\mathbb{Z}[\frac{1}{2}]$ of the affine plane such that E is given by

$$N'_E: \; Y^2 = X^3+AX^2+BX+C$$

where again A,B,C are elements of $\mathbb{Z}$ and the non singularity of E now means: The discriminant of the polynomial $X^3+AX^2+BX+C$ is different from 0.

If we allow transformations of type: $X \longrightarrow X' + \frac{1}{3}A$ we get the usual Weierstraß normal form of E:

$$N''_E: \; Y^2 = X^3-g_2X-g_3$$

where $g_i \in \mathbb{Z}$ without loss of generality and

$$\Delta := 4g_2^3-27g_3^2 \neq 0 \; .$$

The only transformations that preserve the Weierstraß normal form are of the type: $X \longrightarrow X' = \mu^2X$, $Y \longrightarrow Y' = \mu^3Y$ with $\mu \in \mathbb{Q}^*$. Then $g_2$ is transformed to $\mu^{-4}g_2$ and $g_3$ to $\mu^{-6}g_3$. Hence, the discriminant $\Delta$ of $X^3-g_2X-g_3$ is transformed to $\mu^{-12}\cdot\Delta$.

The Weierstraß normal form is very convenient for defining the invariants of E (determining E completely over $\mathbb{Q}$): The absolute invariant $j_E$ of E is given by

$$j_E := 12^3\cdot 4g_2^3\cdot\Delta^{-1} \; ,$$

and the Hasse invariant $\delta_E$ of E is given by

$$\delta_E := -\frac{1}{2}g_2 \cdot g_3^{-1} \bmod \mathbb{Q}^{*2} \quad \text{if } j_E \neq 0, 12^3 .$$

(For all elliptic curves that occur in this paper we have that $j_E \notin \mathbb{Z}$ and hence $j_E \neq 0, 12^3$.)

A most effective tool to study elliptic curves over $\mathbb{Q}$ is the reduction theory:

We give by an equation in generalized Weierstraß normal form:

$$N_E: \; Y^2+\lambda XY+\mu Y = X^3+\alpha X^2+\beta Y+\gamma$$

with coefficients in $\mathbb{Z}$. Let $l$ be a prime and $\bar{\alpha},\bar{\beta},\bar{\gamma},\bar{\lambda},\bar{\mu}$ the residue classes in $\mathbb{F}_l = \mathbb{Z}/l$ of the corresponding coefficients. Then

$$N_{E(l)}: \; Y^2+\bar{\lambda}XY+\bar{\mu}Y = X^3+\bar{\alpha}X^2+\bar{\beta}X+\bar{\gamma}$$

defines a plane affine curve over $\mathbb{F}_l$ whose projective closure $E^{(l)}$ has three possibilities:

1. "Good reduction case": $E^{(l)}$ is an elliptic curve again, i.e. it has no singular points. In case that $\lambda,\mu$ and $\alpha$ are equal to zero and $l \neq 2,3$ there is a simple criterion for this case: We have $v_l(j_E) \geq 0$ and $v_l(4\beta^3-27\gamma^2) = v_l(\Delta) = 0$.

DEFINITION. E has good reduction mod $l$ if there is an equation $N_E$ for E such that $N_{E(l)}$ defines an elliptic curve over $\mathbb{F}_l$.

2. "Multiplicative type": In this case $E^{(1)}$ has a singularity in exactly one point and there are two different tangent lines in that point. The typical case is: $v_1(\lambda) = 0$, $v_1(\mu) > 0$, $v_1(\alpha) > 0$, $v_1(\beta) > 0$ and $v_1(\gamma) = -v_1(j_E) > 0$.

DEFINITION. E has reduction of multiplicative type mod 1 if there is an equation $N_E$ for E such that $N_{E^{(1)}}$ defines a curve with one singular point and different tangent lines in that point.

E has reduction of multiplicative type if and only if $v_1(j_E) < 0$ and $\mathbb{Q}(\sqrt{\delta_E})$ is unramified in 1.

3. "Additive type": This is the "worst" case. Again $N_{E^{(1)}}$ defines a curve over $\mathbb{F}_1$ with one singular point but now there is only one tangent line through this point.

The description of cases 1. and 2. shows that after a finite constant field extension the reduction type of E modulo an extension of 1 is of type 1. or 2., and thereafter the type never changes again. For this reason one says: E has stable reduction mod 1 if there exists a model of E that has good reduction or reduction of multiplicative type mod 1.

The notion "multiplicative type" (resp. "additive type") derives from the fact that the non singular points of $E^{(1)}$ are (as algebraic groups) isomorphic to a torus split by

an extension of degree $\leq 2$ (resp. to the additive group) over $\mathbb{F}_l$.

The most important fact about elliptic curves with reduction of multiplicative type is due to Tate: Let K be a finite extension field of the field $\mathbb{Q}_l$ of l-adic numbers with $\delta_E \in K^{\times 2}$ and assume that E has reduction of multiplicative type mod l. Then the group of K-rational points of E, E(K), is analytically isomorphic to $K/\langle q \rangle$ where q, the l-adic period of E, is an element in $\mathbb{Q}_l$ wit $j_E = \frac{1}{q} + \sum_{i \geq 0} a_i q^i$. The elements $a_i$ are the integers occuring in the usual Fourier expansion of the (classical) j-function over $\mathbb{C}$ (with $q = e^{2\pi i \tau}$). As reference for this theory we mention [7].

We only need the following consequence: Let $E/\mathbb{Q}$ be an elliptic curve with reduction of multiplicative type mod l. Let $E_p$ denote the group of points of order dividing p of $E(\overline{\mathbb{Q}})$, and denote by $K_p$ the field obtained by adjoining the coordinates of points in $E_p$ to $\mathbb{Q}$. Let l be a divisor of l in $K_p$ and $K_{p,l}$ the completion of $K_p$ with respect to l. Then $K_{p,l} = \mathbb{Q}(\zeta_p, \sqrt[p]{j_E})$.

For $l \nmid p$ and the case that E has good reduction mod l Hensel's lemma gives information about $K_{p,l}$, and especially we get: l is unramified in $K_p$.

For brevity's sake we make the

DEFINITION. An elliptic curve E over $\mathbb{Q}$ is stable if it has stable reduction modulo all primes.

The considerations made above prove the following

PROPOSITION 1. Let E be a stable elliptic curve defined over $\mathbb{Q}$. Let $K_p$ be the field extension of $\mathbb{Q}$ obtained by adjoining the coordinates of points in $E_p$. Then $K_p$ is unramified over $\mathbb{Q}$ in all primes $l \neq p$ with $v_l(j_E) \geq 0$ or $v_l(j_E) \equiv 0 \bmod p$.

