Endomorphism algebras of semistable abelian varieties over **Q** of **GL**(2)-type

Kenneth A. Ribet

UC Berkeley

Tatefest
May 2, 2008

The “abelian varieties” in the title are now synonymous with certain types of modular forms. (This is true because we know the Serre conjecture, which was proved recently by Khare and Wintenberger.)

Specifically, we are interested in classical weight-2 newforms on congruence subgroups of $\mathbf{SL}(2, \mathbf{Z})$. These forms are required to be both cuspforms and eigenvectors for all Hecke operators T_n ($n \geq 1$).

Their novelty—the fact that they are *new*forms—means that they should belong essentially to the subgroup of $\mathbf{SL}(2, \mathbf{Z})$, and not to some proper group that contains it.

For the most part, we are concerned with forms on the group $\Gamma_0(N)$ where N is a square free positive integer. This subgroup consists of matrices in $\mathbf{SL}(2, \mathbf{Z})$ that are upper-triangular mod N.

In the language of abelian varieties, this means that we are limiting consideration to semistable abelian varieties whose endomorphism algebras (over $\mathbf{Q}$ and also over $\overline{\mathbf{Q}}$) are totally real fields that are as large as possible: their degrees are equal to the dimensions of the abelian varieties on which they operate.

A newform f of the type we are discussing may be written as a power series $\sum\limits_{n=1}^{\infty} a_n q^n$ where the a_n are algebraic integers in a totally real number field and where q is a shorthand for $e^{2\pi iz}$ where z is the variable in the complex upper-half plane. However, we are largely interested in this series as a formal object and are practically oblivious to the interpretation of q as the exponential of z.

It is an important fact that the subfield $K_f = \mathbf{Q}(\ldots, a_n, \ldots)$ of $\mathbf{C}$ is in fact a finite extension of the rational field $\mathbf{Q}$.

The degree $[K_f : \mathbf{Q}]$ is an interesting (albeit coarse) invariant of f. It is 1 if and only if the a_n are all rational integers, and this is true if and only if the associated abelian variety is an elliptic curve.

For example, suppose $N = 1001 = 7 \cdot 11 \cdot 13$. Looking at the relevant William Stein table, we find that there are exactly 14 newforms of weight 2 on $\Gamma_0(N)$. Here, we consider two newforms to be the same if they differ only by a Galois conjugation (replacement of all a_n by $\sigma(a_n)$, where σ is an element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$).

In increasing order, the degrees of the associated fields are 1, 1, 1, 2, 2, 3, 4, 4, 5, 5, 5, 7, 8, 11.

The question that we will consider is relatively simple minded: can the degree $\deg K_f$ be arbitrarily large?

The response is certainly in the affirmative, although creating K_fs with large degree is mildly more difficult for square free N than for general integers N. The case where N is *prime* was considered by Barry Mazur in his “Eisenstein ideal” article (1977).

This talk concerns the situation where a positive t is given in advance and one considers only N of the form $p_1 \cdots p_t$, where the p_i are distinct primes. The question was posed in this form by Luis Dieulefait, and I am reporting on joint work with him and J. Jiminez.

Mazur's argument

Suppose that N is prime and that ℓ is a prime $\neq 2, 3$ that divides $N - 1$. Then there is a newform f on $\Gamma_0(N)$ and a prime λ dividing ℓ in the ring of integers of K_f for which we have

$$a_p \equiv 1 + p \bmod \lambda$$

for all primes p. In particular, we have $a_2 \equiv 3 \bmod \lambda$.

This latter congruence forces $\deg K_f$ to be bigger than a fixed constant times $\log \ell$ (as we'll see in a moment). Taking ℓ big and using Dirichlet's theorem to find an $N \equiv 1 \bmod \ell$, we can make $\deg K_f$ as big as we like.

It is noteworthy that we take λs for which the associated mod ℓ Galois representations are *reducible*.

