The Ring of Modular Correspondences

1. Introduction.

Let: $\Gamma(N) = \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$, the principal congruence subgroup of level N,

$X(N) = \Gamma(N)\backslash\mathfrak{H}^*$, the associated modular curve,

$J(N) = \mathrm{Jac}(X(N))$, its Jacobian variety,

$\mathbb{E}_N = \mathrm{End}^0(J(N)) = \mathrm{End}(J(N)) \otimes \mathbb{Q}$, the endomorphism algebra of $J(N)$ (Ring of correspondences),

$\mathbb{M}_N = \sum \mathbb{Q}T_A \subset \mathbb{E}_N$, the subring of modular correspondences.

Here, the above sum runs over all matrices $A \in \mathrm{GL}_2(\mathbb{Q})^+$, and

$$T_A = T_A^{(N)} : J_N \to J_N,$$

is the endomorphism defined by the curve (correspondence) C_A on $X_N \times X_N$ which is the image of the curve

$$\tilde{C}_A = \{(z, A(z)) : z \in \mathcal{H}^*\} \subset \mathcal{H}^* \times \mathcal{H}^*.$$

Note: Modular correspondences were introduced by Klein (1879) and were studied by him and by Hurwitz (1883–87). The book of Klein/Fricke (1893) gives a systematic exposition of the theory. Their discussion suggests the following:

Questions: 1) When is every correspondence on X_N modular, i.e., when is $\mathbb{M}_N = \mathbb{E}_N$?

2) How large can $\delta_N := \dim \mathbb{E}_N - \dim \mathbb{M}_N$ be?

3) What is the growth rate of $\dim \mathbb{E}_N$ (and of $\dim \mathbb{M}_N$) as $N \to \infty$?

Remarks: 1) We have the trivial upper bound

$$\dim \mathbb{E}_N \le 2g_N^2,$$

where g_N denotes the genus of $X(N)$, i.e.

$$g_N = 1 + \frac{1}{24}\phi(N)\psi(N)(N-6) \asymp N^3,$$

where $\psi(N) = N\prod_{p|N}(1+\frac{1}{p})$ is the Dedekind ψ-function. Thus, we shall measure the growth rate in terms of g_N.

2) As we shall see, the answer to Question 3) sheds some light on the more general question of determining the growth rate of the function

$$d_g := \max\{\dim \mathrm{End}(J_X) : X/\mathbb{C} \text{ is a curve of genus } g\} \le 2g^2.$$

This question is partially related to the questions asked by Ellenberg (2001) concerning the growth rate of certain subalgebras of $\mathrm{End}(J_X)$.

3) Since $X(N)$ has a canonical model $X(N)_{/\mathbb{Q}}$ over $\mathbb{Q}$, we could also ask the corresponding questions for the subalgebra

$$\mathbb{E}_N^{\mathbb{Q}} := \mathrm{End}(J(N)_{/\mathbb{Q}}) = \mathrm{End}(J(N))^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$$

of endomorphisms which are defined over $\mathbb{Q}$. It turns out that this situation is much easier to analyze.

2. Main Results.

Let: $\mathcal{K} = \{\mathbb{Q}(\sqrt{-n})\}_{n\geq 1}$ be the set of imag.-quad. fields,
$h(D)$ the class number of (forms of) discriminant D, so
$h_K = h(d_K)$ is the class number of K, where $d_K = \mathrm{disc}(K)$.

Theorem 1: If $N \geq 1$, then

$$\begin{aligned}\mathbb{M}_N = \mathbb{E}_N \;&\Leftrightarrow\; h(N^2/d_K) = 1,\ \forall K \in \mathcal{K} \text{ with } d_K|N.\\ &\Leftrightarrow\; \text{either: } 4\nmid N \text{ and } p \equiv 1 \pmod 4, \forall p|N, p \neq 2,\\ &\qquad \text{or: } N \in \{3,4,6,7,8,9,11,14,19,43,67,163\}.\end{aligned}$$

Remark: The second equivalence uses the resolution of the class number 1 problem (Heegner, Stark).

