BSD Summer School, Paris, July 4 and 5, 2002

Bas Edixhoven

July 21, 2002

Parallel to these four lectures, there were four lectures by Joseph Oesterlé giving an introduction on abelian varieties and the statement of the Birch and Swinnerton-Dyer conjecture.

1 Modular parametrisations I (1 hour)

At this conference/Summer school, modular parametrisations (whatever they are) are used to study the arithmetic of elliptic curves, and, more generally, of abelian varieties of GL_2-type, over $\mathbb{Q}$. In particular, one does not ask too much *where* these modular parametrisations come from. Let me nevertheless say a few words about this.

elliptic curves over $\mathbb{Q}$	$E/\mathbb{Q}$	
Galois representations	$\varprojlim_n E(\overline{\mathbb{Q}})[l^n]$	
L-functions	$L(E,s)=\sum_{n\geq 1} a_n n^{-s}$	$(\Re(s)>3/2)$
modular forms	$f_E=\sum_{n\geq 1} a_n q^n$	(Wiles et al.)
elliptic curves	$\mathbb{Z}\otimes_{\mathbb{T}} J_0(N_E)\sim E$	(Eichler-Shimura-Faltings)

With all this, the morphism:

$$\begin{array}{ccccccc} X_0(N_E) & \longrightarrow & J_0(N_E) & \twoheadrightarrow & \mathbb{Z}\otimes_{\mathbb{T}} J_0(N_E) & \twoheadrightarrow & E \\ & & & & & & \\ P & \longmapsto & [P]-[\infty] & & & & \end{array}$$

is a modular parametrisation of E, unique up to sign if we ask the kernel of $\mathbb{Z}\otimes_{\mathbb{T}} J_0(N_E)\to E$ to be cyclic. The morphism from $X_0(N_E)$ to $\mathbb{Z}\otimes_{\mathbb{T}} J_0(N_E)$ is called a *strong* modular parametrisation.

In this lecture, I want to explain the construction of the strong modular parametrisation, first over $\mathbb{C}$, then over $\mathbb{Q}$.

For $N \geq 1$, we let $\Gamma_0(N)$ be the subgroup $\mathrm{SL}_2(\mathbb{Z})$ consisting of the elements $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \equiv 0$ modulo N. We recall that $\mathrm{GL}_2(\mathbb{C})$ acts on $\mathbb{P}^1(\mathbb{C})$, hence $\mathrm{GL}_2(\mathbb{R})$ on $\mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$, which is the same as $\mathbb{C} - \mathbb{R}$ and hence the union of the upper and lower half planes. Hence $\mathrm{GL}_2(\mathbb{R})^+$ acts on the upper half plane $\mathbb{H}$, hence its subgroup $\mathrm{SL}_2(\mathbb{Z})$ too. We let $Y_0(N)(\mathbb{C})$ be the quotient $\Gamma_0(N)\backslash\mathbb{H}$, as a complex analytic curve (which is *not* compact). We let $X_0(N)(\mathbb{C})$ be the union of $Y_0(N)(\mathbb{C})$ with the (finite) set $\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Z})$ of cusps. Then $X_0(N)(\mathbb{C})$ is a compact non-singular complex analytic curve, and we let $X_0(N)_{\mathbb{C}}$ be the corresponding complex algebraic projective curve (by GAGA).

As an example we mention the j-map from $\mathbb{H}$ to $\mathbb{C}$, sending τ to $1/q + 744 + 196884q + \cdots$ (with $q = \exp(2\pi i\tau)$) which identifies $\mathbb{C}$ with $Y_0(1)(\mathbb{C})$. It induces an isomorphism $X_0(N)_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. The ramification of $X_0(N)_{\mathbb{C}} \to X_0(1)_{\mathbb{C}}$ is not hard to compute, and leads to a formula for the genus of $X_0(N)_{\mathbb{C}}$.

The next item in our list of things to explain is the jacobian $J_0(N)(\mathbb{C})$ associated to $X_0(N)(\mathbb{C})$. We have:

$$J_0(N)(\mathbb{C}) := \mathrm{H}^0(X_0(N)_{\mathbb{C}}, \Omega^1)^{\vee}/\mathrm{H}_1(X_0(N)(\mathbb{C}), \mathbb{Z}),$$

where γ in $\mathrm{H}_1(X_0(N)(\mathbb{C}), \mathbb{Z})$ is sent to the map $\omega \mapsto \int_\gamma \omega$. This quotient is a complex torus, and even an abelian variety. The corresponding complex algebraic variety is denoted $J_0(N)_{\mathbb{C}}$.

We will refer to $\mathrm{H}^0(X_0(N)_{\mathbb{C}}, \Omega^1)$ as the *space of complex cusp forms of weight 2 on* $\Gamma_0(N)$, and denote it by $S(\Gamma_0(N), 2)_{\mathbb{C}}$ (in order to relate this with forms of other weights one needs the Kodaira-Spencer morphism). One can view $S(\Gamma_0(N), 2)_{\mathbb{C}}$ as a space of certain functions $\sum a_n q^n$ on $\mathbb{H}$: pullback via the morphism $\mathbb{H} \to X_0(N)(\mathbb{C})$ gives a map

$$\omega \mapsto \left(\sum_{n\geq 1} a_n(\omega) q^n\right) \frac{dq}{q},$$

which is called the q-expansion map at the standard cusp ∞.

This cusp ∞ is also used to define the following map:

$$X_0(N)(\mathbb{C}) \longrightarrow J_0(N)(\mathbb{C}), \qquad P \mapsto \left[\omega \mapsto \int_\infty^P \omega\right].$$

Now the Hecke algebra. It comes from the action of $\mathrm{GL}_2(\mathbb{Q})^+$ on $\mathbb{H}$. For Γ_1 and Γ_2 of finite index in $\mathrm{SL}_2(\mathbb{Z})$, and g in $\mathrm{GL}_2(\mathbb{Q})^+$, one has (with $\Gamma_3 := \Gamma_1 \cap g^{-1}\Gamma_2 g$):

$$\begin{tikzcd} \mathbb{H} \arrow[loop above, "\Gamma_1"] \arrow[loop left, "\Gamma_3"] \arrow[r, "g\cdot", "\sim"'] \arrow[d] \arrow[dr] & \mathbb{H} \arrow[loop above, "\Gamma_2"] \arrow[d] \\ \Gamma_1\backslash\mathbb{H} & \Gamma_2\backslash\mathbb{H} \end{tikzcd} \qquad \begin{tikzcd} & \Gamma_3\backslash\mathbb{H} \arrow[dl] \arrow[dr] & \\ \Gamma_1\backslash\mathbb{H} & & \Gamma_2\backslash\mathbb{H} \end{tikzcd} \qquad \begin{tikzcd} & X(\Gamma_3)_{\mathbb{C}} \arrow[dl, "s_g"'] \arrow[dr, "t_g"] & \\ X(\Gamma_1)_{\mathbb{C}} & & X(\Gamma_2)_{\mathbb{C}} \end{tikzcd}$$

