MODULAR DEGREES AND CONGRUENCES AMONG MODULAR FORMS

KEN RIBET

Suppose that $E/\mathbb{Q}$ is an elliptic curve. Then there is a non-constant map $\pi\colon X_0(N) \to E$ sending ∞ to 0. It induces maps $E \to J_0(N) \to E$ whose composition is multiplication by $\deg \pi$. The map $E \to J_0(N)$ need not be injective, and dually $J_0(N) \to E$ need not have connected kernel. Factor $E \to J_0(N)$ as $E \to E' \to J_0(N)$ where $E \to E'$ is an isogeny and $E' \to J_0(N)$ is injective. By replacing E by E', we may assume that $\pi^*\colon E \to J_0(N)$ is injective and that $\pi_*\colon J_0(N) \to E$ has connected kernel: this is called the *optimal* situation. Let $B = \ker \pi_*$, so B is an abelian subvariety of $J_0(N)$. Let $A = \pi_* E \subseteq J_0(N)$. We might write $A_f = A$; sometimes instead the quotient E is called A_f. We have a map $X_0(N) \to J_0(N)$ sending ∞ to 0.

Perhaps the initial object should have been $f = \sum a_n q^n$, and from this arose an optimal curve E. Zagier gave an algorithm to compute $\deg \pi$ for prime conductor. Cremona generalized it to arbitrary conductor. Agashe-Stein and Stein-Watkins contain data on $\deg \pi$.

Watkins:

- odd modular degrees are rare, and in particular should imply that $E(\mathbb{Q})$ is finite.
- $2^{\operatorname{rank} E(\mathbb{Q})}$ divides $\deg \pi$.

Dummigan: "$2^r \mid \deg \pi$" is explained by a 2-adic $R \xrightarrow{\sim} \mathbb{T}$ conjecture.

Calegari-Emerton: Investigate optimal curves with odd modular degree. We assume this from now on.

Example 0.1. If $\deg \pi$ is odd, then $f|_{w_N} = -f$, where w_N is the principal Atkin-Lehner involution. In particular, the sign of the functional equation for $L(E,s)$ is $+1$; in other words the analytic rank of E is even.

If $\deg \pi$ is odd and w is an Atkin-Lehner involution such that $f|_w = -f$, then $X_0(N) \to X_0(N)/w$ is unramified.

Example 0.2. Suppose there exists f with $\deg \pi$ odd, and $N = pq$ with $p = 43$ and $q = 59$. Suppose $f|_{w_p} = -f$ and $f|_{w_q} = f$, or $f|_{w_q} = -f$ and $f|_{w_p} = f$. Fact: $f|_{w_59} = +f$, $f|_{w_{43}} = -f$. Since $\left(\frac{-59}{43}\right) = -1$, there are no fixed points. We have $p \equiv q \equiv 11 \pmod{16}$.

In $J_0(N)$ we have A and $B = A^\perp$. Then $A \cap B = \pi^*(E[\deg \pi])$. By assumption, $A[2] \cap B = \{0\}$.

Let $X = X_0(N)$ and $X_+ = X_0(N)/w$. Suppose that $X \to X_+$ is ramified. Let J_+ be the image of $J(X_+) \to J(X)$. Let J_- be the kernel of $J(X) \to J(X_+)$. Then $J_+ \cap J_- = J[2]$. We have $A \subseteq J_+$ and $J_- \subseteq B$. Then $A[2] \subseteq J_+[2] \subseteq J_-[2] \subseteq B$, a contradiction.

If $X \to X_+$ is unramified and $\deg \pi$ is odd, and $f|_w = +f$, then $E[2]$ is a reducible Galois module.

Date: June 7, 2007.

Calegari-Emerton: If no w_d acts as $+1$ on f, then N must be divisible by at most two odd primes: i.e., $N = 2^a p^b q^c$ for distinct odd primes p and q and $a, b, c \in \mathbb{Z}_{\geq 0}$.

Calegari-Emerton focus on the case where N is a power of a prime. If N is a power of 2, there are only finitely many elliptic curves, which we inspect individually. So assume $N = p^b$ where p is odd and $b \geq 1$.

Claim: If $b > 1$, then E has CM by $\mathbb{Q}(\sqrt{-p})$, which again leads to only finitely many elliptic curves.

If $\deg \pi$ is odd, then the congruence modulus of f is odd. It is not true that $f \equiv g \pmod 2$, with g an integral form in $S_2(\Gamma_0(N), \mathbb{Z})$ with $f \perp g$.

Given f and χ, we may form $f \otimes \chi := \sum_{n \geq 1} \chi(n) a_n q^n$. This has character χ^2, and level bounded in terms of $\operatorname{cond} \chi$ and the level of f.

Suppose that χ is the quadratic character of conductor p. Then $f \otimes \chi \in S_2(\Gamma_0(N))$. If $N = p^b$ for $b \geq 2$, then $f \equiv f \otimes \chi \pmod 2$ forces $f = f \otimes \chi$, i.e., that f has CM.

The thesis of S. Yazdani considers the case where N is not a prime power.

Remark 0.3. Suppose that $N = p^b q^c$ where p, q are distinct primes and $b, c \geq 1$. If $b > 1$, then E has CM by $\mathbb{Q}(\sqrt{-p})$; then $c \geq 2$, so E has CM by $\mathbb{Q}(\sqrt{-q})$, which is a contradiction. Thus $b = c = 1$.

Theorem 0.4 (Yazdani). *If $N = pq$ and $\deg \pi$ is odd, then either $pq \leq 21$ or $p \equiv q \equiv 3 \pmod 8$.*

Ideas of proof. Let $C \subseteq J_0(N)$ be the cuspidal subgroup. The cusps, in Ogg's notation, are P_1, P_p, P_q, P_{pq}. Ogg computed the order of the class of $P_1 - P_p + P_q - P_{pq}$. Heuristic assertion: C has a large 2-primary component.

The subgroup $E[2]$ of $J := J_0(N)$ is reducible and Eisenstein. We also have $\ker(C \to E) \subseteq B := \ker(\pi_* \colon J \to E)$ in J, and it is Eisenstein and rational, while E has few rational torsion points.

Let $\mathbb{T} = \mathbb{Z}[\ldots T_n \ldots] \subseteq \operatorname{End} J$. We have $\mathbb{T} \twoheadrightarrow \mathbb{Z} \subseteq \operatorname{End} A$ sending T_n to a_n. Composition with $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ gives a homomorphism $\phi \colon \mathbb{T} \to \mathbb{Z}/2\mathbb{Z}$ whose kernel is a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$.

Unless p and q satisfy restrictive congruences, $B[\mathfrak{m}] \neq 0$. This amounts to a mod 2 congruence between f and a perpendicular form, which is impossible. $\square$