UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL ATOMIC ENERGY AGENCY
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.1004/6

SUMMER SCHOOL ON ELLIPTIC CURVES

(11- 29 August 1997)

Elliptic Curves with Isomorphic Galois Torsion Structure and Relations with Diophantine Equations

G. Frey
Institute for Experimental Mathematics
University of Essen
Ellernstrasse 29
D-45326 Essen
Germany

Elliptic Curves with Isomorphic Galois Torsion Structure and Relations with Diophantine Equations

(Extended Abstract)

Gerhard Frey
Institute for Experimental Mathematics
University of Essen
Ellernstraße 29
D-45326 Essen, Germany
e-mail: frey@exp-math.uni-essen.de

1 Diophantine conjectures

In this lecture K is either a number field or a function field in one variable over a perfect field K_0.
To simplify matters we make a general assumption: Every natural number which occurs is prime to $char(K)$.
The aim of the talk is to show that there is a close connection between certain ternary diophantine equations, the arithmetic of elliptic curves and the operation of the absolute Galois group G_K $(= Aut(K_{sep}/K)$ on torsion points of elliptic curves.

We have to fix some notation.
K has two important invariants. The genus $g(K)$ is the genus of the curve C corresponding to K if K is a function field, and equal to $-1/2 \log \mid \Delta_K \mid$ with Δ_K the discriminant of K if K is a number field.
The degree of irrationality $d(K)$ is the degree of K over $\mathbb{Q}$ if K is a number

field, and equal to the minimal degree of covering maps from C to the projective line if K is a function field.
Let Σ'_K be the set of places (= equivalence classes of rank-1 valuations of K over K_0 if K is a function field) and Σ_K the set of non archimedean places of K. For each $\mathfrak{p} \in \Sigma'_K$ we choose a valuation $v_\mathfrak{p}$ such that the product formula holds.

Example: If $K = \mathbb{Q}$ take $v_p(x) = -\log \mid x \mid$ for the archimedean place and $v_p(p) = \log(p)$ for prime numbers.

A divisor of K is a (finite) formal sum $D = \Sigma_{\mathfrak{p}\in\Sigma_K} z_\mathfrak{p}\mathfrak{p}$ with $z_\mathfrak{p} \in \mathbb{Z}$.
Let $\pi_\mathfrak{p}$ be a uniformizing element at $\mathfrak{p}$. Then $\deg D = \Sigma z_\mathfrak{p} \cdot v_\mathfrak{p}(\pi_\mathfrak{p})$ and $supp(D) = \Sigma_{z_\mathfrak{p}\neq 0}\,\mathfrak{p}$.
For $x \in K^*$ define its (projective) height by $h(x) := \Sigma_{\mathfrak{p}\in\Sigma'_K}(max(0\,, v_\mathfrak{p}(x)))$.

Example: If $K = \mathbb{Q}$ and $x = A/B$ with relatively prime integers A, B then $h(x) = log(max(\mid A \mid, \mid B \mid))$.

We are now ready to state a fundamental

Conjecture 1.1 *There are (effectively computable) constants c, $d \in \mathbb{R}$ depending only on $g(K)$ resp. $d(K)$ such that for all $x \in K$ with $x \cdot (x-1) \neq 0$ we have*

$$h(x) \leq c \cdot \deg supp(x(x-1)) \; + \; d$$

.

In the case that $K = \mathbb{Q}$ we take $x = A/B$ and so $x - 1 = C/B$ with $C = A - B$. Hence Conjecture 1.1 states that

$$max(\mid A \mid, \mid B \mid, \mid C \mid) \leq d \cdot (\Pi_{p\mid ABC}\; p)^c.$$

This is the ABC-conjecture stated by Masser and Oesterlé with a much more precise prediction of the constants: For every $\epsilon \in \mathbb{R}_{>0}$ the numbers $c = 1 + \epsilon$ and d depending only on ϵ should do the job. So we shall call Conjecture 1.1 the ABC-conjecture, too.

It is obvious that this conjecture has strong implications for ternary diophantine equations in which increasing exponents are involved. We shall give one:

Fix $a, b, c \in K^*$.
$L_{a,b,c}(n)(K) := \{(x, y, y) \in K^3;\ ax^n + by^n = cz^n\}/\sim$ where $\sim$ means projective equivalence.

Conjecture 1.2 *$\bigcup_{5 \leq n} L_{a,b,c}(n)(K)$ consists of triples of bounded projective height, hence if K is a number field or K_0 is finite we get a finite set.*

We call this conjecture the **Asymptotic Fermat Conjecture.**
It is easy to see that the ABC-conjecture together with Faltings' theorem about the finiteness of $K-$rational points on curves of genus at least 2 implies conjecture 1.2.

Now we relate the ABC-conjecture with the arithmetic of elliptic curves.
Let E be an elliptic curve over K with conductor N_E. Let $h(E)$ be its Faltings height. After a finite extension of K E becomes semi-stable and then $h(E)$ is essentially $h(j_E)$.