The last of these three diagrams is refered to as the *Hecke correspondence* T_g. It induces maps, called *Hecke operators*:

$$\begin{aligned} T_g^*\colon \mathrm{H}^0(X(\Gamma_2)_{\mathbb{C}}, \Omega^1) &\longrightarrow \mathrm{H}^0(X(\Gamma_1)_{\mathbb{C}}, \Omega^1), \quad s_{g*} \circ t_g^* \\ T_{g,*}\colon J(\Gamma_1)_{\mathbb{C}} &\longrightarrow J(\Gamma_2)_{\mathbb{C}}, \quad t_{g*} \circ s_g^* \end{aligned}$$

A study of $\Gamma_0(N)\backslash \mathrm{GL}_2(\mathbb{Q})^+/\Gamma_0(N)$ leads to Hecke operators $T_n\colon J_0(N)_{\mathbb{C}} \to J_0(N)_{\mathbb{C}}$, for all $n \geq 1$. To describe these, it is convenient to use the moduli interpretation of $Y_0(N)(\mathbb{C})$: it is the set of isomorphism classes of pairs $(E/\mathbb{C}, G)$, with E a complex elliptic curve and $G \subset E(\mathbb{C})$ a cyclic subgroup of order N. To be precise, a point τ of $\mathbb{H}$ is sent to the pair $(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \mu_N)$. With this description, the correspondence T_n (say on the level of divisors) is given by:

$$T_n\colon [(E, G)] \mapsto \sum_H [(E/H, \overline{G})],$$

where H runs through the set of subgroups of order n of $E(\mathbb{C})$ (not necessarily cyclic) such that $H \cap G = \{0\}$, and $\overline{G}$ denotes the image of G under $E \mapsto E/H$. These correspondences T_n commute with each other, and satisfy the relations (as correspondences; no equivalence relation is necessary) encoded in the following equality of formal Dirichlet series:

$$\sum_{n \geq 1} T_n n^{-s} = \prod_{p \mid N} (1 - T_p p^{-s})^{-1} \prod_{p \nmid N} (1 - T_p p^{-s} + p^{1-2s})^{-1}.$$

In terms of q-expansion at ∞ one has the identities:

$$a_n(T_m(\omega)) = \sum_{\substack{d \mid (n,m) \\ (d,N)=1}} d\, a_{nm/d^2}(\omega).$$

We let $\mathbb{T}_N$ be the subring of $\mathrm{End}(J_0(N)_{\mathbb{C}})$ generated by the T_n. This ring $\mathbb{T}_N$ is called the *Hecke algebra* of level N; it is a commutative ring, free as $\mathbb{Z}$-module of rank $g(X_0(N)_{\mathbb{C}})$. In fact, if we define:

$$S(\Gamma_0(N), 2)_{\mathbb{Z}} := \{\omega \in S(\Gamma_0(N), 2)_{\mathbb{C}} \mid a_n(\omega) \in \mathbb{Z} \text{ for all } n\},$$

then:

$$\mathbb{T}_n \times S(\Gamma_0(N), 2)_{\mathbb{Z}} \longrightarrow \mathbb{Z}, \quad (t, \omega) \mapsto a_1(t\omega)$$

is a perfect pairing of $\mathbb{Z}$-modules, in the usual sense that each side is identified with the dual of the other.

Eigenforms. Suppose that ω in $\S(\Gamma_0(N), 2)_{\mathbb{C}}$ is a common eigenform for the T_n:

$$T_n\omega = \lambda_n\omega$$

for all n, with suitable λ_n in $\mathbb{C}$. Then one has:

$$a_n(\omega) = \lambda_n \, a_1(\omega)$$

for all n; hence an eigenform is determined by the eigenvalues and its first Fourier coefficient. An eigenform form ω is called *normalized* if $a_1(\omega) = 1$. We also note that the non-zero qcommon eigenspaces for $\mathbb{T}_N$ acting on $S(\Gamma_0(N), 2)_{\mathbb{C}}$ are one-dimensional (and generated by the normalized form that they contain). We note that for a normalized eigenform ω the subring $\mathbb{Z}[\{a_n(\omega)\}]$ of $\mathbb{C}$ is an order in a number field, as it is the image of $\mathbb{T}_N$ under a morphism of rings $\mathbb{T}_N \to \mathbb{C}$. We remark that $S(\Gamma_0(N), 2)_{\mathbb{C}}$ can be seen as the $\mathbb{C}$-vector space $\mathrm{Hom}(\mathbb{T}_N, \mathbb{C})$ of $\mathbb{Z}$-module morphisms from TT_N to $\mathbb{C}$, and that the eigenforms correspond exactly to the morphisms of rings.

A normalized eigenform ω in $S(\Gamma_0(N), 2)_{\mathbb{C}}$ is called a *newform* if its system of eigenvalues $a_p(\omega)$ for $p \nmid N$ does not occur in any $S(\Gamma_0(M), 2)_{\mathbb{C}}$ with M a proper divisor of N.

Let now ω be a newform of level N, and let O_ω be the subring $\mathbb{Z}[\{a_n(\omega)\}]$ of $\mathbb{C}$. Then we define:

$$A_\omega := O_\omega \otimes_{\mathbb{T}_N} J_0(N)_{\mathbb{C}} = J_0(N)_{\mathbb{C}} / I_\omega J_0(N)_{\mathbb{C}},$$

where I_ω is the kernel of the morphism of rings $\mathbb{T}_N \to \mathbb{C}$ corresponding to ω. (By definition, $I_\omega J_0(N)_{\mathbb{C}}$ is the smallest abelian subvariety of $J_0(N)_{\mathbb{C}}$ containing the images of all elements of I_ω.) The quotient $J_0(N)_{\mathbb{C}} \to A_\omega$ is called the *optimal quotient* associated to ω (or more precisely, to the Galois orbit of ω, as it depends only on I_ω). The reason to call it optimal is that its kernel is connected, which is equivalent to the condition that the dual morphism: $A_\omega^\vee \to JJ_0(N)_{\mathbb{C}}$ be injective. Yet another way equivalent condition for a quotient of complex abelian varieties $A \to B$ to be optimal is that the induced map $\mathrm{H}_1(A, \mathbb{Z}) \to \mathrm{H}_1(B, \mathbb{Z})$ be surjective.

Of course, A_ω is an elliptic curve if and only if $O_\omega = \mathbb{Z}$. More generally, the dimension of A_ω is that of the $\mathbb{Z}$-module O_ω. We remark that the theory of newforms by Atkin-Lehner gives a description of $J_0(N)_{\mathbb{C}}$ up to isogeny as product of A_ω's where ω runs through the set of newforms of level dividing N.

We note the following analytic description of A_ω:

$$A_\omega = \frac{S(\Gamma_0(N), 2)_{\mathbb{C}}^\vee / I_\omega S(\Gamma_0(N), 2)_{\mathbb{C}}^\vee}{\mathrm{H}_1(X_0(N)(\mathbb{C}), \mathbb{Z}) / I_\omega \mathrm{H}_1(X_0(N)(\mathbb{C}), \mathbb{Z})} = \frac{S(\Gamma_0(N), 2)_{\mathbb{C}}[I_\omega]^\vee}{\mathrm{H}_1(X_0(N)(\mathbb{C}), \mathbb{Z})},$$

and $S(\Gamma_0(N), 2)_{\mathbb{C}}[I_\omega]$ has as $\mathbb{C}$-basis the set of Galois conjugates of ω.