Examples: (a) $\mathbb{M}_N = \mathbb{E}_N$, if $N \leq 11$ or if $N = 13, 14, 17, 25, \ldots$
(b) $\mathbb{M}_N \neq \mathbb{E}_N$, if $N = 12, 15, 16, 18, 20, 21, 22, 23, 24, \ldots$

Theorem 2: If $N \geq 30$, then

$$\begin{aligned}\sqrt[3]{3/4}\, g_N^{4/3} \;\leq\; \dim \mathbb{M}_N \;&\leq\; \psi(N) g_N + O(g_N^{1+\varepsilon})\\ &\leq\; \log\log(g_N) g_N^{4/3} + O(g_N^{1+\varepsilon}).\end{aligned}$$

Remark: This uses the recent result of Solé/Planat (2011):

$$\psi(N) \leq e^{\gamma} \log\log(N) N, \quad \text{if } N \geq 30.$$

Theorem 3: For any $\varepsilon > 0$

$$\delta_N := \dim \mathbb{E}_N - \dim \mathbb{M}_N = O(g_N^{4/3+\varepsilon}) \text{ but } \delta_N \neq O(g_N^{4/3-\varepsilon}).$$

Thus

$$\dim \mathbb{E}_N = O(g_N^{4/3+\varepsilon}).$$

If we restrict N to primes and/or to prime powers, then more can be said.

Theorem 4: If $N = p$ is prime, then

$$\dim(\mathbb{M}_p) = 2\sqrt[3]{3}\, g_p^{4/3} + O(g_p).$$

Moreover, for any $\varepsilon > 0$

$$\dim(\mathbb{E}_p) = 2\sqrt[3]{3}\, g_p^{4/3} + O(\log(g_p)^2 g_p).$$

Remark: This follows from a preprint of K.-Mohit, which gives an explicit formula for $\dim \mathbb{M}_p$.

Theorem 5: If $N = p^r$ is a prime power with $p \equiv 3 \pmod 4$, then

$$\delta_N = 24\sqrt[3]{3}\,\frac{h(-p)^2}{p^2} g_N^{4/3} + O(\log(p) g_N).$$

Remarks: 1) Thus, the "error term" δ_N is almost as large as (the lower bound for) $\dim \mathbb{E}_N$.

Theorem 6: (a) Every $\mathbb{Q}$-rational endomorphism $f \in \mathbb{E}_N^{\mathbb{Q}}$ is modular, i.e.,

$$\mathbb{E}_N^{\mathbb{Q}} = \mathbb{M}_N^{\mathbb{Q}} := (\mathbb{M}_N)^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}.$$

(b) If $N > 12$, then

$$g_N < \dim \mathbb{E}_N^{\mathbb{Q}} \le \sigma_0(N^2) g_N;$$

In particular, $\dim E_N^{\mathbb{Q}} = O(g_N^{1+\varepsilon})$, for all $\varepsilon > 0$.

Remark: Theorem 6 follows easily from the results of K. (2008).

3. Basic Ingredients.

Main Steps: 1) Use Atkin-Lehner theory etc., to study the action of $\mathbb{M}_{N,\mathbb{C}} := \mathbb{M}_N \otimes \mathbb{C}$ on the space

$$V = S_2(\Gamma(N)),$$

and use this to determine the algebra structure of

$$\overline{\mathbb{M}}_{N,\mathbb{C}} = \text{the image of } \mathbb{M}_{N,\mathbb{C}} \text{ in } \mathrm{End}_{\mathbb{C}}(V).$$

2) Determine $\mathrm{Ker}(\mathbb{M}_{N,\mathbb{C}} \to \overline{\mathbb{M}}_{N,\mathbb{C}})$. For this, it is useful to split V as

$$V = V^{nCM} \oplus V^{CM}$$

where V^{CM} is the subspace of forms with complex multiplication (CM) and V^{nCM} the subspace of forms without CM, and to study the action on these spaces separately. This leads to the decomposition

$$\overline{\mathbb{M}}_{N,\mathbb{C}} = \overline{\mathbb{M}}_{N,\mathbb{C}}^{nCM} \oplus \overline{\mathbb{M}}_{N,\mathbb{C}}^{CM}.$$