If E is stable we find for all primes l a generalized Weierstraß equation with integral coefficients such that the reduction mod l of this equation is optimal. Since $\mathbb{Z}$ is a principal domain we find one generalized Weierstraß equation corresponding to E with optimal reduction behaviour modulo all primes simultaneously. This equation is called a "minimal Weierstraß equation", and from now on we will assume that

$$N_E: Y^2+\lambda XY+\mu Y = X^3+\alpha X^2+\beta X+\gamma$$

with $\alpha,\beta,\gamma,\lambda,\mu \in \mathbb{Z}$ is a minimal equation. The discriminant of $N_E$ is called the discriminant of E and denoted by $\Delta_E$.

The following facts hold:

Assume that E is stable. Then $v_l(\Delta_E) = -\mathrm{Min}(v_l(j_E),0)$ for all primes l, and the geometric conductor of E is equal to $N := \prod_{v_l(\Delta_E)>0} l$.
(For the definition of the conductor we refer to [9].)

2. Stable elliptic curves. Now we want to construct elliptic curves E with stable reduction modulo all primes such that the corresponding field $K_p$ has only small ramification over $\mathbb{Q}(\zeta_p)$.

We begin with relatively prime integers A and B such that $A \equiv 0 \bmod 2^5$ and $B \equiv 1 \bmod 4$ and put $C := A-B$.
Let E be the elliptic curve given by the equation

$$N_E: \quad Y^2 = X^3+(A+B)X^2+ABX \ .$$

A Weierstraß normal form of E is given by the equation

$$N_{\tilde{E}}: \quad \tilde{Y}^2 = \tilde{X}^3-\frac{1}{3}(A^2+B^2-AB)\tilde{X}+\frac{1}{27}(A+B)(2A^2+2B^2-5AB) \ .$$

The discriminant of $N_{\tilde{E}}$ is equal to $\Delta = A^2.B^2.C^2$.
Hence the j-invariant of E is equal to

$$j_E = 2^8(A^2+B^2-AB)^3.A^{-2}.B^{-2}.C^{-2}$$

and the Hasse invariant of E is equal to

$$\delta_E \equiv \frac{1}{2}\cdot\frac{A^2+B^2-AB}{(A+B)(2A^2+2B^2-5AB)} \bmod \mathbb{Q}^{*2} \ .$$

From those data we can verify the following properties of E:

i) The points of order 2 of E are $\mathbb{Q}$-rational and are equal to $P_o = (0,0)$, $P_1 = (-A,0)$, $P_2 = (-B,0)$ where $P_i$ are points in $N'_E$.

ii) $v_2(j_E) = 8-2v_2(A) \leq -2$ and $\delta_E \equiv B \bmod \mathbb{Q}_2^{*2}$.

By assumption we have: $B \equiv 1 \bmod 4$ so that E has reduction of multiplicative type mod 2.

Now assume that $3 \nmid A\cdot B\cdot C$. Then $A-B = C \not\equiv 0 \bmod 3$ and so $A \not\equiv B \bmod 3$. Hence the polynomial $X^3+(A+B)X^2+ABX$ has 3 different zeros mod 3 and $N_{E(3)}$ is a curve without singularities and E has good reduction mod 3.

In the case that $3 \mid A\cdot B\cdot C$ we get: $v_3(j_E) = -v_3(\Delta) < 0$ and $v_3\left(\frac{1}{2}\,\frac{A^2+B^2-AB}{(A+B)(2A^2+2B^2-5AB)}\right) = 0$ and hence $\mathbb{Q}(\sqrt{\delta_E})$ is unramified in the divisors of 3: E has reduction of multiplicative type mod 3.

If l is a prime different from 2 and 3 then (since $\gcd(AB(A-B), A^2+B^2-AB) = 1$) we get: E has good reduction mod l if and only if $v_l(j_E) \geq 0$, and $v_l(j_E) < 0$ if and only if $l \mid A^2\cdot B^2\cdot C^2$. In the latter case it follows that $v_l(\delta_E) = 0$ and hence E has reduction of multiplicative type mod l.

It follows: E is a stable curve over $\mathbb{Q}$ and the conductor of E is equal to

$$N = \prod_{l \mid A\cdot B\cdot C} l \ .$$

iii) It is easy to find a minimal equation for E:

$$N_E\colon\ Y^2+XY = X^3+ \frac{A+B-1}{4} X^2+ \frac{A\cdot B}{16} X$$

is such an equation, the discriminant of E is equal to

$$\Delta_E = \frac{A^2\cdot B^2\cdot C^2}{2^8} \ .$$

iv) Let p be any odd prime and let $K_p$ be the field obtained by adjoining the coordinates of point of order p of E to $\mathbb{Q}$. Then

$$K_p(\sqrt[p]{2^4\cdot ABC})/\mathbb{Q}(\sqrt[p]{2^4\cdot ABC})$$

is unramified outside of divisors of p.

We specialize the numbers A, B, C.

For relatively prime integers $a_1,a_2,a_3$ and $n_1,n_2,n_3 \in \mathbb{N}$ we define a Fermat type equation: $C\colon a_1 Z_1^{n_1} - a_2 Z_2^{n_2} = a_3 Z_3^{n_3}$. We assume that $(z_1,z_2,z_3)$ is a solution of C with $\gcd(z_1,z_2,z_3) = 1$, $2^5 \mid a_1 z_1^{n_1}$ and $a_2 z_2^{n_2} \equiv 1 \bmod 4$. Put $A = a_1 z_1^{n_1}$, $B = a_2 z_2^{n_2}$ and $C = a_3 z_3^{n_3}$. Then the corresponding elliptic curve is stable with discriminant

$$\Delta_E = 2^{-8}\cdot a_1^2 a_2^2 a_3^2 \cdot z_1^{2n_1}\cdot z_2^{2n_2}\cdot z_3^{2n_3}$$

and conductor

$$N = \prod_{v_1(\Delta_E)>0} 1 .$$

It follows:

$$\frac{2^8\Delta_E}{N} > a_1a_2a_3 \cdot z_1^{2n_1-1} \cdot z_2^{2n_2-1} \cdot z_3^{2n_3-1} .$$

Now we turn to Fermat's equation: Take $a_1, a_2, a_3 = 1$ and $n_1 = n_2 = n_3 = p$ where p is prime $\geq 5$. Then the considerations made above give

PROPOSITION 2: Let $(z_1, z_2, z_3)$ be a solution of $Z_1^p - Z_2^p = Z_3^p$ and assume without loss of generality that $2 | z_1$ and $z_2 \equiv 1 \bmod 4$. Then the elliptic curve E given by the minimal equation

$$Y^2+XY = X^3 + \frac{z_1^p+z_2^p-1}{4} X^2 + \frac{z_1^p \cdot z_2^p}{16} X$$

is stable over $\mathbb{Q}$. Its points of order 2 are $\mathbb{Q}$-rational. Its conductor is equal to $N = \prod_{1 | z_1z_2z_3} 1$, the discriminant $\Delta_E$ is equal to $(2^{-4} \cdot z_1 \cdot z_2 \cdot z_3)^{2p}$, hence $2^8\Delta_E \geq N^{2p}$. The field $K_p$ obtained by adjoining the coordinates of points of order p of E to $\mathbb{Q}$ is unramified over $\mathbb{Q}$ outside the divisors of $2 \cdot p$. If $v_p(j_E) < 0$ then the ramification in divisors of p is "moderately" ramified[1], i.e. for

[1] This notion is due to Serre. A hint concerning its representation-theoretical meaning is given in the next section.