Now over $\mathbb{Q}$. Up to now, everything has been done over $\mathbb{C}$. We want to have everything over $\mathbb{Q}$. For that, we use the moduli interpretation. The complex curve $X_0(N)_{\mathbb{C}}$ has a natural model $X_0(N)_{\mathbb{Q}}$ over $\mathbb{Q}$, (i.e., a $\mathbb{Q}$-scheme that gives $X_0(N)_{\mathbb{C}}$ after base change from $\mathbb{Q}$ to $\mathbb{C}$), namely, the compactified coarse moduli scheme associated to the (contravariant) functor:

$$\Gamma_0(N) \colon \mathrm{Sch}/\mathbb{Q} \longrightarrow \mathrm{Sets}, \quad S \mapsto \{(E/S, G)\}/\cong,$$

where E/S is an elliptic curve over a $\mathbb{Q}$-scheme, and where G is a closed finite subgroup scheme of E locally free of rank N, such that for every geometric point x of S the group $G(x)$ is cyclic. This means: in the category of contravariant functors $\mathrm{Sch}/\mathbb{Q} \to \mathrm{Sets}$, the morphism $\Gamma_0(N) \to Y_0(N)_{\mathbb{Q}}$ is universal for morphisms to representable functors. Classically, one also demands the map $\Gamma_0(N)(\overline{\mathbb{Q}}) \to Y_0(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})$ to be bijective, but this is automatically true. We remark that for the congruence subgroups $\Gamma_1(N)$ with $N \geq 5$ the situation is much simpler: the corresponding functor (pairs $(E/S, i)$ with $i\colon \mu_{N,S} \hookrightarrow E$) is representable, say by $X_1(N)_{\mathbb{Q}}$.

It follows that we have a model over $\mathbb{Q}$ for $J_0(N)_{\mathbb{C}}$:

$$J_0(N)_{\mathbb{Q}} := \mathrm{Pic}^0_{X_0(N)_{\mathbb{Q}}/\mathbb{Q}}, \quad A_{\omega,\mathbb{Q}} := O_\omega \otimes_{\mathbb{T}_N} J_0(N)_{\mathbb{Q}}.$$

Galois representations. $V_{\omega,l} := \mathbb{Q} \otimes \varprojlim_n A_\omega(\overline{\mathbb{Q}})[l^n]$ is free of rank 2 over $\mathbb{Q}_l \otimes O_\omega$, hence this gives:

$$\rho_{\omega,l}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_l \otimes O_\omega).$$

For every $\sigma\colon O_\omega \to \mathbb{C}$ we get an L-function:

$$L_\sigma(\rho_{\omega,l}) := \prod_p \det\left(1 - p^{-s}\,\mathrm{Frob}_p\,|(V_{\omega,l})_{I_p}\right)^{-1},$$

where one chooses for each factor a prime number $l \neq p$ (the subscript I_p stands for "co-invariants for the inertia at p"). It is not so hard to show that:

$$L_\sigma(\rho_{\omega,l}) = \sum_{n\geq 1} \sigma(a_n(\omega))n^{-s},$$

because at the places where ρ_ω is much ramified, the Euler factor is trivial. In particular, one has:

$$L(A_{\omega,\mathbb{Q}}, s) = \prod_{\sigma\colon O_\omega \to \mathbb{C}} \sum_{n\geq 1} \sigma(a_n(\omega))n^{-s}.$$

It is a difficult theorem by Eichler-Shimura-Langlands-Deligne-Carayol (simplified by Nyssen) that $\rho_{\omega,l}|_{D_p}$ corresponds by a suitable normalized local Langlands correspondence to $\pi_{\omega,p}$, the Euler factor at p of the automorphic representation associated to ω ($\pi_{\omega,p}$ is a smooth irreducible representation of $\mathrm{GL}_2(\mathbb{Q}_p)$). In particular, local ε-factors match. A consequence of this is that the conductor of ρ_ω is N.

2 Modular parametrisations II (1 hour)

2.1 Strong parametrisations; Stevens's conjecture

Let $E/\mathbb{Q}$ be an elliptic curve, N its conductor. As E is modular, there exists a *unique* $E' \hookrightarrow J_0(N)_\mathbb{Q}$ with E' isogeneous to E. Equivalently, we have:

$$X_0(N)_\mathbb{Q} \longrightarrow J_0(N)_\mathbb{Q} \xrightarrow{\text{optimal}} E' \longrightarrow E,$$

where the last isogeny can be chosen such that its kernel is cyclic (and then it is unique up to sign).

Question: how to characterise E' in the isogeny class of E?

Answer: I don't know.

Example. There are three elliptic curves of conductor 11: $11A = X_1(11)_\mathbb{Q}$, covering $11B = X_0(11)_\mathbb{Q}$ (quotient for the action of $(\mathbb{Z}/11\mathbb{Z})^*/\{1,-1\}$), covering $11C$ (quotient by the cuspidal group). Among these three, $11A$ has the smallest Faltings height. Also note that the isogenies are of degree 5 and that their kernels are constant group schemes over $\mathbb{Q}$, so that they extend to etale morphisms between Néron models over $\mathbb{Z}$.

The main point of this section is to say that Glenn Stevens, in his article in Invent. math. 98 (1989) has formulated a better question. Instead of parametrising with the modular curves $X_0(N)$, one should seriously consider parametrisations by arbitrary modular curves, i.e., corresponding to arbitrary congruence subgroups. Stevens has shown that "stabilisation takes place at $\Gamma_1(N)$", so that it makes better sense to replace $X_0(N)_\mathbb{Q}$ by $X_1(N)_\mathbb{Q}$. We recall that in these lectures $X_1(N)_\mathbb{Q}$ classifies elliptic curves with embeddings of μ_N (i.e., not of $\mathbb{Z}/N\mathbb{Z}$); this is necessary for example for the cusp ∞ to be $\mathbb{Q}$-rational. In view of what follows, one is tempted to say that considering parametrisations by $X_0(N)_\mathbb{Q}$ is somehow an historical error.

Better question (Stevens): what is the unique E'' inside $J_1(N)_\mathbb{Q}$ isogeneous to E?

Conjectural answer (Stevens): E'' is the one with the smallest Faltings height in the isogeny class of E.