The point about $a_2 \equiv 3 \bmod \lambda$ is that the complex absolute values of the Galois conjugates of a_2 are all bounded above by $2\sqrt{2} \approx 2.83$. In particular, $a_2 - 3$ is non-zero. The norm of this algebraic integer is divisible by ℓ, but in absolute value it is at most $(3 + 2\sqrt{2})^{\deg K_f}$. Hence

$$\ell \leq (3 + 2\sqrt{2})^{\deg K_f},$$

which gives a logarithmic lower bound on $\deg K_f$.

In this argument, we can use a_3 (or a_5 or ...) instead of a_2; we still get a logarithmic lower bound (with a smaller constant).

What if N is now the product of several primes? To adapt Mazur's argument, we would be delighted to have a supply of newforms at level N for which there are mod ℓ situations (with ℓ as large as we like) where the congruence $a_2 \equiv 3 \bmod \lambda$ holds for some λ dividing ℓ.

As far as I know, there has been little study of Eisenstein primes at composite level. The article "Crystalline cohomology and $\mathbf{GL}(2, \mathbf{Q})$" by G. Faltings and B. Jordan comes closest; it gives necessary conditions for ℓ to be Eisenstein at level N. The theme of their article is that the situation for weight $k > 2$ (with k bounded by ℓ or $\ell+1$) is not significantly harder than the situation for weight 2.

Setting aside Eisenstein primes for the moment, I will present the Dieulefait–Jiminez argument that Goldbach's conjecture implies a positive answer to the question about large degrees at levels $p_1 \cdots p_t$ with $t \geq 2$:

Let ℓ be a (large) prime number, and use Goldbach to write the even number $2^{\ell+4}$ as the sum of two prime numbers: $2^{\ell+4} = p + q$. Note that p and q are necessarily distinct. Let F be the semistable Frey curve associated to the A, B, C solution $p + q = 2^{n+4}$. Its conductor is $2pq$, while its discriminant is $\Delta = (2^{\ell+4}pq)^2/2^8 = (2^{\ell}pq)^2$.

The mod ℓ representation $F[\ell]$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is irreducible and unramified at 2. Although it comes initially from a newform of level $2pq$, by level-lowering (Conjecture ϵ) it arises from a form of level pq. The trace of the action of $\mathrm{Frob}_2 \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $F[\ell]$ is $\pm(1 + 2)$, so we get $a_2 \equiv \pm 3$ for the form of level pq. This gives what we want in the case of a product of two primes.

To treat the case of more than two primes, we modify the argument for two primes by raising the level. Starting with the irreducible mod ℓ representation afforded by $F[\ell]$, we can find forms of level $pq \cdot p_3 p_4 \cdots p_t$ by adding extra primes $p_3, \ldots, p_t$ into the level. For this, we have to take care not to lose spurious primes as we add on new ones. The required analysis is carried out in the article by F. Diamond and R. Taylor: "Nonoptimal levels of mod l modular representations."

We don't know Goldbach's conjecture, but we do have Chen's partial result "On the representation of a larger even integer as the sum of a prime and the product of at most two primes" (1973). It shows, for sufficiently large ℓ, that $2^{\ell+4}$ is the sum of a prime and an integer that is either prime for the product of two primes. Using it, together with level-raising as needed, we can prove that $\deg K_f$ is unbounded when levels are restricted to be the product of three or more primes.

Using Mazur's argument for $t = 1$ and Chen + Barcelona for $t \geq 3$, we arrive at a situation where only the case $t = 2$ requires further analysis. (A proof of Goldbach's conjecture would be sufficient to handle this case.)

One way to treat the case where $N = pq$ without proving Goldbach's conjecture is to appeal to Ogg's 1974 article "Hyperelliptic modular curves." If p and q are distinct primes, Ogg finds a degree 0 cuspidal divisor on $X_0(pq)$ whose image on $J_0(pq)$ has order equal to the numerator of the fraction $(p-1)(q+1)/24$.