$\mathfrak{p}|p$ we get the completion of $K_p$ with respect to $\mathfrak{p}$ by a Kummer extension over $\mathbb{Q}_p(\zeta_p)$ with a radical element (namely $j_E$) with $v_p(j_E) \equiv 0 \bmod p$.

The proposition tells us that the existence of a solution of Fermat's equation implies the existence of an elliptic curve over $\mathbb{Q}$ with very remarkable properties. In the next section we will state conjectures assuring that no such curves exist and hence implying Fermat's conjecture. But before doing this we will show that the "converse" of proposition 2 is true too:
Assume that $E/\mathbb{Q}$ is a stable elliptic curve with $\mathbb{Q}$-rational points of order 2. Assume moreover that $K_p$ is ramified over $\mathbb{Q}$ only in divisors of $2 \cdot p$, that $v_2(j_E) < 0$ and that $\mathrm{Min}(v_p(j_E),0) \equiv 0 \equiv v_2(j_E)-8 \bmod p$.
Let

$$N_E: Y^2 = X^3+AX^2+BX$$

be an equation for E with $A,B \in \mathbb{Z}$ and $\gcd(A,B) = 1$. The stability condition for E ensures that we always can find an equation of this type locally at the nonarchimedean completions of $\mathbb{Q}$ and since $\mathbb{Z}$ is a principal domain we find such an equation globally too.

The discriminant of $X^3+AX^2+BX$ is equal to $B^2(A^2-4B)$ and $B^2(A^2-4B)$ is a $2 \cdot p$-th power: $B^2(A^2-4B) = u^{2p}$ with $u \in \mathbb{Z}$. The greatest common divisor of B and $A^2-4B$ is equal to 1

hence there are elements $v,w \in \mathbb{Z}$ with $A^2-4B = v^{2p}$ and $B = w^p$. Hence:

$$(A-v^p)(A+v^p) = 4B = 4w^p .$$

It follows: There are elements $z_1,z_2 \in \mathbb{Z}$ with $z_1^p \cdot z_2^p = B$ and

$$2A = 2^\alpha z_1^p + 2^\beta z_2^p \quad \text{with } 0 \leq \alpha,\ \beta \leq 2 \text{ and } \alpha+\beta = 2$$

and

$$2v^p = 2^\alpha z_1^p - 2^\beta z_2^p .$$

Now assume that, say, $\alpha = 0$. Then $2 \mid z_1$ and it would follow that $2 \mid B$ and $2 \mid A$.

Hence $\alpha = \beta = 1$. As a consequence we get:

$(z_1,z_2,v)$ is a solution of Fermat's equation.

Let us state all those results in form of the

THEOREM. For a prime $p \geq 5$ the following three conditions are equivalent:

1. There exists a solution of Fermat's equation:
   $z_1^p - z_2^p = z_3^p$.
2. There exists a stable elliptic curve E over $\mathbb{Q}$ such that
   i) the points of order two of E are $\mathbb{Q}$-rational,
   ii) the field $K_p$ obtained by adjoining the coordinates of the points of order p to $\mathbb{Q}$ is unramified outside $2 \cdot p$,

iii) $\mathrm{Min}(0,v_p(j_E)) \equiv 0 \equiv v_2(j_E)-8 \bmod p$.

3. There exists a stable elliptic curve E over $\mathbb{Q}$ with a minimal equation

$$Y^2+XY = X^3+\alpha X^2+\beta X \quad \text{with } \alpha,\beta \in \mathbb{Z}$$

and

$$2^8 \cdot \Delta_E \in \mathbb{Z}^{2p} .$$

REMARK. The so-called "first case" of Fermat's conjecture is that $p \nmid z_1 \cdot z_2 \cdot z_3$. Clearly this is equivalent to

$$p \nmid \Delta_E$$

for the corresponding curve.

## III. Conjectures

1. Modular elliptic curves. For $N \in \mathbb{N}$ let $X_o(N)$ be the modular curve parametrizing elliptic curves with cyclic isogenies of degree N.

$X_o(N)$ is defined over $\mathbb{Z}$, one gets a model over $\mathbb{C}$ in the following way: The group

$$\Gamma_o(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl(2,\mathbb{Z});\ c \equiv 0 \bmod N\}$$

operates on

$$\mathbb{H}^* := \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\} \cup \{i\cdot\infty,\ q \in \mathbb{Q}\}$$

in the usual way. Then $X_o(N) \otimes \mathbb{C}$ is equal to $\mathbb{H}^*/\Gamma_o(N)$ as

Riemann surface.

Modular forms of weight 2 and level N are holomorphic functions on $\mathbb{H}$ with the transformation rule

$$f(\tfrac{az+b}{cz+d}) = (cz+d)^2 f(z) \quad \text{for all } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_o(N)$$

and bounded growth in the cusps $\{i\cdot\infty,\ q \in \mathbb{Q}\}$.

It follows that f has a Fourier expansion in $i\cdot\infty$ with parameter $q = e^{2\pi i z}$:

$$f(z) = \sum_{i=0}^{\infty} a_i q^i \ .$$

We are interested in <u>cusp forms</u> which by definition have the property that $a_o = 0$. A cusp form is normalized if $a_1 = 1$. The reason for their interest is that cusp forms of weight 2 and level N correspond one-to-one to holomorphic differentials on $X_o(N)$:

If $\omega$ is a holomorphic differential then

$$\omega = f \frac{dq}{q} \quad \text{with } q = e^{2\pi i z}$$

and f a cusp form of weight 2 and level N.

Let $J_o(N)$ denote the Jacobian variety of $X_o(N)$.

For our purpose it is enough to assume that N is a <u>square free</u> integer. In this case it is a theorem of Ribet that

$$\mathrm{End}_{\mathbb{Q}}(J_o(N)) = \mathrm{End}_{\mathbb{C}}(J_o(N) \otimes \mathbb{C}) = \mathrm{End}(J_o(N)) \ .$$

Moreover there are well-known elements in $\mathrm{End}(J_o(N))$:

The Hecke operators $T_n$ ($n \in \mathbb{N}$; $\gcd(n,N) = 1$) and the Fricke involutions $w_n$ ($n|N$). Those endomorphisms generate a commutative algebra, the Hecke algebra $\mathbb{T}$, and again Ribet showed that $\mathbb{T} \otimes \mathbb{Q} = \mathrm{End}(J_o(N)) \otimes \mathbb{Q}$.