2.1.1 Theorem. (Stevens) *Each isogeny class of elliptic curves over $\mathbb{Q}$ contains a unique curve of smallest Faltings height, and that one admits étale isogenies to all others (one Néron models over $\mathbb{Z}$).*

Some explanation is in order here. Let $A/\mathbb{Q}$ be an abelian variety, and $A_\mathbb{Z}$ its Néron model over $\mathbb{Z}$. One puts:

$$\underline{\omega}_{A_\mathbb{Z}/\mathbb{Z}} := \bigwedge^{\dim(A)} 0^*\Omega^1_{A_\mathbb{Z}/\mathbb{Z}};$$

it is a free $\mathbb{Z}$-module of rank 1. Integration over $A(\mathbb{C})$ equips $\underline{\omega}_{A_\mathbb{Z}/\mathbb{Z}}$ with a hermitian metric, and one defines the Faltings height of A to be the Arakelov degree:

$$h(A) := \deg_{\mathrm{Ar}}(\underline{\omega}_{A_\mathbb{Z}/\mathbb{Z}}) = -\frac{1}{2}\log\left(\left(\frac{i}{2}\right)^d \int_{A(\mathbb{C})} \omega_1\overline{\omega_1}\cdots\omega_d\overline{\omega_d}\right),$$

where $(\omega_1, \ldots, \omega_d)$ is a $\mathbb{Z}$-basis of $0^*\Omega^1_{A_\mathbb{Z}/\mathbb{Z}}$. In words: the Faltings height of A is minus one half of the logarithm of the covolume of the period lattice of $A(\mathbb{C})$ with respect to a basis of Néron differentials.

For $E/\mathbb{Q}$ an elliptic curve, one has $0^*\Omega^1_{E_\mathbb{Z}/\mathbb{Z}} = \mathbb{Z}{\cdot}\omega_E$, with ω_E unique up to sign; these are called the Néron differentials of E. If $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ is a globally minimal Weierstrass equation for E, then:

$$\omega_E = \pm\frac{dx}{2y + a_1x}.$$

An isogeny $\phi\colon E \to E'$ of elliptic curves over $\mathbb{Q}$ is étale if $\phi^*\omega_{E'} = \pm\omega_E$.

2.1.2 Theorem. (Vatsal, preprint Febr. 2002) *If E is semistable, then Stevens's conjecture is true up to an isogeny of degree a power of 2.*

Let us mention the ingredients of his proof: geometric class field theory, a theorem of Ihara (that we recall in a moment), Heegner points of conductor p^n with $n \to \infty$, work of Rubin and Hida involving special values of L-functions.

Ihara's result alluded to is the following. For $N \geq 1$, we let Σ_N be the kernel of $J_0(N_\mathbb{Q}) \to J_1(N)_\mathbb{Q}$; it is called the *Shimura subgroup* of $J_0(N)_\mathbb{Q}$. Equivalently, the Cartier dual Σ_N^D is the Galois group of the largest unramified cover of $X_1(N)_\mathbb{Q}$ in $X_1(N)_\mathbb{Q} \to X_0(N)_\mathbb{Q}$ (which is Galois with group $(\mathbb{Z}/N\mathbb{Z})^*/1, -1)$. Then Ihara shows that the sequence (obtained by reducing modulo a prime p that does not divide N):

$$\mathbb{Z}[X_0(N)(\mathbb{F}_{p^2})^{\mathrm{s.s.}}]_0 \longrightarrow \mathrm{Pic}(X_0(N)_{\mathbb{F}_{p^2}}) \longrightarrow \Sigma_N^D \longrightarrow 0$$

is exact. The superscript "s.s." stands for "supersingular", and the subscript zero for the kernel of the sum map to $\mathbb{Z}$.

In the same preprint, Vatsal proves the following theorem, generalising work of Mazur for N prime (using very different methods).

2.1.3 Theorem. (Vatsal) *For N square free, $2^\infty\Sigma_N$ is the largest μ-type subgroup of $J_0(N)_\mathbb{Q}$.*

The recent results mentioned in this talk show perhaps that the use of L-functions (and especially p-adic ones) looks very promising.

2.2 Manin constants

Let $\phi\colon X_0(N)_{\mathbb{Q}} \to E$ be a *strong* modular parametrisation, $f_E\,dq/q$ the normalized newform on $X_0(N)_{\mathbb{Q}}$ corresponding to E, and ω_E a Néron differential on E. Then $\phi^*\omega_E = c_E{\cdot}f_E\,dq/q$ with c_e in $\mathbb{Q}^*$ (use multiplicity one). The number c_E, defined up to sign, is called the *Manin constant* of E. It is of interest for the Birch and Swinnerton-Dyer conjecture, because ω_E plays a rôle in it, but in practice one has to work with f_E, so that it is important to know the relation between the two. (This is especially so for optimal quotients of higher dimension.)

2.2.1 Conjecture. (Manin) $c_E = \pm 1$.

Question. What does this conjecture mean? Geometrically, say.

Answer. I don't know. The parametrisation ϕ being strong means that from the point of view of etale cohomology one has taken ϕ to be optimal (sujective on H_1, even with torsion coefficients). Then one would ask: is ϕ optimal for de Rham cohomology (over $\mathbb{Z}$)? But, first of all, it is not that easy to make sense out of this, because of bad reduction, and, secondly, the conjecture asks if $\phi^*\omega_E$ is a generator of $\Omega^1_{X_0(N)/\mathbb{Z}}$ at a given point, namely the cusp ∞. So even if one knows quite a lot about this conjecture, and that there seems little doubt that it is true, I claim not to understand what the conjecture really means. Anyway, the Stevens version of Manin's conjecture (same article as mentioned above) that we will state in a moment is a cleaner one, but suffers from the same problem.

2.2.2 Conjecture. (Stevens) Every *elliptic curve $E/\mathbb{Q}$ admits a parametrisation $\phi\colon X_1(N_E)_{\mathbb{Q}} \to E$ such that $\phi^*\omega_E = \pm f_E\,dq/q$.*

Let us mention the *results* about these conjectures obtained so far (in a non-chronological order).

1. For all parametrisations ϕ (of elliptic curves over $\mathbb{Q}$), by any $X_1(N)_{\mathbb{Q}}$ or $X_0(N)_{\mathbb{Q}}$, the corresponding Manin constant is in $\mathbb{Z}$. The proof of this just uses that the completion of the modular curves $X_0(N)_{\mathbb{Z}}$ and $X_1(N)_{\mathbb{Z}}$ over $\mathbb{Z}$ (defined by extending the moduli problems to arbitrary schemes) along the cusp ∞ correspond to $\mathbb{Z}[[q]]$, via the Tate curve, and that ϕ extends to a neighborhood of ∞ because to the Néron property of $E_{\mathbb{Z}}$. Proofs of this can be found Stevens's article and in an article by Edixhoven in the 1989 Texel proceedings.

   A nice consequence of this result is as follows. Let f be a newform in $S(\Gamma_0(N),2)_{\mathbb{Q}}$. Then one has the elliptic curve $\mathbb{C}$ moduly the period lattice of $f\,dq/q$. The standard Weierstrass equation of this elliptic curve (associated to the differential dz and the period lattice in $\mathbb{C}$) gives coefficients c_4 and c_6 that are in $\mathbb{Z}$. They correspond to the c_4 and c_6 of a minimal Weierstrass equation if and only if Manin's conjecture is true for the strong curve isogeneous to E. The same type of result is true for newforms in $S(\Gamma_1(N),2)_{\mathbb{Q}}$. In particular, this makes it possible first to compute the elliptic curve $\mathbb{Z} \otimes_{\mathbb{T}} X_0(N)$, and secondly to verify the conjecture about the Manin constant for that curve. All curves in Cremona's tables satisfy Manin's conjecture. Stevens also verified his version in some cases.

