Some Modular Degree and Congruence Modulus Computations

William A. Stein

September 29, 2002

Contents

1 The Definitions **1**

2 The History **2**

3 The Naive Algorithms **3**

3.1 A way to compute m_E 3

3.2 A way to compute c_E 3

4 The Examples **3**

5 The Future **4**

1 The Definitions

Let $E/\mathbf{Q}$ be an elliptic curve that is an *optimal quotient* of $J_0(N_E)$, where $N = N_E$ is the conductor of E. Here $J_0(N)$ is the Jacobian of the algebraic curve $X_0(N)$ and a deep theorem implies that there is a surjective morphism $\pi : X_0(N) \to E$. The condition that E is optimal means that the induced map $\pi_* : J_0(N) \to E$ has (geometrically) connected kernel.

Definition 1.1. The *modular degree* of E is

$$m_E = \deg(\pi).$$

One reason that the modular degree is well worth thinking about is that an assertion about how m_E grows relative to N_E is equivalent to the ABC Conjecture.

Let $f = f_E = \sum a_n q^n \in S_2(\Gamma_0(N))$ be the newform attached to E.

Definition 1.2. The *congruence modulus* of E is

$$c_E = \# \left(\frac{S_2(\Gamma_0(N), \mathbf{Z})}{\mathbf{Z}f + (\mathbf{Z}f)^{\perp}} \right),$$

where $(\mathbf{Z}f)^{\perp}$ is the unique $\mathbf{T} = \mathbf{Z}[\ldots T_n \ldots]$-module complement of $\mathbf{Z}f$ in $S_2(\Gamma_0(N), \mathbf{Z})$. Equivalently,

$$c_E = \max\{c : f \equiv g \pmod{c} \text{ for some } g \in (\mathbf{Z}f)^{\perp}\}.$$

2 The History

- **<1984:** ??
- **1984:** Don Zagier wrote the often-cited paper *Modular parametrizations of elliptic curves* (1985), in which he gave an algorithm to compute m_E (sometimes?). The paper inclcued
  - A result of Ribet:

    Theorem 2.1 (Ribet). *If N_E is prime, then*

    $$m_E = c_E.$$

  - It also said

    $$c_E \mid m_E.$$

- **1998:** Frey and Müller published a wonderful survey: *Arithmetic of modular curves and applications.*
  - They ask: **Question 4.4**: Let E be an optimal quotient of any conductor. Does $m_E = c_E$?
  - They remark that $c_E \mid m_E$ and give two references [Ribet 83, Inventiones] and [Zagier 1985].

- **1995:** Cremona wrote a Math. Comp. paper, and computed m_E for every curve of conductor $\leq N$, where N is a few thousand.

- **2001:** Mark Watkins computed m_E for some curves with N_E **HUGE**, using an algorithm he created from a formula of M. Flach.[1]

3 The Naive Algorithms

3.1 A way to compute m_E

Use the (not-exact!) sequence:

$$H_1(E, \mathbf{Z}) \to H_1(X_0(N), \mathbf{Z}) \to H_1(E, \mathbf{Z}).$$

The composition map from $H_1(E, \mathbf{Z}) \to H_1(E, \mathbf{Z})$ is multiplication by m_E, and $H_1(E, \mathbf{Z})$ can be computed because its image in $H_1(X_0(N), \mathbf{Z})$ is saturated, as E is optimal. This algorithm is described in detail in [Kohel-Stein, ANTS IV], and amounts to finding "left and right eigenvectors" and taking their dot product.

3.2 A way to compute c_E

Compute $S_2(\Gamma_0(N), \mathbf{Z}) \subset \mathbf{Z}[[q]]$ to precision $[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(N)]/6$ using, e.g., modular symbols, then use a Smith Normal Form algorithm.

4 The Examples

These examples were computed by myself and Amod Agashe.

- **54B**: Let E be the elliptic curve $y^2 + xy + y = x^3 - x^2 + x - 1$. Then $m_E = 2$ and $c_E = 6$. In fact, it's easy to see that $3 \mid c_E$ "by hand" by writing down the form f corresponding to **54B** and the form g corresponding to $X_0(27)$ and noting that $f(q) \equiv g(q) + g(q^2) \pmod 3$. (Because of the "Sturm Bound", it suffices to check this up to $O(q^{19})$.)

[1] Watkins: "The formula appears in Flach surely, but Flach claims it comes essentially from Hida. Zagier says it is essentially due to Rankin. I would merit that Shimura's contribution is not irrelevant either."

Hey $c_E \neq m_E$!! In fact, $c_E \nmid m_E$!! When we first did this computation, Ribet had already mentioned to us that he had really proved that $m_E \mid c_E$, not vice-versa. We were, however, extremely surprised to find so quickly an example in which $c_E \neq m_E$.

- **T-shirt**: My t-shirt has **243A** and **243B** on it. For **243A**, we have $m_E = 9$ and $c_E = 27$. For **243B**, we have $m_E = 6$ and $c_E = 54$. I designed the t-shirt many months before I knew that question 4.4 had a negative answer.

- **242B**: $N = 2 \cdot 11^2$.

$$m_E = 2^4 \neq c_E = 2^4 \cdot 11$$

  The failure is probably not just a "small primes" phenomenon.

Moral: A little computation sometimes greatly cleans the air.

5 The Future

Based on computations, Amod and I conjectured and Ribet proved the following theorem.

Theorem 5.1 (Ribet, 2001). *Let E be an elliptic curve of conductor N. If $p^2 \nmid N$ then $\mathrm{ord}_p(m_E) = \mathrm{ord}_p(c_E)$.*

New Version of "**Question 4.4**. For all $N_E \leq 539$, we have

$$2 \cdot \mathrm{ord}_p(c_E/m_E) \leq \mathrm{ord}_p(N_E).$$

In particular, for $p \geq 5$, do we have

$$\mathrm{ord}_p(c_E/m_E) \leq 1?$$

Is this true in general?