Since $X_o(N)$ is defined over $\mathbb{Z}$ all the objects mentioned above have a $\mathbb{Z}$-structure, e.g. a holomorphic differential $\omega|\mathbb{Z}$corresponds to a cusp form $\sum_{i=1}^{\infty} a_i q^i$ with $a_i \in \mathbb{Z}$. Moreover it makes sense to speak about cusp forms over $\mathbb{F}_p = \mathbb{Z}/p$ for primes p (cf. [3] for example, for definition (and complications)).

Now we return to elliptic curves.

DEFINITION. An elliptic curve E over $\mathbb{Q}$ is a modular elliptic curve of conductor N if E is a factor of $J_o(N)$ and if N is minimal.

It is a result of Carayol that for modular elliptic curves the "modular" conductor is equal to the "geometric" conductor.
Hence, if E is stable over $\mathbb{Q}$ then N is square free.

The projection from $J_o(N)$ to E induces a non trivial morphism

$$\varphi: X_o(N) \longrightarrow E$$

("modular parametrization").

Of course $\varphi$ is not unique. We define:

$\varphi$ is a strong parametrization (and E is a strong modular elliptic curve) if $\varphi$ cannot be factorized through a non trivial isogeny to E.

Assume now that

$$\varphi: X_o(N) \longrightarrow E$$

is a strong parametrization and that N is square free. Let $\omega$ be the Néron differential of E, i.e. take a minimal equation of E and take $\omega := \frac{dX}{2Y+\lambda X+\mu}$.

Then $\varphi^*\omega$ is a holomorphic differential on $X_o(N)$, hence

$$\varphi^*\omega = f \cdot \frac{dq}{q} \quad \text{with}$$

$$f(z) = \sum_{i=1}^{\infty} a_i q^i \,, \quad q = e^{2\pi i z} \,.$$

f is "the cusp form of weight 2 and level N" corresponding to E.

One knows (Mazur, Raynaud):

$$f(z) = c(q + \sum_{i=2}^{\infty} a_i q^i) \text{ with } a_i \in \mathbb{Z} \text{ and } c = 1 \text{ or } c = 4,$$

and f is an eigenfunction under the action of the Hecke algebra.

FACT (Eichler, Shimura). For primes $l \nmid N$ the coefficient $a_l$ is the eigenvalue of the Hecke operator $T_l$, and

$$a_l = 1+l- \# E^{(l)}(\mathbb{F}_l) .$$

One could have the feeling that modular elliptic curves are very exotic objects. But there is a famous conjecture saying just the contrary:

CONJECTURE TS (Taniyama-Shimura). Every elliptic curve over $\mathbb{Q}$ is a modular elliptic curve.

2. Serre's conjecture.[2] We want to introduce modular representations. For the purpose of this paper we say:

DEFINITION. A representation

$$\rho: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gl}_2(\mathbb{Z}/p)$$

is modular of level M and weight k, if

i) $\rho$ is irreducible, and

ii) there is a normalized modular form $\overline{g}$ with coefficients in $\mathbb{F}_p$ of level M and weight k that is an eigenform with respect to the Hecke algebra $\mathbb{T}$ with Fourier series $\overline{g} = \sum_{i=1}^{\infty} \overline{b}_i q^i$ such that for l a prime, $l \nmid p \cdot M$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with $\rho(\sigma)$ a Frobenius element modulo l we have

$$\mathrm{Trace}(\rho(\sigma)) = \overline{b}_l .$$

[2] I would like to thank Prof. Serre for a letter in which he formulated these conjectures.

Ramifications of representations. Again assume that

$$\rho: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Gl_2(\mathbb{Z}/p)$$

is a representation. $\rho$ is unramified in a prime $l$ if the fixed field of the kernel of $\rho$ is unramified over $\mathbb{Q}$ in all divisors of $l$.

We have to look at the special case $l = p$ more closely:

DEFINITION (Serre). $\rho$ is finite in $p$ if the representation $\rho$ can be prolonged to the representation of a group scheme of type $(p,p)$ over $\mathbb{Z}$ that is finite and flat in $p$.

Criterion. Let $K$ be the fixed field of the kernel of $\rho$ and $\mathfrak{p}$ a divisor of $p$, $K_{\mathfrak{p}}$ the completion of $K$ with respect to $\mathfrak{p}$, and $K_{\mathfrak{p}} = \mathbb{Q}_p(\zeta_p, \sqrt[p]{a})$ with $v_p(a) \equiv 0 \bmod p$ (i.e. $\rho$ is "moderately ramified" in $p$). Then $\rho$ is finite in $p$.

Now we can state Serre's conjectures about modular representations of weight 2:

CONJECTURE S. 1. Let $\rho$ be a modular representation of level $p \cdot M$ and weight 2, assume that $p \nmid M$ and that $\rho$ is finite in $p$. Then $\rho$ is a modular representation of level $M$ and weight 2.

2. Let $\rho$ be a modular representation of level $M_1 \cdot M_2$ and weight 2 with $\gcd(M_1, pM_2) = 1$. Assume that $\rho$ is unrami-

fied in all divisors of $M_1$. Then $\rho$ is a modular representation of level $M_2$ and of weight 2.

Now we return to Fermat's equation.

Assume that we have a solution $Z_1^p - Z_2^p = Z_3^p$ with corresponding elliptic curve E. Hence $p > 163$ and thanks to Mazur (cf. [4]) we know that the representation $\rho_E$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ induced by the action on the points of order p of E is irreducible.

Assume that E is a modular curve. Hence $\rho_E$ is modular of level N (square free) and weight 2, finite in p if $p|N$ and unramified outside $2 \cdot p$.

Hence the conjecture S implies: $\rho_E$ is modular of level 2 and weight 2. But $X_o(2)$ is of genus 0 so that there is no such representation; we get a contradiction.

RESULT. Conjectures TS and S imply Fermat's last theorem.

REMARKS. 1. The "first case" of Fermat's theorem is: $p \nmid z_1 z_2 z_3$. This case follows from TS and S 2. already.
2. Serre's conjecture can be applied to some other Ferma type equations too: Take the equation

$$a_1 Z_1^p - a_2 Z_2^p = a_3 Z_3^p$$

and

$$N' = 2. \prod_{\substack{1 \nmid 2 \\ v_1(a_1a_2a_3)>0}} 1 \quad .$$

Assume that the genus of $X_o(N')$ is equal to 0. Then TS and S imply that this equation has no non trivial solution.