Now that we know that Manin constants are integers, the question becomes: what primes can divide them?

2. The two conjectures are related:

$$\begin{tikzcd}
J_1(N_E)_{\mathbb{Q}} & E' \arrow[l, hook'] \\
J_0(N_E)_{\mathbb{Q}} \arrow[u] & E \arrow[l, hook'] \arrow[u] \\
\Sigma_{N_E} \arrow[u, hook] & E \cap \Sigma_{N_E} \arrow[l, hook'] \arrow[u, hook]
\end{tikzcd}$$

   Now $(E \cap \Sigma_{N_E})^D$ is a constant group scheme over $\mathbb{Q}$, in E, and hence, by Mazur's work, of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ with $1 \leq n \leq 4$, or $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$. We conclude that the two conjectures on Manin constants are equivalent as far as primes numbers $p > 7$ are concerned.

3. Now consider a strong parametrisation $\phi \colon X_0(N_E)_{\mathbb{Q}} \to E$. Then we have the following results.

   (a) $p \nmid N_E$ implies that $p \nmid c_E$ (Mazur for $p > 2$, Abbes-Ullmo plus Raynaud for $p = 2$).

   (b) $p^2 \nmid N_E$ together with $p > 2$ imply that $p \nmid c_E$ (Mazur).

   (c) $2^2 \nmid N_E$ implies that $2^2 \nmid c_E$ (Raynaud, see Abbes-Ullmo).

   (d) $p > 7$ implies that $p \nmid c_E$ (Edixhoven (1992), details *still* not yet published (shame on me!)).

   The tools used for these results: geometry over $\mathbb{Z}_p$, plus everything else if necessary. The last result also uses that Stevens has shown that if his conjecture holds for E, then it also holds for twists of E over quadratic extensions of $\mathbb{Q}$ that are unramified at all p whose square divide N_E.

For example, let us prove, after Mazur, that $p^2 \nmid N_E$ together with $p > 2$ imply that $p \nmid c_E$. Then $J_0(N_E)_{\mathbb{Q}}$ has semistable reduction at p. We have an exact sequence:

$$0 \longrightarrow A \longrightarrow J_0(N_E)_{\mathbb{Q}} \longrightarrow E \longrightarrow 0,$$

which induces a complex of Néron models:

$$0 \longrightarrow A_{\mathbb{Z}_p} \longrightarrow J_0(N_E)_{\mathbb{Z}_p} \longrightarrow E_{\mathbb{Z}_p} \longrightarrow 0.$$

This complex is exact at all terms except possibly $E_{\mathbb{Z}_p}$. The induced complex on cotangent spaces:

$$0 \longleftarrow \mathrm{Cot}_0(A_{\mathbb{F}_p}) \longleftarrow \mathrm{Cot}_0(J_0(N_E)_{\mathbb{F}_p}) \longleftarrow \mathrm{Cot}_0(E_{\mathbb{F}_p}) \longleftarrow 0$$

is exact (this uses that $p > 2$ because of the usual condition "$e < p-1$"). It follows that $\phi^*\omega_E|_{E_{\mathbb{F}_p}}$ is not zero, etc.…

Other tools that are used.

1. More complicated geometry (pass to finite extensions of $\mathbb{Q}_p$ over which one has stable reduction).

2. Analytic tools: $\deg(\phi)\,\mathrm{Vol}(E(\mathbb{C}), \omega) = ||f_E||^2 c_E^2$, and:

   $$||f_E||^2 = C[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N_E)]\mathrm{Res}_2 \sum_{n\geq 1} |a_n(f_E)|^2 n^{-s}$$

   from an article by Zagier on degrees of modular paramatrisations, and:

   $$\frac{L(\mathrm{Sym}^2 E, 2)}{\pi i \Omega} = \frac{\deg(\phi)}{N c_E^2} \prod_{p^2|N} U_p(2)$$

   by Shimura (1976) (used by Flach, see recent work by Mark Watkins from Penn State for computational issues). The factor U_p reflects the difference between the two symmetric square L-functions that one may define: the usual one from the symmetric square of the l-adic representation, the other one (more naively) purely in terms of the local factors of $L(E, s)$.

It is interesting to note that the Euler factors at p of $L(\mathrm{Sym}^2 E, 2)$ gets a geometrical interpretation using reduction mod p: the factors p are powers of Frobenius, etc.

3 Non-triviality of Heegner points I; André-Oort conjecture (1 hour)

Let $E/\mathbb{C}$ be an elliptic curve. Then $\mathrm{End}(E) = \mathbb{Z}$ or $\mathrm{End}(E) \cong O_{K,c} = \mathbb{Z} + cO_K$ ($c \geq 1$) with $\mathbb{Q} \to K$ an imaginary quadratic extension. In the second case we say that E has no *complex multiplications (CM), by the order $O_{K,c}$ of conductor c*. Just to show that there are many (but only countably) elliptic curves with CM: for τ in $\mathbb{H}$, $\mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$ has CM if and only if $\mathbb{Q} \to \mathbb{Q}(\tau)$ is a quadratic extension.

3.1 Galois action

CM elliptic curves are defined over $\overline{\mathbb{Q}}$, for the simple reason that if $E/\mathbb{C}$ has CM, then for every automorphism σ of $\mathbb{C}$, the conjugate E^σ has CM, and we have just seen that there are only countably many.

Let $K \subset \overline{\mathbb{Q}}$ quadratic imaginary, and $c \geq 1$. Then we define a set:

$$S_{K,c} := \{(E/\overline{\mathbb{Q}}, \alpha) \mid \alpha\colon O_{K,c} \xrightarrow{\sim} \mathrm{End}(E) \text{ inducing } K \to \overline{\mathbb{Q}} \text{ via } \mathrm{Lie}(E)\}$$

The group $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on $S_{K,c}$. But also the group $\mathrm{Pic}(O_{K,c})$:

$$(L, E) \mapsto L \otimes_{O_{K,c}} E,$$

where $L \otimes_{O_{K,c}} E$ is the representable functor on K-schemes that sends a K-scheme S to $L \otimes_{O_{K,c}} E(S)$. Indeed, one can realise L as the kernel of an idempotent p in $\mathrm{M}_2(O_{K,c})$ (choose two generators of L, and a splitting of $O_{K,c}^2 \to L$), which shows that $L \otimes_{O_{K,c}} E$ is the same as $\ker(p\colon E^2 \to E^2)$. For $E = \mathbb{C}/\Lambda$ and $\alpha\colon O_{K,c} \xrightarrow{\sim} \mathrm{End}(E)$, one sees that Λ is an invertible $O_{K,c}$-module (use that $O_{K,c}$ is of the form $\mathbb{Z}[x]/(g)$, hence is Gorenstein). This implies the following important fact:

> $S_{K,c}$ is a $\mathrm{Pic}(O_{K,c})$-torsor.

