The Hecke automaton at conductor 163: monotonicity, $\mathbb{Z}/2\mathbb{Z}$ symmetry, and confinement on the formal-group quotient

Abstract

Let $E/\mathbb{Q}$ be the elliptic curve $163a1$, $y^2+y=x^3-2x+1$, and let $f=\sum a_n q^n$ be its weight-2 newform. We classify the action of the six small Hecke operators T_p, $p\in\{3,7,11,19,43,67\}$, on the formal-group quotient at the prime 3, and show it has the structure of a finite-state automaton on the state space $\{\mathrm{VAC}\}\cup(\mathbb{F}_3^\times\times\mathbb{Z}_{\geq 0})$. The automaton has three theorems attached. *(i) Monotonicity:* every gate other than T_3 is shell-non-decreasing, so the conductor depth $k=v_3(z)$ is a monotone counter under any gate sequence that avoids the annihilator. *(ii) Boundary symmetry:* the residue action of the five non-annihilator gates generates the group $\mathbb{Z}/2\mathbb{Z}$, with T_7 realising the unique nontrivial involution and $T_{11},T_{19},T_{43},T_{67}$ acting trivially on the boundary. *(iii) Confinement:* the reachable set from any unit state (r,k) with $r\in\mathbb{F}_3^\times$, $k\geq 0$, in the gate semigroup generated by $\{T_7,T_{11},T_{19},T_{43},T_{67}\}$, is contained in the maximal ideal $\mathfrak{m}=3\mathbb{Z}_3$ once a single shift has been applied; the matter sector $k=0$ is one-way reachable but never re-entered. The constants $\sum_p a_p^2=129=3\cdot 43$ and $\mathrm{SWAP}^2=\mathrm{ID}$ follow as corollaries of the gate table.

1 Setup

Fix the elliptic curve $E: y^2+y=x^3-2x+1$ of conductor 163 (Cremona label $163a1$), with j-invariant $-2^{18}\cdot 3^3\cdot 5^3\cdot 23^3\cdot 29^3/163^2$ and Mordell–Weil rank one, generator $P=(0,0)$. Write $f=\sum a_n q^n$ for its associated weight-2 newform.

For each prime $p\neq 163$ the Hecke operator T_p acts on f by the scalar $a_p\in\mathbb{Z}$. Tabulating for the six smallest such primes:

p	3	7	11	19	43	67
a_p	0	2	-6	-6	7	-2

These are the six *gates* of the automaton.

Lemma 1. $$\sum_{p\in\{3,7,11,19,43,67\}} a_p(E)^2 \;=\; 129 \;=\; 3\cdot 43.$$

Proof. $0+4+36+36+49+4=129$, and $129=3\cdot 43$. □

2 Gate classification

For an integer $n\neq 0$, write $v_3(n)$ for its 3-adic valuation and $\mathrm{u}_3(n):=(n/3^{v_3(n)}) \bmod 3\in\mathbb{F}_3^\times$ for its leading 3-adic unit.

Definition 2. For each gate prime $p\in\{3,7,11,19,43,67\}$, define the gate type by:

- if $a_p = 0$, T_p is an *annihilator*;
- if $a_p \neq 0$ and $v_3(a_p) = 0$, T_p is a *permutation gate* with multiplier $\mathrm{u}_3(a_p) \in \mathbb{F}_3^\times$;
- if $a_p \neq 0$ and $v_3(a_p) \geq 1$, T_p is a *shift gate* of depth $v_3(a_p)$ and unit multiplier $\mathrm{u}_3(a_p)$.

A permutation gate with multiplier 1 is called *identity*, with multiplier 2 is called *swap*.