3. One can formulate another version of S avoiding (or rather modifying the conjecture TS):

S': Let E be a stable elliptic curve over $\mathbb{Q}$ with conductor

$$N = \prod_{v_1(j_E)<0} 1 \text{ and } N' := \prod_{\text{Min}\{0,v_1(j_E)\}\not\equiv 0 \bmod p} 1$$

There is a normalized modular form

$$\overline{f} = \sum_{i=1}^{\infty} \overline{a}_i q^i$$

of level N' and weight 2 over $\mathbb{F}_p$ such that for almost all primes 1 the number $1+1-\#E^{(1)}$ reduced mod p is $\overline{a}_i$.

3. Conditions on the degree of the modular parametrization. We continue to assume that we have a solution of $Z_1^p - Z_2^p = Z_3^p$ and that E is the corresponding curve with discriminant $\Delta_E$ and conductor N.

At first we look at the inequality

$$2^8 . \Delta_E \geq N^{2p} \quad .$$

So for large p the discriminant of E is very large compared with the conductor of E.

This contradicts a conjecture of Szpiro:

SZ: There is a number c such that for all stable elliptic curves $\tilde{E}$ with conductor N we have $|\Delta_{\tilde{E}}| \leq N^c$. (Here again $\Delta_{\tilde{E}}$ is the discriminant of a "minimal" equation of $\tilde{E}$ which has stable reduction modulo all primes.)

We should mention that the conjecture of Szpiro is supported by an analogue result in the function field case, in this case c = 6 is enough as one sees by applying the Hurwitz genus formula.

Again it is clear that conjecture SZ implies Fermat's last theorem for large p.

A hint how one could possibly attack conjecture SZ if one assumes that E is parametrized by $X_o(N)$ is given by the following formula (cf. [10]):

Let $\varphi: X_o(N) \longrightarrow E$ be a non trivial morphism and f the corresponding modular form of weight 2 and level N. We choose our usual equation

$$N_E: Y^2 = X^3+(z_1^p+z_2^p)X^2+z_1^p z_2^p X$$

and then we get with $\mathbb{H} = \{\tau = u+iv \in \mathbb{C},\ v > 0\}$:

$$2^{\delta} \cdot \int_{\mathbb{H}/\Gamma_0(N)} |f(\tau)|^2 \, du \, dv = \frac{1}{4\pi^2} \cdot \deg(\varphi) \cdot \mathrm{Vol}(E)$$

where deg $\varphi$ is the degree of $\varphi$, Vol(E) is the area of a fundamental period parallelogram for the lattice $\Lambda$ corresponding to $N_E$ and $\delta$ is an integer $\geq 0$.
Hence there is a constant $k \in \mathbb{R}$ independent of N such that

$$\deg(\varphi) \geq k' \cdot \mathrm{Vol}(E)^{-1} .$$

Now $|j_E| < 1$ since $g_2 = z_1^{2p} + z_2^{2p} - z_1^p z_2^p$ is positive and so we find in [10] again

$$\mathrm{Vol}(E) \leq k'' \cdot \Delta_E^{-1/6} \quad \text{with}$$
$$k'' \in \mathbb{R} \text{ independent of } N ,$$

and hence:

$$\deg \varphi \geq k \cdot \Delta_E^{1/6} \geq k \cdot N^{2p} .$$

From this equation one sees that upper bounds for deg $\varphi$ give upper bounds for the discriminant of E, and hence we state

CONJECTURE D. There is a number $d \in \mathbb{N}$ with the following property: Let $\tilde{E}$ be a stable elliptic curve over $\mathbb{Q}$ with conductor N and a strong modular parametrization $\varphi$. Then there is a curve C and morphisms $\psi_1, \psi_2$ such that

$$X_o(N) \xrightarrow{\psi_1} C \xrightarrow{\psi_2} \tilde{E} \quad \text{with}$$

$$\psi_2 \circ \psi_1 = \varphi \text{ and } \deg(\psi_2) \leq N^d .$$

Conjecture D implies at once that $\deg(\varphi) \leq N^{d+1}$: Since $\tilde{E}$ is a strong modular elliptic curve the genus of C is larger than 1 and hence by the Hurwitz genus formula the degree of $\psi_1$ is bounded by the genus of $X_o(N) \leq N$.

Moreover the condition that $\tilde{E}$ has to be a strong modular elliptic curve can be removed easily: If $\tilde{E}$ is any stable elliptic curve with parametrization $\varphi$ then $\tilde{E}$ is isogenous over $\mathbb{Q}$ to a strong modular elliptic curve, and the degree of this isogeny can be bounded by 163 (cf. [4]). Hence conjecture D implies:

Assume that $\tilde{E}$ is a stable elliptic curve with conductor N and parametrization $\varphi'$: $X_o(N) \longrightarrow \tilde{E}$. Then there is a constant d independent of N and $\tilde{E}$ such that $\tilde{E}$ is parametrized by $\varphi$ with $\deg(\varphi) \leq N^d$.

The computation made above shows that then $N^d \geq k \cdot \Delta_{\tilde{E}}^{1/6}$ and hence conjecture SZ follows if we assume that the Taniyama-Shimura conjecture TS holds.

REMARKS. 1. It would be crucial to have an effective method to compute d, an estimate from below for d is 3/2 and can be found in [10]. So one could conjecture that $d = 3/2 + \varepsilon$ with $\varepsilon > 0$ suffices.

2. The conjectures SZ resp. (D+TS) have much stronger consequences for diophantine equations of Fermat type than the representation-theoretical conjecture S of Serre. For instance one would get from SZ or (D+TS): For fixed relatively prime integers $a_1, a_2, a_3$ and monotonous functions $\alpha_1, \alpha_2, \alpha_3$: $\mathbb{N} \longrightarrow \mathbb{N}$ there are only finitely many natural numbers n such that the equation

$$a_1 Z_1^{\alpha_1(n)} - a_2 Z_2^{\alpha_2(n)} = a_3 Z_3^{\alpha_3(n)}$$

has a solution $(z_1, z_2, z_3)$ with relatively prime integers with $|z_1 z_2 z_3| > 1$.

## IV. Congruence numbers

Serre's conjecture S states:

If $\rho$: $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gl}_2(\mathbb{Z}/p)$ is a modular representation of weight 2 and level M corresponding to a modular form f of minimal level M which is unramified in a prime $l \nmid p$ with $l \| M$ (resp. which is finite in p and again $p \| M$) then l (resp. p) can be "cancelled" in the level.

Hence a very weak form of this conjecture is:

There is a cusp form $g \neq f$ with

$$f \equiv g \bmod p$$

and so p is a congruence prime.