3) Using the results of Ribet (1980), study the structure of $\mathbb{E}_N$. For this, note that we have an isogeny decomposition

$$J(N) \sim J(N)^{nCM} \times J(N)^{CM}$$

which induces algebra decompositions

$$\mathbb{E}_N = \mathbb{E}_N^{nCM} \oplus \mathbb{E}_N^{CM} \quad \text{and} \quad \mathbb{M}_N = \mathbb{M}_N^{nCM} \oplus \mathbb{M}_N^{CM},$$

where $\mathbb{E}_N^{nCM} = \mathrm{End}(J(N)^{nCM}) \otimes \mathbb{Q}$, $\mathbb{E}_N^{CM} = \mathrm{End}(J(N)^{CM}) \otimes \mathbb{Q}$, and $\mathbb{M}^{nCM} = \mathbb{E}_N^{nCM} \cap \mathbb{M}_N$ and $\mathbb{M}^{CM} = \mathbb{E}_N^{CM} \cap \mathbb{M}_N$.

4. The Structure of $\overline{\mathbb{M}} = \overline{\mathbb{M}}_{N,\mathbb{C}}$.

Notation: Let $\mathcal{N}(V)$ denote the set of normalized newforms (of all levels) in $V = S_2(\Gamma(N))$.

Observation: The group A_N^* of characters on $A_N := (\mathbb{Z}/N\mathbb{Z})^\times$ acts on $\mathcal{N}(V)$. (This action is induced by twisting.) Let

$$\overline{\mathcal{N}}(V) = \mathcal{N}(V)/A_N^* \quad \text{(orbit space)}.$$

Theorem 7: V has multiplicity one as an $\overline{\mathbb{M}}$-module. More precisely, if $V(f)$ denotes the $\overline{\mathbb{M}}$-module generated by $f \in \mathcal{N}(V)$, then $V(f)$ is irreducible and one has the decomposition

$$V = \bigoplus_{f \in \overline{\mathcal{N}}(V)} V(f)$$

into pairwise non-isomorphic $\overline{\mathbb{M}}$-modules. Thus

$$\dim_{\mathbb{C}} Z(\overline{\mathbb{M}}) = |\overline{\mathcal{N}}(V)| = |\mathcal{N}^{nCM}|/\phi(N) + 2|\mathcal{N}^{CM}|/\phi(N),$$

where $\mathcal{N}^{nCM} = \mathcal{N}(V) \cap V^{nCM}$ and $\mathcal{N}^{CM} = \mathcal{N}(V) \cap V^{CM}$.

Theorem 8: If $N \geq 5$, then

$$|\mathcal{N}(V)| = \frac{1}{24}\phi(N)^2(\psi(N) - 6),$$

and hence $\dim_{\mathbb{C}} Z(\overline{\mathbb{M}}) \leq \frac{1}{12}\phi(N)(\psi(N) - 6)$.

Theorem 9 (K.-Mohit): We have that

$$\dim_{\mathbb{C}} V(f) \leq \psi(N), \quad \text{for all } f \in \mathcal{N}(V).$$

Remark: In our preprint we give in a precise formula for $\dim V(f)$. (This uses the results of Atkin/Li (1978).)

Corollary: If $N \geq 5$, then

$$\sqrt[3]{\frac{3}{4}g_N^{4/3}} \;\leq\; \dim_{\mathbb{C}} \overline{\mathbb{M}} \;\leq\; \psi(N) g_N.$$

Remark: This follows from Theorems 7-9 because of the following simple fact:

