William - Here are some more details on my talk today Dick

On the local divisibility of Heegner points

The following problem on elliptic curves formed the motivation for this paper. Let E be an elliptic curve over $\mathbb{Q}$, of conductor N, whose L-function is non-zero at $s=1$. Then the group $E(\mathbb{Q})$ is finite. However, if K is any imaginary quadratic field where all primes dividing N are split, then the group $E(K)$ is expected to be infinite, of odd rank.

Let p be a prime which is inert in K, and let $E(p^2)$ be the finite group of points on $E \pmod{p}$ over the field of p^2 elements. What is the image of the reduction homomorphism $E(K) \to E(p^2)$?

~~[illegible]~~

We will address this question in a simple case, when the Heegner point P_K in $E(K)$ has infinite order. Kolyvagin has then studied the divisibility of P_K in the group $E(K)$. To study the image of $E(K)$ in $E(p^2)$, we will consider the divisibility of P_K in the local group $E(K_p)$.

We could also do experiments when $E(\mathbb{Q})$ has rank ≥ 2, so P_K is torsion.

1. We first recall the definition of Heegner points, adapted to the situation above. Fix a factorization of ideals: $(N) = n \cdot \bar{n}$ in K, with $\gcd(n, \bar{n}) = 1$. Let $\mathcal{O}_K$ denote the ring of integers of K, and consider the isogeny of tori: $\mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/n^{-1}$. This defines a

complex point x on $X_0(N)$. By the theory of complex multiplication, x is defined over the Hilbert class field H of K.

The Galois group of H is a semi-direct product: $\mathrm{Gal}(H/K) \rtimes \langle \tau \rangle$, where τ is any complex conjugation. Define the divisor E_K of degree zero on $X_0(N)$ by

$$E_K = \sum (x^{\sigma}) - \sum (x^{\sigma\tau})$$

Both sums are over σ in $\mathrm{Gal}(H/K)$. Then E_K is rational over K, and in the minus eigenspace for $\mathrm{Gal}(K/\mathbb{Q})$. Let e_K denote its class in the Jacobian $J_0(N)(K)^{-}$. If $\pi : J_0(N) \to E$ is a surjective homomorphism, we define $P_K = \pi(e_K)$. This is the Heegner point described above. It has infinite order when the L-function of E over K vanishes to order 1 at $s = 1$, and depends (up to sign) on the factorization of the ideal (N).

More generally, we will want to consider the divisibility of the class e_K in the Hecke modules $J_0(N)(K)^-$ and $J_0(N)(K_p)^-$.

2. We recall some results of Ribet on maximal ideals in the Hecke algebra, which will allow us to formulate our results. Let T denote the Hecke algebra of $X_0(N)$, acting on the space of cusp forms of weight 2. Then T is a commutative subring of $\mathrm{End}(J_0(N))$, generated

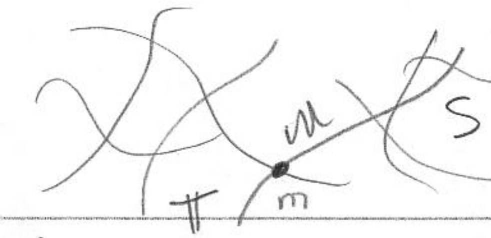
by the operators T_n, for all $n \geq 1$. Let $m \subset T$ be a maximal ideal, which satisfies

1) the ideal m has support in the finite T-module $J_0(N)(p^2)^-$, and has residual characteristic ℓ prime to $2Np$.

2) the kernel $V = J_0(N)[m]$ of multiplication by m on $J_0(N)$ over $\bar{\mathbb{Q}}$, which is isomorphic (by hypothesis 1)) to $(T/m)^2$, affords an irreducible representation of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, of Artin-Serre conductor N.

3) $p \not\equiv 1 \pmod{\ell}$, so the eigenvalues -1 and $-p$ of $Frob(p)$ on V are distinct.

In this situation, $J_0(N)(p^2)^- \otimes T_m$ is a cyclic, non-trivial T_m-module, and we will



determine when the Heegner ~~[illegible]~~ divisor e_K generates it

3. Ribet associates to the maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ a maximal ideal $\mathcal{M}$ of the p-new quotient S of the Hecke ring of $X_0(Np)$. The map $\mathbb{T} \to S/\mathcal{M}$, taking T_n to $T_n \pmod{\mathcal{M}}$ for all n prime to p, is well-defined, and induces an isomorphism of fields $\mathbb{T}/\mathfrak{m} \simeq S/\mathcal{M}$.