This shows that congruence primes are interesting in our context, and moreover it turns out that they are related to the degree of modular parametrizations too.

To be more precise we denote by $S(N)$ the $\mathbb{Z}$-module of cusp forms of weight 2 and level $N$ whose Fourier coefficients are in $\mathbb{Z}$, we assume that $f \in S(N)$ is an eigenfunction with respect to the Hecke algebra $T$ and define

$$L := \langle f \rangle^{\perp}$$

as the orthogonal complement of the span of $f$ with respect to the Petersson metric.

DEFINITION. $r :=$ largest number such that there is a $g \in L$ with $f \equiv g \bmod r$.
The prime divisors of $r$ are called congruence primes with respect to $f$.

Obviously there are other characterizations of $r$: $r$ is the exponent of the finite group $S(N)/(\mathbb{Z}f+L)$, or:

$$r^{-1}(f,f)\mathbb{Z} = \{(f,g);\ g \in S(N)\}$$

(here $(\ ,\ )$ is the Petersson scalar product).

Now assume that $N$ is square free and that $f$ belongs to a strong modular parametrization of an elliptic curve $E$ with map

$$\varphi: X_0(N) \longrightarrow E\ .$$

We follow the ideas in [10] to prove

PROPOSITION 3 (Hida). The degree of $\varphi$ divides r.

The proof is a copy of the proof given by Zagier in [10] so we can be very short:

First step: $\varphi$ induces a map $\varphi_*: J_0(N) \longrightarrow E$ with a dual map $\varphi^*: E \longrightarrow J_0(N)$ which is injective because $\varphi$ is assumed to be a strong parametrization, and $\varphi_* \circ \varphi^*$ is multiplication by $\deg \varphi =: n$.
Define $A := \ker(\varphi_*)$. Then A is a codimension 1 abelian subvariety of $J_0(N)$ and $A \cap \varphi^*(E)$ is a finite group which turns out to be equal to $E_n$ (points of order dividing n of E).

Second step: The isogeny $\beta: E \times A \longrightarrow J_0(N)$ given by $\beta(b,a) := \varphi^*(b)-a$ induces a splitting of

$$\mathrm{End}(J_0(N)) \otimes \mathbb{Q} = \mathrm{End}(E) \otimes \mathbb{Q} \oplus \mathrm{End}(A) \otimes \mathbb{Q} .$$

Let e correspond to (1,0) in this splitting. Then n is the denominator of e in $\mathrm{End}(J_0(N))$.

Third step: Since N is square free Ribet's theorem states that

$$\mathbb{T} \subset \mathrm{End}(J_0(N)) \quad \text{and}$$
$$\mathbb{T} \otimes \mathbb{Q} = \mathrm{End}(J_0(N)) \otimes \mathbb{Q} .$$

Let m be the denominator of e in $\mathbb{T}$. Then $n \mid m$.

On the other side Zagier uses the pairing

$$\langle\ ,\ \rangle\colon S(N) \times \mathbb{T} \longrightarrow \mathbb{Z}$$

which sends $(h,T_n)$ to the first Fourier coefficient of $T_n(h)$ to show that $m = r$, and hence $\deg \varphi \mid r$.

REMARK. Zagier shows more: For N a prime one has $\deg \varphi = r$. The crucial point is that due to Mazur in this case $\mathbb{T} = \mathrm{End}(J_o(N))$. So any description of $[J_o(N):\mathbb{T}]$ in the square free case would improve proposition 3.

We now assume that E is a stable modular elliptic curve with parametrizing map

$$\varphi\colon X_o(N) \longrightarrow E$$

where

$$N = \prod_{v_1(\Delta_E)>0} 1 \quad \text{and} \quad 2 \mid N\ .$$

Let

$$\varphi_*\colon J_o(N) \longrightarrow E$$

be the induced map and

$$\varphi^*\colon E \longrightarrow J_o(N)$$

the dual map, $E^* := \varphi^*(E) \subset J_o(N)$.

PROPOSITION 4. Let 1,p be odd primes with $p > 3$ and assume that $1^{p^k} \mid \Delta_E$ for $k \in \mathbb{N}$. Assume moreover that E (and

hence $E^*$) has no $\mathbb{Q}$-rational isogeny of degree p. Then $E^*_{p^k}$, the group of points of order dividing $p^k$ of $E^*(\overline{\mathbb{Q}})$, is in the kernel of $\varphi_*$.

Proof. We use the description of the Néron model $\tilde{J}_o(N)$ of $J_o(N)$ over $\mathbb{Z}$ due to Deligne-Rapoport and Mazur (see [3]): By assumption $l|N$. Up to elements of 2- or 3-power order the group of connected components of $\tilde{J}_o(N) \otimes \overline{\mathbb{F}}_l$ is generated by the image of the $\mathbb{Q}$-rational cusp divisor $c = (0)-(\infty)$.[3)]

It follows that connected components $C_i^o$ of the Néron model $\tilde{E}$ of $E^*$ modulo l with $p^k.C_i^o = C_o^o$, the connected component of the unit of $\tilde{E} \otimes \overline{\mathbb{F}}_l$, are contained in the connected component of $\tilde{J}_o(N) \otimes \overline{\mathbb{F}}_l$ for the norm map from $J_o(N)$ to $J_o(\frac{N}{2})$ maps $E^*$ to 0 and c to a divisor $\tilde{c}$ with $\text{order}(\tilde{c}) = \frac{\text{order}(c)}{3}$. Hence $\varphi_*(C_i^o)$ is contained in the connected component of the Néron model of E mod l.

Now let P be a point of order $p^k$ of E and let E' be the Néron model of E over $\mathbb{Q}(P)$ with respect to a divisor $\mathfrak{l}|l$ of $\mathbb{Q}(P)$. Since E has multiplicative reduction mod l we have a natural map of the components of $\tilde{E}$ mod l to the components of E' mod $\mathfrak{l}$, and since $p^k | \Delta_E$ P lies in a component $C_i^o$ of $\tilde{E} \otimes \overline{\mathbb{F}}_l$ with $p^k.C_i^o = C_o^o$. So $\varphi_*$ maps

3) In [3] the hypothesis is made that N is prime to 6. But by re-doing the calculations made in Mazur's paper one can get the cited result in the general case too.

P mod l into the connected component of E' mod l, hence by Tate's theory $\varphi_*(E^*_{p^k})$ is a cyclic group. Since $E^*$ has no $\mathbb{Q}$-rational cyclic isogeny of degree p it follows that $\varphi_*(E^*_{p^k}) = 0$.

Let E be as above and let f be the cusp form corresponding to $\varphi$.

COROLLARY. Under the assumptions of the proposition we get: There is a cusp form $g \in S(N)$ of weight 2 and level N with $f \neq g$ and $f \equiv g \bmod p^k$.