Conjecture 1.3 *There exist constants c_1, d_1 in $\mathbb{R}_{>0}$ depending only on $g(K)$ resp. $d(K)$ such that for all elliptic curves E/K with $K/K_0(j_E)$ separable if K is a function field we have*

$$h(E) \leq c_1 \cdot \deg N_E + d_1.$$

We call conjecture 1.3 *the height conjecture for elliptic curves.*

Remark 1.1 *Conjecture 1.3 is a stronger version of Szpiro's conjecture.*

Proposition 1.1 *Conjecture 1.3 implies conjecture 1.2 (with constant $c = 2c_1$).*

To prove proposition 1.1 we use the dictionary between solutions of $A - B = C$ and the elliptic curve $E_{A,B}$ given by the equation

$$Y^2 = X(X - A)(X - B).$$

Proposition 1.2 *If K is a function field over K_0 then conjecture 1.3 is true with constants $c_1 = 1/2$ and $d = g(K) - 1$.*

We shall give a very short proof of proposition 1.2 which uses only Hurwitz genus formula for separable covers of curves. This proof gives no idea how to attack conjecture 1.3 in the number field case. There is a more involved proof by Szpiro which uses the theory of algebraic surfaces and especially the inequality $c_1^2 \leq 3c_2$ for Chern classes of such surfaces. There is hope that one can find analogous inequalities for arithmetical surfaces. (According to a result of Kani and myself it would suffice to get this for surfaces whose generic fibre is a curve of genus 2.)

2 Conjectures about Galois representations

Before coming to elliptic curves we shall spend some lines to expose a general philosophy.
Assume that we have two simple non isogenous abelian varieties A_1 and A_2 over K and $K-$ isogenies λ_i from A_i into a third abelian variety A over K. Then $\lambda_1(A_1)$ has a finite intersection with $\lambda_2(A_2)$. How large can this set be or, in other words how complicated can the internal structure of A be?
To make this question more precise define:

Definition 2.1 *A finite K-subgroup scheme H of an abelian variety A/K is exceptional if*
i) there is no subgroup scheme $0 \neq H_1$ of H which is the kernel of an endomorphism of A and
ii)H is not contained in a proper abelian K-subvariety of A.

Let $h_{geom}(A)$ be the geometric Faltings height of A. Assume that all isogeny factors of A have multiplicity 1.

Question 1 *Are there numbers $N = N(K, dim A)$ and $M = M(K, dim A)$ such that $\mid H \mid > N$ implies that $h_{geom}(A) < M$?*

To give a flavour of the question we discuss special cases.

1.) Let K be a number field and fix d as well as a finite set S_0 of places of K. Look at abelian varieties over K of dimension d with good reduction outside of S_0. Then deep results of Faltings and Masser-Wüstholz imply that such numbers N, M exist and that they depend on $d, S_0, g(K)$ only.

2.) Take $d = 1$. Hence we look for exceptional subgroups of elliptic curves which have to be cyclic. So our question becomes

Conjecture 2.1 *There are numbers M, N such that for elliptic curves E over K with $K-$rational cyclic isogeny of degree $> N$ we have $h(j_E) < M$. Moreover N and M should depend only on $g(K)$ resp. $d(K)$.*

The local arithmetic of elliptic curves shows that conjecture 2.1 follows from the height conjecture for elliptic curves and hence it is true over function fields.
But this can be seen in a more elementary way: Each non constant point on the modular curve $X_0(n)$ which is $K-$rational induces an embedding of the function field of $X_0(n)$ into K over K_0 and hence $d(X_0(n)) \leq d(K)$ and $g(X_0(n)) \leq g(K)$, and since both $d(X_0(n)$ and $g(X_0(n))$ are of the size $O(n)$ the assertion follows.

Now we come to the special case to which the first part of the title of the lecture refers.

3.) Take $A = E_1 \times E_2$ where E_1 and E_2 are non isogenous elliptic curves over K. Assume that H is exceptional in A. After the discussion in **2.)** we can assume that H does not contain a Galois invariant cyclic subgroup and that it is isomorphic to $\mathbb{Z}/n \times \mathbb{Z}/n$ for $n \in \mathbb{N}$. Since it is not contained in E_i we get a G_K-isomorphism

$$\alpha : E_1[n] \to E_2[n]$$

such that H is the graph of α.
In other words: Let $\rho_{E_i,n}$ be the representation of G_K induced by its action on $E_i[n]$. Then $\rho_{E_1,n}$ is equivalent to $\rho_{E_2,n}$.

A question of Mazur in his IHES-paper on the Eisenstein ideal was whether such a thing could occur over $\mathbb{Q}$. Now there are many examples of pairs

of elliptic curves over $\mathbb{Q}$ with isomorphic representations found (by Kraus, Cremona, Müller,..) up to $n = 13(?)$.