The actions of $\mathrm{Pic}(O_{K,c})$ and G_K commute, which means that G_K acts on $S_{K,c}$ as $\mathrm{Pic}(O_{K,c})$-torsor. But, as $\mathrm{Pic}(O_{K,c})$ is commutative, the automorphism group of a $\mathrm{Pic}(O_{K,c})$-torsor is just $\mathrm{Pic}(O_{K,c})$ itself (it acts by right-translations, after one identifies $S_{K,c}$ with $\mathrm{Pic}(O_{K,c})$). It follows that G_K acts on $S_{K,c}$ via a morphism $G_K \to \mathrm{Pic}(O_{K,c})$. The main result of complex multiplication theory for elliptic curves says:

> G_K acts on $S_{K,c}$ via a morphism $G_K \to \mathrm{Pic}(O_{K,c})$; this morphism is unramified outside c; for $m \subset O_K$ a maximal ideal not containing m, the morphism sends Frob_m to the class $[m]^{-1}$ of $\mathrm{Pic}(O_{K,c})$.

In order to formulate the conjecture of André-Oort in the context of elliptic curves, we need to define (or rather make explicit) the notion of special subvariety of products of modular curves.

3.2 Definition. Let $n \geq 0$, and Γ_i ($1 \leq i \leq n$) be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Let $X_i := \Gamma_i \backslash \mathbb{H}$ be the (affine) complex modular curve associated to Γ_i, and $X := \prod_i X_i$. Let $Z \subset X$ be a closed irreducible subvariety of X. Then Z is called *special* if there exists a partition of $\{1, \ldots, n\}$ into subsets $S_1, \ldots, S_r$ such that $Z = \prod_{1 \leq j \leq r} Z_j$ with each $Z_j \subset \prod_{i \in S_j} X_i$ of one of the forms:

1. $|S_j| = 1$ and Z_i is a CM-point;

2. the image of $\mathbb{H} \to \prod_{i\in S_j} X_i$ under $\tau \mapsto (i \mapsto [g_i{\cdot}\tau])$ for certain g_i in $\mathrm{GL}_2(\mathbb{Q})^+$.

3.3 Conjecture. (Special case of André-Oort) *Let Σ be a set of CM-points in X (notation as above). Then all irreducible components of the Zariski closure of Σ are special.*

3.4 Theorem. *The conjecture is true, if one accepts the generalised Riemann hypothesis for imaginary quadratic fields (Edixhoven, 1999, not yet published). For $n = 2$ is has been proved unconditionally by Yves André (Crelle), and conditionally by Edixhoven (published! (Compositio)).*

We remark that Florian Breuer has proven analogous statements for rank two Drinfel'd modules (see his thesis). For the next lecture we want to give a relatively simple proof of the following weaker version.

3.5 Theorem. *Let K be imaginary quadratic, and $c \geq 1$. Let $\Sigma \subset X$ be a set of CM-points such that for every x in Σ, and for every i, one has $\mathrm{End}(E_{x_i}) = \mathbb{Z} + c_{x,i}O_K$ with $c_{x,i}|c^\infty$. Then all irreducible components of Σ^{Zar} are special.*

This case follows from a much more general result by Ben Moonen (Compositio, 1998), but in this simpler case we can give a much simpler proof. Actually, my intention was to adapt Moonen's proof for this lecture, but it still stays quite technical in this situation (and one has to consider base changes from the p-adic numbers to the complex numbers, for instance, with all kinds of different notions of convergence).

Proof. Let Z be an irreducible component of Σ^{Zar}. We replace Σ by $\Sigma \cap Z$. Consider the projections $\mathrm{pr}_i\colon X \to X_i$. If $\mathrm{pr}_i Z$ is a point, then it is a CM-point, and we can replace X by the product of the X_j with $j \neq i$. So we may (and do) assume that all pr_i are dominant. Suppose now that $i \neq j$ and $\mathrm{pr}_{i,j}\colon Z \to X_i \times X_j$ is not dominant. Then, admitting the theorem for $n = 2$ for the moment, the closure of $\mathrm{pr}_{i,j}Z$ is the graph of a Hecke correspondence in $X_i \times X_j$, call it T, itself of the form $\Gamma\backslash\mathbb{H}$ for some Γ. So we can replace the factor $X_i \times X_j$ by T. So we may (and do) assume that all $\mathrm{pr}_{i,j}$ (with $i \neq j$) are dominant, and we have to prove that $Z = X$.

Now consider the map $X \to \mathbb{C}^n$, where we view $\mathbb{C}$ as $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. We must show that the image of Z is $\mathbb{C}^n$, so we replace Σ by its image in $\mathbb{C}^n$, and must show that $Z = \mathbb{C}^n$.

We use induction on n: we may suppose that all $\mathrm{pr}_I\colon \mathbb{C}^n \to \mathbb{C}^{n-1}$ are dominant. As Σ consists of $\overline{\mathbb{Q}}$-points, Z is defined over $\overline{\mathbb{Q}}$, hence over a finite extension F of $\mathbb{Q}$. Take l a prime number such that $l \geq 13$, $l \geq \deg(\mathrm{pr}_I)$ for all I, l split in $O_{K,c}$ and in F.

3.5.1 Lemma. $T_l Z \subset Z$.

Proof. For all x in Σ, and for all σ in G_F, we have $\sigma(x) \in Z$. Now take $\sigma = \mathrm{Frob}_m$, with m a maximal ideal of O_F containing l. Then we see: $\sigma(x) \in T_l x$, hence $\sigma(x) \in T_l Z$, hence $x \in T_l Z$. $\square$

3.5.2 Lemma. *$T_l Z$ is absolutely irreducible if $n \geq 3$.*

Proof. We work over $\mathbb{C}$. Let Γ_l be the kernel of the (surjective) morphism of groups $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_l)$, and let X denote $\Gamma_l \backslash \mathbb{H}$. Then $X \to \mathbb{C}$ is Galois, with group $\mathrm{SL}_2(\mathbb{F}_l)/\{1, -1\}$. We consider the following diagram:

$$\begin{tikzcd}
X^n \arrow[loop above, "G^n"] \arrow[d, "\pi_n"'] \arrow[dr, phantom, "\square"] & \pi_n^{-1} Z \arrow[l, hook'] \arrow[loop above, "G^n"] \arrow[d] \\
\mathbb{C}^n & Z \arrow[l, hook']
\end{tikzcd}$$