Lemma: Let $A \subset \mathrm{End}_{\mathbb{C}}(V)$ be a $\mathbb{C}$-algebra such that V is semisimple and has multiplicity one as an A-module. Then

$$\frac{g^2}{z} \;\leq\; \dim_{\mathbb{C}} A \;\leq\; Mg,$$

where $g = \dim_{\mathbb{C}} V, z = \dim_{\mathbb{C}}(Z(A))$, and

$$M = \max\{\dim(V_i) : V_i \subset V \text{ is irreducible}\}.$$

Remark: More precisely, if

$$V = \bigoplus_i V_i$$

is the decomposition of V into irreducible A-modules, then

$$\dim A = \sum (\dim V_i)^2.$$

5. The Kernel of $\mathbb{M}_{N,\mathbb{C}} \to \overline{\mathbb{M}}_{N,\mathbb{C}}$.

Theorem 10: We have that

$$\dim_{\mathbb{C}}(\mathrm{Ker}(\mathbb{M}_{N,\mathbb{C}} \to \overline{\mathbb{M}}_{N,\mathbb{C}})) = \dim_{\mathbb{C}} \overline{\mathbb{M}}_{N,\mathbb{C}}^{CM}$$

and so

$$\dim \mathbb{M}_N = \dim_{\mathbb{C}} \overline{\mathbb{M}}_{N,\mathbb{C}}^{ncM} + 2 \dim_{\mathbb{C}} \overline{\mathbb{M}}_{N,\mathbb{C}}^{CM}.$$

Remark: This result is proved by studying the $\mathbb{M}_N$-structure of the module $H^1(X(N), \mathbb{C}) \simeq V \oplus V^*$. Here $V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ is the contragredient $M_{N,\mathbb{C}}$-module. A key ingredient is:

Theorem 11: If $f \in \mathcal{N}(V)$, then

$$V(f)^* \simeq_{\mathbb{M}} V(f) \quad \Leftrightarrow \quad f \in \mathcal{N}^{nCM}.$$

Theorem 12: The number of CM-newforms in V is

$$|\mathcal{N}(V)^{CM}| \ = \ \frac{\phi(N)}{2} \sum_{d_K|N} h(N^2/d_K),$$

where the sum is over all (fundamental) discriminants of imaginary quadratic fields $K \in \mathcal{K}$ with $d_K|N$. Thus

$$\dim_{\mathbb{C}} Z(\overline{\mathbb{M}}_{N,\mathbb{C}}^{CM}) = \sum_{d_K|N} h(N^2/d_K),$$

and

$$\dim \mathbb{M}_{N,\mathbb{C}}^{CM} = O(N^{3+\varepsilon}) = O(g_N^{1+\varepsilon}), \quad \forall \varepsilon > 0.$$

In particular,

$$\dim \mathbb{M}_N = \dim \overline{\mathbb{M}}_N + O(g_N^{1+\varepsilon}).$$

6. The Structure of $\mathbb{E}_N$.

Notation: If $K \in \mathcal{K}$, let V_K^{CM} denote the subspace of V of forms with CM by $\psi_K = \psi_{d_K} = \left(\frac{d_K}{\cdot}\right)$, and put $s_K = \dim_{\mathbb{C}} V_K^{CM}$.

Theorem 13: If $N \geq 5$, then

$$J(N)^{CM} \sim \prod_{d_K|N} E_K^{s_K},$$

where $E_K/\mathbb{C}$ is any elliptic curve with $\mathrm{End}^0(E_K) = K$. Thus

$$\mathbb{E}_N^{CM} \simeq \bigoplus_{d_K|N} M_{s_K}(K) \text{ and so } \dim \mathbb{E}_N^{CM} = 2\sum_{d_K|N} (s_K)^2.$$

Remark: This follows from the results of Shimura (1976), Ribet (1980) and Theorem 11. Moreover, from the results of Ribet and Theorems 7 and 10 we obtain:

Theorem 14: $\mathbb{E}_N^{nCM} = \mathbb{M}_N^{nCM}$.

Corollary: If $N \geq 5$, then

$$\dim Z(\mathbb{M}_N) - \dim Z(\mathbb{E}_N) = 2\sum_{d_K|N} (h(N^2/d_K) - 1),$$

and

$$\dim \mathbb{E}_N - \dim \mathbb{M}_N \leq 2\sum_{d_K|N} s_K h(N^2/d_K)(h(N^2/d_K) - 1).$$

Remark: This corollary implies Theorem 1!