Take $\ell > 3$; we want it to be large anyway. If ℓ divides $(p-1)(q+1)$, we can mimic Mazur's arguments to find an eigenform f at level pq that is Eisenstein mod ℓ. For us, this means that the coefficient $a_2(f)$ is 3 mod some prime λ dividing ℓ, and we deduce that the degree of K_f is large as before.

We need to ensure that f is genuinely a newform, i.e., that its eigenvalues do not arise at level p or at level q. We begin as before by taking ℓ large. Then we find $q \equiv -1 \bmod \ell$ and pick p to be a random prime that is *not* 1 mod ℓ. Since the Eisenstein primes at prime level N are divisors of $N-1$, we see that ℓ is not an Eisenstein prime at either level p or level q.

Suppose that p and q are distinct primes. What are the Eisenstein primes at level pq?

In other words, what prime numbers ℓ have the property that there is a newform of weight 2 on $\Gamma_0(pq)$ whose prime-indexed coefficients a_r satisfy the Eisenstein congruence $a_r \equiv r + 1 \mod \lambda$ for some prime ideal $\lambda | \ell$?

Perhaps out of sheer laziness, we will always assume ℓ prime to $6pq$.

If f is a newform of level pq, there are two signs associated with f: $f|T_p = \pm f$, $f|T_q = \pm f$. Suppose that one of the signs, say the second one, is -1. If $\lambda|\ell$ is an Eisenstein prime, the semisimplication of the mod λ Galois representation attached to f is the direct sum of the trivial representation and the mod ℓ cylotomic character. In particular, the trace of the action of Frob_q in this semisimplifcation is $1 + q$.

But it is also $-(1 + q)$ because of the equation $f|T_q = -f$. Hence we may deduce that ℓ divides $q + 1$.

In this situation, one can prove that $f|T_p = +f$; the two Atkin–Lehner operators T_p and T_q cannot both act as -1 in an Eisenstein situation. (The argument is like the one that Mazur uses to prove that the minus sign does not occur at prime level.)

Conversely, one can prove that if ℓ divides $q+1$, there is an Eisenstein situation mod ℓ for some newform of level pq with signs $(+,-)$.

More generally, suppose that D is a product of an odd number of primes and that q is a prime that does not divide D. If ℓ divides $q+1$, there is a newform f at level Dq that is Eisenstein mod ℓ and that satisfies

$$f|T_p = +f \text{ for all } p|D, \quad f|T_q = -q.$$

This statement can be used to solve the original problem (deg $K_f \to \infty$) when the level is a product of t primes with t even.

To prove the assertion, one looks at the Jacobian $J = J_0^{Dq}(1)$ associated with the Shimura curve made with the rational quaternion algebra of discriminant Dq. Let Ψ be the component group attached to the mod q reduction of the Néron model of J. One can analyze Ψ as in my 1990 Inventiones paper and exhibit an Eisenstein quotient of Ψ whose order is roughly $q+1$. ("Roughly" means "away from 2 and 3.")

To see the quotient, you need to choose a prime p dividing D and compare Ψ with the component groups in the mod p reductions of $J_0^{D/p}(p)$ and $J_0^{D/p}(pq)$. These groups are independent of p! This is something that never occurred to me 20 years ago because I always took $D = p$. However, I believe that it was noticed soon after my work when people contemplated natural generalizations.

A parallel result concerns the case where the level is a product of an odd number of primes. If D is again such a product and $\ell > 3$ is a divisor of $\varphi(D)$, then one proves (by choosing $p|D$ and examining the component group in the mod p reduction of $J_0^{D/p}(p)$) that there is an Eisenstein prime mod ℓ at level D. The construction shows more precisely that there is a newform f of level D that is Eisenstein mod ℓ and that satisfies $f|T_p = f$ for all $p|D$.

For example, there is a newform of level 1001 that is Eisenstein mod 5. On Stein's list, it is the last newform (the one generating a field of degree 11) that fits the bill. (Aside: is there a reason why the degree needs to be so large?)