Proof. The corollary follows from proposition 3 and proposition 4 and the condition that E has no $\mathbb{Q}$-rational isogeny of degree p, and so replacing E by a strong modular elliptic curve does not change the divisibility of $\Delta_E$ by $l^{p^k}$.

REMARK. Proposition 4 is true for p = 2 if E belongs to A,B,C with A-B = C and none of the numbers A,B and C is a power of 2.

Proposition 4 gives a convenient tool to construct congruence primes. Take E corresponding to A-B = C as in II. and assume that $l^{p^k} | A \cdot B \cdot C$. Then $p^k$ is a congruence number.

Example. The equation $2^8 - 13 = 3^5$ leads to the elliptic curve

$$Y^2 = X^3+269X^2+2^8\cdot 13X$$

with conductor $78 = 2\cdot 3\cdot 13$. In the table of [5] it corresponds to the curve 78B. Our proposition states that 5 is a congruence prime, and indeed the cusp form g corresponding to the curve 26B of level 26 is congruent modulo 5 to the cusp form of 28A which is isogeneous to 78B. We note that 2 is no congruence prime.

For $l \nmid p$ we state a different version of proposition 4:

PROPOSITION 4'. Assume that $A^*$ is a simple abelian subvariety of $J_o(N)$ with corresponding factor $\varphi_*(A^*) = A$ and that $C^*$ resp. $C = \varphi_*(C^*)$ are subgroups of $A^*(\bar{\mathbb{Q}})_{p^k}$ resp. $A(\bar{\mathbb{Q}})_{p^k}$ with

i) $C^* \cong C \cong (\mathbb{Z}/p^k)^2$,

ii) $\mathbb{Q}(C^*) = \mathbb{Q}(C)$ is a Galois extension of $\mathbb{Q}$ with Galois group $Gl_2(\mathbb{Z}/p^k)$ which is unramified in divisors $l|l$, and

iii) the reduction of C mod l intersects with the connected component of the Néron model of A modulo l in a cyclic subgroup. Then $p^k$ is a congruence number for the cusp forms f belonging to A.[4)]

4) Due to Shimura's results the simple factors of $J_o(N)$ correspond to $G(\bar{\mathbb{Q}}/\mathbb{Q})$-conjugacy classes of cusp forms of weight 2 and level N. For the definition of congruence numbers for for non-rational cusp forms see [6] for example.

A consequence of proposition 4 is that (under the assumptions we made there) there are simple abelian subvarieties $A_1,\dots,A_k$ of $J_o(N)$ with $A_i \cap E^* \supset E_p^*$.
Let A be the hull of all such subvarieties, let $f_1,\dots,f_k$ be cusp forms belonging to $A_1,\dots,A_k$.

Assume that $f_i$ is of level N but not $\frac{N}{l}$. Then $A_i$ is in the kernel of the mapping from $J_o(N)$ to $J_o(\frac{N}{l})$ induced by the norm map from $X_o(N)$ to $X_o(\frac{N}{l})$. Again by Deligne-Rapoport we can conclude: The special fibre $A_i^o$ of the Néron model of $A_i$ modulo l is a finite extension of a torus.

Now we numerate $A_1,\dots,A_k$ in such a way that exactly $A_1,\dots,A_t$ belong to such forms.

PROPOSITION 5. We continue to assume that E is as in proposition 4. Assume that $l \not\equiv 1 \bmod p$. Then we have $t < k$.

Proof. Assume that $t = k$ and hence $A = [A_1,\dots,A_k]$ is an abelian variety in $J_o(N)$ such that the special fibre of its Néron model modulo l is of multiplicative type.

Let $B \subset J_o(N)$ be a complementary abelian subvariety. Then $K := B \cap A$ is a finite group scheme over $\mathbb{Q}$ with $K \cap E_p^* = \{0\}$ by assumption. Define

$$\psi: J_o(N) \longrightarrow J_o(N)/K = A/K \times B/K =: A' \times B' .$$

$\psi$ maps the connected component of $\tilde{J}_o(N)$ mod l to the connected component of A' x B' mod l, and hence the components $C_i^o$ of the Néron model of $E^*$ mod l with $p \cdot C_i^o = C_o^o$ are mapped into the connected component of the unity of A' mod l (cf. proof of prop. 4). Hence we have the following situation: There is an elliptic curve $E'/\mathbb{Q}$ isogeneous to E with $v_l(j_{E'}) \equiv 0 \bmod p$ which is a subvariety of an abelian variety A' having totally degenerated reduction of multiplicative type mod l, and $E'_p$ is contained in the connected component $A'^o$ of A' mod l, where l is a divisor of l in $K_p$.

There are an elliptic curve $\tilde{E}/\mathbb{Q}$ isogeneous to E with $v_l(j_{\tilde{E}}) \equiv 0 \bmod p$, an abelian variety B/Q and an isogeny $\alpha: \tilde{E} \times B \longrightarrow A'$ defined over Q with $\alpha(\tilde{E}) = E'$ and $\mathrm{Ker}(\alpha) \cap \tilde{E} = \{0\}$.

Now we use the fact that A' and $\tilde{E} \times B$ have totally degenerated reduction mod l: There is an unramified extension K of $\mathbb{Q}_l$ such that $A' \otimes K \cong G_m^d/\Gamma$ where $d = \dim(A')$ and $\Gamma$ is a lattice in $(K^*)^d$ uniquely determined by A' and $(\tilde{E} \times B) \otimes K \cong G_m/\langle q \rangle \times G_m^{d-1}/\Gamma_1$ with $\Gamma_1$ a lattice in $(K^*)^{d-1}$ and q the l-adic period of $\tilde{E}$; the isomorphisms are in the category of rigid analytic spaces. Since A' (resp. $\tilde{E}$ and B) are defined over $\mathbb{Q}_l$ we have for $\sigma \in G(K/\mathbb{Q}_l)$: $\sigma\Gamma = \Gamma$ (resp. $\sigma\Gamma_1 = \Gamma_1$) and hence $G_m^d/\Gamma$

(resp. $G_m/\langle q\rangle \times G_m^{d-1}/\Gamma_1$) are abelian varieties defined over $\mathbb{Q}_1$. The isogeny $\alpha\colon \tilde{E} \times B \longrightarrow A'$ induces an isogeny $\tilde{\alpha}$ of $G_m/\langle q\rangle \times G_m^{d-1}/\Gamma_1$ to $G_m^d/\Gamma$ which is rational over K. But $\tilde{\alpha}$ is induced by a mapping of the lattice $\langle q\rangle \times \Gamma_1$ to $\Gamma$ and hence is defined over $\mathbb{Q}_1$ already. To be more precise: For all finite overfields L of K we have analytic maps

$$\gamma_1\colon (\tilde{E} \times B)(L) \longrightarrow L^*/\langle q\rangle \times (L^*)^{d-1}/\Gamma_1 \text{ and}$$
$$\gamma_2\colon A'(L) \longrightarrow (L^*)^d/\Gamma$$
$$\text{with } \gamma_2 \circ \alpha = \tilde{\alpha} \circ \gamma_1 .$$