We may define the ideal $\mathcal{M}$ as follows. Let Y be the free $\mathbb{Z}$-module of divisors of degree 0 on the supersingular points of $X_0(Np)$ (mod p). Since Y is the character group of the maximal torus in the reduction of the Néron model of $J_0(Np)$ (mod p), the p-new Hecke algebra S acts on Y. This action is faithful; ~~[illegible]~~ in fact $Y \otimes \mathbb{Q}$ is a free $S \otimes \mathbb{Q}$-module of rank 1. We will define $\mathcal{M}$ as the annihilator of a certain finite quotient of Y.

The supersingular points on $X_0(Np)$ (mod p) can be identified with the supersingular points on $X_0(N)$ (mod p). They are all rational over the field of p^2 elements. Hence the divisor class map gives a group homomorphism

$$\mathrm{div} : Y \longrightarrow J_0(N)(p^2)$$

This is a map of S-modules, with T_n acting naturally for n prime to p, and U_p acting as $\mathrm{Frob}(p)$ on $J_0(N)(p^2)$.

Ihara determined the cokernel of the divisor class map, which is dual to the Shimura subgroup Σ_N. His results imply that the composition

$$Y \longrightarrow J_0(N)(p^2)^{-}/m$$

is surjective. This is the finite quotient of Y which is annihilated by $\mathcal{M}$.

Emerton has shown that the completion $Y_{\mathcal{M}} = Y \otimes S_{\mathcal{M}}$ is a free $S_{\mathcal{M}}$-module of rank 1. ~~This~~ His proof uses the cyclicity of the quotient $Y/\mathcal{M} = J_0(N)(p^2)^-/m$ as an $S/\mathcal{M} = T/m$-module. Since p is inert in K, the divisor $E_K \pmod p$ defines an element of Y. We will determine when $E_K \pmod p$ gives a basis for the free $S_\mathcal{M}$-module $Y_\mathcal{M}$.

4. We now recall Kolyvagin's results, on the global divisibility of e_K. These hold for any maximal ideal $m \subset T$ satisfying condition 2)

Logachev?

<u>Proposition 4.1</u> (Kolyvagin) The following conditions are all equivalent

a) the class e_K is not divisible by m in $J_0(N)(K)^- \otimes T_m$

b) the m-Selmer group $\mathrm{Sel}(J_0(N)/K, m)$ is isomorphic to T/m as a T-module, and is generated by the image of e_K

c) the T_m-module $J_0(N)(K)^- \otimes T_m$ is free of rank 1, with basis e_K, and the Tate-Shafarevic group of $J_0(N)$ over K has no m-torsion.

~~[illegible]~~

In fact, the three conditions of Proposition 4.1 <u>should</u> be equivalent to the simpler:

d) the m-Selmer group $Sel(J_0(N)/K, m)$ is isomorphic to T/m as a T-module

But, for the moment, this is out of reach.

5. Our results on the local divisibility of e_K take a similar form. First, we have the following localized version of Ihara's theorem

<u>Proposition 5.1</u> The following conditions are all equivalent

a) the class e_K is not divisible by m in $J_0(N)(K_p) \otimes T_m$

b) the class $e_K \pmod{p}$ is non-trivial in $J_0(N)(p^2)^- / m$

c) the divisor $E_K \pmod{p}$ is a basis for the free S_M-module Y_M.

Next, let $A \subset J_0(Np)$ be the p-new Abelian sub-variety, with $\dim A = \operatorname{rank} S = \operatorname{rank} Y$. The p-new Hecke ring S is a sub-ring of $\operatorname{End}(A)$, and the M-torsion on A can be identified with the T/m-module $V = J_0(N)[m]$ over $\bar{Q}$.

<u>Proposition</u> 5.2 The equivalent conditions of Prop 5.1 imply that the Selmer group $\operatorname{Sel}(A/K, M)$ is trivial.

We expect that the condition $\operatorname{Sel}(A/K, M) = 0$ is, in fact, <u>equivalent</u> to the fact that e_K is not divisible by m in $J_0(N)(K_p)^- \otimes T_m$. Again, this seems a bit out of reach.