As $T_l Z$ is an image of $\pi_n^{-1} Z$, it suffices to show that $\pi_n^{-1} Z$ is irreducible. Let V be an irreducible component of $\pi_n^{-1} Z$, and H its stabilizer in G^n. All that we have to show is that $H = G^n$. Now consider:

$$\begin{tikzcd}
V \arrow[loop above, "H"] \arrow[r, hook] & \pi_n^{-1} Z \arrow[loop above, "G^n"] \arrow[r, hook] \arrow[d] & X^n \arrow[loop above, "G^n"] \arrow[r, "\mathrm{pr}_I"] \arrow[d] & X^{n-1} \arrow[loop above, "G^{n-1}"] \arrow[d] \\
 & Z \arrow[r, hook] & \mathbb{C}^n \arrow[r, "\mathrm{pr}_I"] & \mathbb{C}^{n-1}
\end{tikzcd}
\qquad
\begin{tikzcd}
P_I \arrow[loop above, "G^{n-1}"] \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & X^{n-1} \arrow[loop above, "G^{n-1}"] \arrow[d] \\
Z \arrow[r] & \mathbb{C}^{n-1}
\end{tikzcd}$$

Because of the hypotheses $l \geq \deg(\mathrm{pr}_I)$ and $l \geq 13$ the fibered product P_I is irreducible. It follows that the projection $V \to P_I$ is dominant, hence that $\mathrm{pr}_I H = G^{n-1}$. The next wel known lemma (proof left as exercise) finishes the proof of the lemma. $\square$

3.5.3 Lemma. (Kolchin?) *Let G be a non-commutative simple group, $n \geq 2$, $H \subset G^n$ a subgroup such that $\mathrm{pr}_I H = G^2$ for all $I \subset \{1, \ldots, n\}$ with $|I| = 2$. Then $H = G^n$.*

So we have:

$$Z = T_l Z.$$

But all T_l-orbits in $\mathbb{C}^n$ are dense (even for the archimedian topology): the subgroup of $\mathrm{GL}_2(\mathbb{Z}[1/l])$ generated by $\mathrm{SL}_2(\mathbb{Z})$ and $\left(\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right)$ contains $\mathrm{SL}_2(\mathbb{Z}[1/l])$, and this last group is dense in $\mathrm{SL}_2(\mathbb{R})$ (as SL_2 is generated by additive groups).

It only remains to prove the theorem for $n = 2$. The reader is refered to my article in Compositio Math. 114 (1998) for that. $\square$

4 Non-triviality of Heegner points II (1 hour)

Reference: C. Cornut, “Non-trivialité des points de Heegner”, CRAS, 2002.

Let $E/\mathbb{Q}$ be an elliptic curve, N its conductor, $\pi\colon X_0(N)_{\mathbb{Q}} \to E$ a modular parametrisation, $\mathbb{Q} \to K$ a quadratic extension such that O_K/NO_K is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$ (as rings), $\mathcal{N} \subset O_K$ an ideal such that $\mathcal{O}_K/\mathcal{N} = \mathbb{Z}/N\mathbb{Z}$. We note that there are 2^r choices for $\mathcal{N}$ if N is composed of r distinct primes. For $c \geq 1$ we put:

$$\mathcal{N}_c := \mathcal{N} \cap O_{K,c}, \quad x_c := [\mathbb{C}/O_K \to \mathbb{C}/\mathcal{N}_c] \in X_0(N)(\mathbb{C}).$$

The point x_c is called a *Heegner point of conductor c*. In fact, x_c is in $X_0(N)(K[c])$, where $K \to K[c]$ is the abelian extension unramfied outside c that corresponds by class field theory to the quotient $\mathrm{Pic}(O_{K,c})$ of $(K \otimes \hat{\mathbb{Z}})^*$. As K is fixed in this talk, we drop it from the notation from now on. We are going to take a somewhat closer look at this group $\mathrm{Pic}(O_c)$.

The first thing we note is how to understand O_c “geometrically”:

$$\begin{tikzcd} O \arrow[r, two heads] & O/cO \,. \\ O_c \arrow[u, hook] \arrow[r, two heads] \arrow[ur, phantom, "\square"] & \mathbb{Z}/c\mathbb{Z} \arrow[u, hook] \end{tikzcd}$$

This means that $X_c := \mathrm{Spec}(O_c)$ is obtained from $X := \mathrm{Spec}(O)$ by “pinching” the closed subscheme O/cO into $\mathbb{Z}/c\mathbb{Z}$. Let f denote the morphism $X \to X_c$. Then we have a short exact sequence:

$$0 \longrightarrow \mathcal{O}_{X_c}^* \longrightarrow f_*\mathcal{O}_X^* \longrightarrow Q_c \longrightarrow 0,$$

with Q_c a skyscraper sheaf supported on $\mathbb{Z}/c\mathbb{Z}$. The long exact cohomology sequence reads:

$$0 \longrightarrow O_c^* \longrightarrow O^* \longrightarrow \frac{(O/cO)^*}{(\mathbb{Z}/c\mathbb{Z})^*} \longrightarrow \mathrm{Pic}(O_c) \longrightarrow \mathrm{Pic}(O) \longrightarrow 0.$$

Now we fix a prime number p that does not divide N, and we define $K[p^\infty] := \cup_{n\geq 0} K[p^n]$, and x_n will denote the previously defined x_{p^n}. We let $G := \mathrm{Gal}(Kp^\infty/K)$, and we have:

$$0 \longrightarrow \mathbb{Z}^* \longrightarrow O^* \longrightarrow \frac{(\mathbb{Z}_p \otimes O)^*}{\mathbb{Z}_p^*} \longrightarrow G \longrightarrow \mathrm{Pic}(O) \longrightarrow 0.$$

Using this, one sees that $\mathrm{Hom}(G, \mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_p$. It follows that there is a unique

$\mathbb{Z}_p$-extension:

$$\begin{tikzcd} K[p^\infty] & \\ & H_\infty \arrow[ul, "G_0 = G_{\mathrm{tors}}"'] \\ K \arrow[uu, "G"] \arrow[ur, "\cong \mathbb{Z}_p"'] & \end{tikzcd}$$

with G_0 a finite group.

4.1 Theorem. (Cornut) *For almost all $n \geq 0$ the Heegner point $\mathrm{trace}_{G_0}(\pi(x_n))$ in $E(H_\infty)$ is of infinite order.*

Before giving the proof, we want to mention that a previous proof was given, first in the case where $\mathbb{Q} \to K$ is ramified at only one prime by Vatsal, and in the general case by Cornut, using a theorem in ergodic theory by Marina Ratner. That tool has been replaced in this proof (following Cornut) by the special case of the conjecture of André and Oort of the previous talk. In any case, the proof uses some miraculous properties of the extension $K \to K[p^\infty]$: it has certain finite residue fields, the Galois group G has certain elements of order 2. These properties follow immediately from the description as inverse limit of the $\mathrm{Pic}(O_{p^n})$ that we have given above.