I stated the

Conjecture 2.2 *Fix E_0/K. There is a number $N = N(g(K), E_0)$ resp. $N = N(d(K), E_0)$ such that for elliptic curves E/K and numbers $n > N$ with $\rho_{E_0,n} \sim \rho_{E,n}$ it follows that E is isogenous to E_0.*

Again conjecture 2.2 follows from the height conjecture for elliptic curves and hence is true in the function field case. So we see already a connection between representation theory and arithmetical properties of elliptic curves. But more is true:

Proposition 2.1 *Let K be a number field. Then conjecture 1.2 (the Asymptotic Fermat conjecture) implies conjecture 2.2 for even numbers n.*

The proof uses again the local arithmetic of elliptic curves and the dictionary between $A - B = C$ and $E_{A,B}$.

For fixed n the curve E with $\rho_{E,n} \sim \rho_{E_0,n}$ corresponds to a $K-$rational point on a twisted modular curve $X_{E_0}(n)$ and hence conjecture 2.2 is a conjecture about rational points on the union of such curves.
A much keener conjecture goes back to Darmon in the number field case and states:

Conjecture 2.3 *There are numbers $N = N(g(K)), M = M(g(K))$ resp. $N = N(d(K)), M = M(d(K))$ such that for all elliptic curves E_i over K with*
$\rho_{E_i,n} \sim \rho_{E_j,n}$ for some $n > N$ it follows that either E_i is isogenous to E_j or that the geometric Faltings height of both curves is bounded by M.

There is a modular interpretation for this conjecture. Let $X(n)$ be the modular curve corresponding to $\Gamma(n)$. Its group of automorphisms is equal to $PSl(2, \mathbb{Z}/n)$. Let

$$\alpha : E_1[n] \to E_2[n]$$

be a G_K-isomorphism. Then (E_1, E_2, α) gives rise to a $K-$rational point on

$$Z_{n,\epsilon} := (\alpha_\epsilon(PSl(2,\mathbb{Z}/n)) \setminus (X(n) \times X(n)$$

with a diagonal embedding

$$\alpha_\epsilon : PSl(2,\mathbb{Z}/n) \to (PSl(2,\mathbb{Z}/n))^2$$

induced by α with $\epsilon = det(\alpha)$.
$Z_{n,\epsilon}$ is a diagonal surface which was investigated recently by Kani, Schanz and Herrmann.

Result: For $n > 12$ the surface $Z_{n,\epsilon}$ is of general type. For $n \leq 12$ rational or $K3-$surfaces occur, for instance $Z_{7,\epsilon}$ is rational, and this explains why there are lots of numerical examples of elliptic curves with isomorphic Galois torsion structure for small n.

Now recall **Lang's conjecture**: If X is a surface of general type then the $K-$rational points have either small height (depending on K) or lie on curves of genus < 2 on X.
So assuming this conjecture the conjecture 2.3 is implied by the following conjecture stated by Kani:

Conjecture 2.4 *For $n > 22$ the only curves of genus < 2 on $Z_{n,\epsilon}$ are related to (twisted) Hecke correspondances and hence points on these curves correspond to pairs of isogenous elliptic curves and isomorphisms α induced by isogenies.*

An especially interesting case is $\epsilon = -1$. It leads to curves of genus 2 with elliptic differentials. I shall not go to details but refer to [Frey-Kani: Curves of genus 2 covering elliptic curves and a diophantine application, in Progr. Math.89,1991,153-175, resp. Frey: On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2, in Conf.on Elliptic Curves and Modular Forms, Hong Kong, IP 1995, 79-98].

To end we specialize to $K = \mathbb{Q}$.
We know already that the Asymptotic Fermat conjecture implies conjecture 2.2 for elliptic curves whose points of order 2 are $\mathbb{Q}-$rational.

Theorem 2.1 *Conjecture 1.2 is equivalent with conjecture 2.2 with even n and $E_0[2] \in E(\mathbb{Q})$.*
More precisely:
a) Fix E_0 . Assume that the asymptotic Fermat conjecture holdsover $\mathbb{Q}$. The set of all elliptic curves $E/\mathbb{Q}$ with $E[2] \in E(\mathbb{Q})$ and such that there is a number $n > 4$ with $\rho_{E_0,n} \sim \rho_{E,n}$ is finite.
b) Assume that conjecture 2.3 holds for all even n and for all elliptic curves E_0 whose conductor divides $2^\delta \cdot N$ with $\delta \leq 4$ and depending on N. Then the Asymtotic Fermat conjecture is true for all $a, b, c \in \mathbb{Z}$ with $supp(abc) \mid N$.

Remark 2.1 *If for given N (for instance $N = 1$) there is no elliptic curve with conductor dividing $2^\delta \cdot N$ then the Asymptotic Fermat conjecture is true for corresponding coefficients a, b, c.*