Observe that the mod 5 representation that comes from the unique newform of level 11 arises from a newform of level $11 \cdot 7 \cdot 13$ but not from a form of level $11 \cdot 7$ or level $11 \cdot 13$. This phenomenon never occurs for irreducible mod ℓ representations.

Indeed, suppose that ρ is such a representation and that $N(\rho)$ is its Serre conductor. Then, as we know, ρ arises from a form of level $N(\rho)$. If it comes also from a newform of level $N(\rho)M$, where M is square free, it comes from newforms of all levels $N(\rho)d$, where d runs over the positive divisors of M.

It is validating—and great fun—to find in Stein's tables the various newforms whose existence is predicted by general theory.

One can ask for a complete description of the Eisenstein primes at square free level. Consider the special case of level pq. A priori, we should analyze the question for four pairs of signs, but the case $f|T_p = f|T_q = -f$ never occurs, and the case $f|T_p = -f$, $f|T_q = T_q$ reduces by symmetry to the $+,-$ case, which we already understand: ℓ is an Eisenstein prime in this situation if and only if ℓ divides $q+1$.

We are left with the case where f is fixed by both T_p and T_q. This case is parallel to the prime-level case, where we can borrow Mazur's argument (comparison with an Eisenstein series) to deduce that ℓ divides $(p-1)(q-1)$. Again by symmetry, we can and will assume: ℓ divides $p-1$.

In this case, there is an Eisenstein prime at level p, and we are asking about the possibility of “raising level” from level p to level pq. If f is a newform that is Eisenstein mod λ, one thinks immediately of the congruences

$$a_q(f) \equiv \pm(1+q) \bmod \lambda,$$

which are the standard necessary and sufficient conditions for raising level. The two possible signs correspond to the eigenvalues for T_q after the level has been raised.

Because we’re in an Eisenstein situation, the congruence $a_q(f) \equiv 1+q$ is satisfied *for all* q, and the congruence $a_q(f) \equiv -(1+q)$ amounts to the divisibility of $1+q$ by ℓ, which indeed is the condition for having an Eisenstein prime with signs $(+,-)$.

It is perhaps tempting to guess initially that the condition for raising levels with signs $(+,+)$ is the empty condition, since the congruence $a_q \equiv 1 + q$ is always satisfied. However, already when $p = 11$, there is a mod 5 Eisenstein prime at level $11q$ only for certain q. In particular, none of the four newforms of level 77 is Eisenstein at 5.

Experiments show convincingly that the condition for raising to level $11q$ is that q needs to be ±1 mod 11 or 1 mod 5 (or both).

The natural generalization of this condition (when 11 is replaced by p) is as follows. Because ℓ divides $p - 1$, there is a unique Eisenstein maximal ideal $\mathfrak{m}$ of residue characteristic ℓ in the Hecke ring $\mathbf{T}$ at level p. The level-raising condition is that the element $T_q - q - 1$ of $\mathfrak{m}$ should fail to be a local generator of the Eisenstein ideal I of $\mathbf{T}$.

According to Mazur's article, this failure occurs precisely when q is 1 mod ℓ or q is an ℓth power mod p.

Here's a quick explanation of why $\mathfrak{m}$ is Eisenstein at level pq if $T_q - q - 1$ does not generate I locally at $\mathfrak{m}$: Let Ψ be the component group of J_0^{pq} at q and let Φ be the component group of $J_0(p)$ at p. Finally, let X be the character group of the torus in the mod p reduction of $J_0(p)$. There is an exact sequence

$$0 \to \Phi \to X/(T_q - q - 1)X \to \Psi^+ \to 0,$$

where the "$^+$" refers to the action of the Atkin–Leher T_q on Ψ. (Of course, the T_q in the exact sequence is the T_q at level p.) The group Φ is free of rank 1 over $\mathbf{T}/I$. Also, X is a locally free $\mathbf{T}$-module of rank 1. If $T_q - q - 1$ is a non-generator at $\mathfrak{m}$, the image of $(X/(T_q - q - 1)X)_\mathfrak{m}$ in Ψ^+ is non-trivial.