Now take $P \in \tilde{E}(K\cdot K_p)$ and $\sigma \in G(K_p\cdot K/\mathbb{Q}_1)$. Then we get

$$\gamma_2(\sigma(\alpha(P))) = \gamma_2(\alpha(\sigma P)) = \tilde{\alpha}(\gamma_1(\sigma P)) = \varepsilon(\sigma)\sigma(\tilde{\alpha}(\gamma_1(P)))$$

with

$$\varepsilon(\sigma) = \begin{cases} 1 \text{ if } \tilde{E} \text{ is a Tate curve over the fixed field of } \sigma \\ -1 \text{ else} \end{cases} .$$

Hence: $\gamma_2(\sigma(\alpha(P))) = \varepsilon(\sigma)\sigma(\gamma_2(\alpha(P)))$ or:
For points $Q \in E'_p$ and $\sigma \in G(K_p\cdot K/\mathbb{Q}_1)$ we have

$$\gamma_2(\sigma Q) = \varepsilon(\sigma)\sigma(\gamma_2(Q)) .$$

We know that $\gamma_2(Q)$ is contained in the connected component of the unity of $(K^*)^d/\Gamma$, hence it can be represented by a tuple $(\zeta_1,\ldots,\zeta_d) \neq (1,\ldots,1)$ of p-th roots of unity.

Assume at first that E' is a Tate curve over an extension $K_o$ of $\mathbb{Q}_l$ (of degree $\leq 2$) such that $K_o$ contains no primitive p-th root of unity. Then there is an element $\sigma \in G(K_p \cdot K/K_o)$ such that for all $Q \in E'_p$ we get: $\sigma(\gamma_2(Q)) \neq \gamma_2(Q)$. On the other side $\varepsilon(\sigma) = 1$ implies: $\sigma Q \neq Q$. But since $v_l(j_{E'}) \equiv 0 \bmod p$ there is a point $Q_o$ of order p in $E'_p$ which is invariant under $\sigma$, and we get a contradiction. Next assume that $l \equiv -1 \bmod p$ and that $E'/\mathbb{Q}_l$ is not a Tate curve. Take $\sigma$ as an extension of the generator of $G(\mathbb{Q}_l(\sqrt{\delta_{E'}})/\mathbb{Q}_l)$ where $\delta_{E'}$ is the Hasse invariant of E'. Then for all $Q \in E'_p$ we get:

$$\gamma_2(\sigma Q) = -\sigma(\gamma_2(Q)) = \gamma_2(Q)$$

since $\sigma(\zeta_i) = \zeta_i^{-1}$ for all p-th roots of unity. Hence $\sigma Q = Q$ for all $Q \in E'_p$, and this is false for all points Q which are not contained in the connected component of E' modulo l.

REMARK. The result of the proposition has also been obtained by B. Mazur even in a more general frame.[5)]

COROLLARY. Assume that E is a stable elliptic curve such that the representation $\rho_E$: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gl}_2(\mathbb{Z}/p)$ in-

5) I would like to thank J. Oesterlé and J.F. Mestre for telling me this.

duced by the action on $E_p$ is irreducible. Let N be the conductor of E and $\varphi: X_o(N) \longrightarrow E$ a modular parametrization. Assume that $2 \cdot l^p \mid \Delta_E$ and that $l \not\equiv 1 \bmod p$. Then $\rho_E$ is a modular representation of weight 2 and level $\frac{N}{l}$.

REMARKS. 1. Of course this corollary can be applied if $l = p$ and proves S1 for $\rho_E$. The technique described above can be used to prove S1 for more general representations too: Assume that the modular representation is induced by the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on a group C contained in the group of points of order p of a simple factor A of $J_o(N)$ with the following property: If $P \in C$ lies in the connected component $C_i$ of the Néron model of A over $\mathbb{Q}(C)$ modulo a divisor $\mathfrak{p}$ of p then $C_i$ corresponds to a connected component of the Néron model of A over $\mathbb{Q}_p$. This condition implies that the reduction of C is in the connected component of $\tilde{J}_o(N)$ modulo p, and hence one gets: If $\rho$ is moderately ramified in p then $\rho$ is modular of level $\frac{N}{p}$.

2. The same techniques can be used to prove: If $p^k$ is large compared with l (e.g. $p^k > l$) and if $2 \cdot l^{p^k} \mid \Delta_E$ then l can be cancelled in the level of $\rho_E$.

3. Using Weil's results about the eigenvalues of the Frobenius acting on the Tate module of abelian varieties one can get an estimation for deg $\varphi$. But Oesterlé and Mestre will produce a much better result:

$\deg \varphi < c \cdot 3^{N(1+\varepsilon)}$ in a forthcoming paper.[5)]

Of course our results are much too weak to help to prove Fermat's last theorem even under the assumption that TS holds. But nevertheless they support Serre's conjecture, and the procedure which relates solutions of diophantine equations of Fermat type to representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with well-known ramification should give interesting examples both for accessible algebraic number fields with Galois group $\mathrm{Gl}_2(\mathbb{Z}/p)$ and for modular forms and congruence numbers.

## REFERENCES


[1] S.I. BOREWICZ und I.R. SHAFAREVIČ, Zahlentheorie. Basel-Stuttgart 1966.

[2] G. FREY, Rationale Punkte auf Fermatkurven und getwistete Modulkurven. J. Reine Angew. Math. 331, (1982), 185-191.

[3] B. MAZUR, Modular curves and the Eisensteinideal. Publ. math. IHES (1977).

[4] B. MAZUR, Rational isogenies of prime degree. Invent. Math. 44, 1978, 129-162.

[5] Modular functions of one variable IV. Lecture Notes in Math. 476 (1972).

[6] K. RIBET, Mod p Hecke operators and congruences between modular forms. Invent. Math. 71, 1983, 193-205.

[7] P. ROQUETTE, Analytic theory of elliptic functions over local fields. Hamb. Math. Einzelschriften, Neue Folge, Heft 1, 1969.

[8] J.P. SERRE, Letter to Mestre, 1985.

[9] J. TATE, The arithmetic of elliptic curves. Invent. Math. 23, 1974, 176-206.

[10] D. ZAGIER, Modular parametrization of elliptic curves. Can. Math. Bull. 28, 1985, 372-384.

Gerhard Frey
Fachbereich 9 Mathematik
der Universität des Saarlandes

D-6600 Saarbrücken

(received 16.12.1985)