4.2 Lemma. *$E(H_\infty)_{\mathrm{tors}}$ is finite.*

Proof. For q prime, different from p and inert in K, $K \to K_{[}p^\infty]$ is completely decomposed at q: Frob_q in $\mathrm{Gal}(K[p^n]/K) = \mathrm{Pic}(O_{p^n})$ corresponds to the class of the ideal qO_{p^n}, hence is trivial. So we have morphisms $O_{p^\infty} \to \mathbb{F}_{q^2}$ for all such q. As prime-to-q torsion specializes injectively, and the image is in the finite group $E(\mathbb{F}_{q^2})$, it suffices to take two different q's. $\square$

To prove the thereom, it is enough to prove that the fibres of the following map f are finite:

$$X_0(N)^{G_0} \xrightarrow{\ \pi\ } E \xrightarrow{\ \ \Sigma\ \ } E$$

$$n \longmapsto (\sigma \mapsto \sigma(x_n)) \longmapsto \mathrm{trace}_{G_0}(\pi(x_n))$$

$$\mathbb{N} \xrightarrow{\qquad\qquad f \qquad\qquad} E(H_\infty)$$

Now the idea is to distinguish in G_0 the "geometric part" and the "chaotic part". Let $q_1, \ldots, q_g$ be the primes that are ramified in K, other than p, and let $Q_1, \ldots, Q_g$ be the maximal ideal of O_K over the q_i. Then Frob_{Q_i} has order 2 in G, because its image in each $\mathrm{Pic}(O_{K,p^n})$ corresponds to the class of Q_i, and we have $Q_i^2 = q_i O_{K,p^n}$. We let G_1 be the subgroup of G_0 that is generated by the Frob_{Q_i}. We have:

$$G \supset G_1 = \oplus_i \mathbb{F}_2 \cdot \mathrm{Frob}_{Q_i}\,.$$

This subgroup G_1 accounts for the "geometric part" of the action of G_0. We define:

$$N' := Nq_1 \cdots q_g, \quad \mathcal{N}' := \mathcal{N} Q_1 \cdots Q_g, \quad x'_n := [\mathbb{C}/O_{p^n} \to \mathbb{C}/\mathcal{N}'_{p^n}] \in X_0(N')(K[p^n]).$$

We note that N' is square free and prime to p.

For $1 \leq i \leq g$, we have the Atkin-Lehner involution W_{q_i} of $X_0(N')$; it sends (F,G,H) (with F an elliptic curve, G a subgroup of order q_i and H a cyclic subgroup of order N'/q_i) to $(F/G, F[q_i]/G, \overline{H})$. This gives 2^g degeneracy maps from $X_0(N')$ to $X_0(N)$, indexed by G_1. We let δ denote their product: $\delta\colon X_0(N') \to X_0(N)^{G_1}$. We define a new parametrisation $\pi'\colon X_0(N') \to E$ by:

$$\begin{array}{ccccccc} \pi'\colon X_0(N') & \xrightarrow{\delta} & X_0(N)^{G_1} & \xrightarrow{\pi} & E^{G_1} & \xrightarrow{\Sigma} & E \\ x'_n & \longmapsto & (\sigma \mapsto \sigma(x_n)) & & \longmapsto & & \mathrm{trace}_{G_1}(\pi(x_n)) \end{array}$$

We note that π' is dominant because its derivative at ∞ is non-zero (all degeneracy maps making up δ are ramified at ∞ except one)[1].

Let now R be a set of representatives for $G_1 \subset G_0$, and consider:

$$\begin{array}{ccccccc} & & X_0(N')^R & \xrightarrow{\pi'} & E^R & \xrightarrow{\sigma} & E \\ n & \longmapsto & H(n) := (\sigma \mapsto \sigma(x'_n)) & & \longmapsto & & \mathrm{trace}_{G_0}(\pi(x_n)) \end{array}$$

4.3 Proposition. *For $I \subset \mathbb{N}$ infinite, $H(I)$ is Zariski dense in $X_0(N')^R$.*

Of course, this proves that f has finite fibers, hence proves the theorem.

Proof. Because of the theorem of the previous lecture, if suffices to prve:

> Suppose σ_1, σ_2 are in G_0, $M \geq 1$, such that $(j(\sigma_1(x'_n)), j(\sigma_2(x'_n)))$ is in $X_0(M)$ for infinitely many n, then $\sigma_1^{-1}\sigma_2$ is in G_1.

[1] I thank Florian Breuer for pointing out to me that one has to verify that π' is not constant; the answer that I gave to his question during the lecture was nonsense

4.4 Lemma. *Let E_1 and E_2 have CM by K: $\mathrm{End}(E_i) = O_{c_i}$. Let $f\colon E_1 \to E_2$ be a cyclic isogeny, $d := \deg(f)$. Then f factors as follows:*

$$\begin{tikzcd} E_1 \arrow[r, "f"] \arrow[d, "f_1"'] & E_2 \\ O_{c'} \otimes_{O_{c_1}} E_1 \arrow[r, "f'"] & O_{c'} \otimes_{O_{c_2}} E_2 \arrow[u, "f_2^\vee"'] \end{tikzcd} \qquad c' = \frac{c_1}{\deg(f_1)} = \frac{c_2}{\deg(f_2)}, \qquad (c', \deg(f')) = 1.$$

Proof. The problem can be analyzed prime by prime, as it is a question about $\mathbb{Z}$-lattices in K. For every prime l, think of the tree of lattices up to $\mathbb{Q}_l^*$ in $V_l(E) \cong \mathbb{Q}_l \otimes K$, with E chosen such that $\mathrm{End}(E) = O$. To each lattice one associates the exponent of l in the conductor of the endomorphism ring. Then one gets the following pictures.

l **inert** There is one point with label 0, and the labels at all points are the distance to this one point.

l **split** The is a unique path, infinite in two directions, and the labels are the distance to this path.

l **ramified** There are two neighboring points such that the labels are the distance to these two points.

This shows that cyclic isogenies behave with respect to conductors of endomorphism rings as the lemma claims. $\square$

Now we finish the proof of the proposition. Suppose that σ_1, σ_2 and M are as in that proposition. Then we have infinitely many $f_n\colon E_n \to \sigma_1^{-1}\sigma_2 E_n$ of degree M, with $\mathrm{End}(E_n) = O_{p^n}$. The last lemma gives us infinitely many $f'_n\colon E'_n \to \sigma_1^{-1}\sigma_2 E'_n$ of fixed degree M' prime to p, with $\mathrm{End}(E'_n) = O_{p^{n-a}}$ (a fixed), and ideals $m_n \subset O$ of index M', such that:

$$\begin{tikzcd} E'_n \arrow[r] \arrow[dr, "\mathrm{can}"'] & \sigma_1^{-1}\sigma_2 E'_n \arrow[d, equal] \\ & (m_n \cap O_{p^{n-a}})^{-1} \otimes_{O_p^{n-a}} E'_n \end{tikzcd}$$

There are only finitely many possibilities for m_n, so we may assume that $m_n = m$, independent of n. Then in $G = \varprojlim_n \mathrm{Pic}(O_{p^n})$ we have:

$$[m] = \sigma_1\sigma_2^{-2} \in G_0 = G_{\mathrm{tors}}.$$

This means that for some $e \geq 1$ the intersection $m \cap O_{p^n}$ is principal for all $n \geq 0$. Some thinking gives that m is then of the form $Q_1^{e_1} \cdots Q_g^{e_g}$, hence that $\sigma_1\sigma_2^{-1}$ is in G_1, as we had to prove. $\square$