Proposition 3. *At conductor* 163 *the six small gates have the types:*

p	a_p	$v_3(a_p)$	$\mathrm{u}_3(a_p)$	*type*
3	0	–	–	*annihilator*
7	2	0	2	*swap*
11	−6	1	1	*shift* $(+1, \times 1)$
19	−6	1	1	*shift* $(+1, \times 1)$
43	7	0	1	*identity*
67	−2	0	1	*identity*

Proof. Direct computation from the table of a_p. All 3-adic data is integer arithmetic; $7 \equiv 1 \pmod 3$, $-2 \equiv 1 \pmod 3$, $-6 = -2 \cdot 3$ has $v_3 = 1$ and unit $-2 \equiv 1 \pmod 3$, and $2 \not\equiv 1 \pmod 3$. □

3 The state machine

Definition 4. The *Hecke automaton* $\mathcal{A}_{163}$ has state space

$$Q \;=\; \{\mathrm{VAC}\} \;\cup\; \big\{(r,k) : r \in \mathbb{F}_3^\times,\ k \in \mathbb{Z}_{\geq 0}\big\},$$

six input symbols $\{T_p : p \in \{3, 7, 11, 19, 43, 67\}\}$, and transition function $\delta : Q \times \{T_p\} \to Q$ given by:

$$\delta(\mathrm{VAC}, T_p) = \mathrm{VAC}, \qquad \delta\big((r,k), T_3\big) = \mathrm{VAC},$$

$$\delta\big((r,k), T_p\big) \;=\; \begin{cases} \mathrm{VAC} & \text{if } \mathrm{u}_3(a_p) \cdot r \equiv 0 \pmod 3, \\ \big(\mathrm{u}_3(a_p) \cdot r \bmod 3,\ k + v_3(a_p)\big) & \text{otherwise,} \end{cases}$$

for $p \neq 3$, where $v_3(a_p) \in \{0, 1\}$ by Proposition 3. The state VAC is absorbing.

Remark 5. Since $\mathrm{u}_3(a_p) \in \mathbb{F}_3^\times = \{1, 2\}$ for $p \neq 3$, the residue component never collapses to 0 under the non-annihilator gates, and the *otherwise* branch always applies. Hence the only path into VAC from a unit state is through T_3.

4 The three theorems

Let $\Sigma = \{T_3, T_7, T_{11}, T_{19}, T_{43}, T_{67}\}$ and $\Sigma^* = \Sigma \setminus \{T_3\}$. For a word $w = g_1 \cdots g_n \in \Sigma^n$ and a state $q \in Q$, write $\delta(q, w)$ for the iterated transition.

Theorem 6 (Monotonicity)**.** *For every word $w \in (\Sigma^*)^*$ and every unit state (r,k), the result $\delta((r,k), w)$ is again a unit state (r', k') with*

$$k' \;=\; k \;+\; \sum_{i=1}^{|w|} v_3\big(a_{p(g_i)}\big) \;\geq\; k.$$

The shell coordinate is a non-decreasing additive counter, strictly increasing iff w contains at least one shift gate T_{11} or T_{19}.

Proof. By Proposition 3, every $g \in \Sigma^*$ has either $v_3(a_p) = 0$ (types swap, identity) or $v_3(a_p) = 1$ (shifts T_{11}, T_{19}). The transition $(r, k) \mapsto (\mathrm{u}_3(a_p)r \bmod 3,\ k + v_3(a_p))$ never produces VAC since $\mathrm{u}_3(a_p) \in \{1, 2\}$ and $r \in \{1, 2\}$. Iterating, the shell coordinate accumulates $\sum v_3(a_{p(g_i)}) \geq 0$, with strict inequality iff some $g_i \in \{T_{11}, T_{19}\}$. □

Theorem 7 (Boundary $\mathbb{Z}/2\mathbb{Z}$). *Let $\pi : Q \setminus \{\mathrm{VAC}\} \to \mathbb{F}_3^\times$ be projection to the residue coordinate. The induced action of Σ^* on $\mathbb{F}_3^\times$ factors through the group $\mathbb{F}_3^\times \cong \mathbb{Z}/2\mathbb{Z}$, with*

$$T_7 \mapsto (\textit{nontrivial involution}), \qquad T_{11}, T_{19}, T_{43}, T_{67} \mapsto (\textit{identity}).$$

In particular T_7^2 acts as identity on residues, so $\mathrm{SWAP}^2 = \mathrm{ID}$.

Proof. By Definition 4 the residue acts by multiplication by $\mathrm{u}_3(a_p) \in \mathbb{F}_3^\times$. Reading off Proposition 3, $\mathrm{u}_3(a_7) = 2$ while $\mathrm{u}_3(a_p) = 1$ for $p \in \{11, 19, 43, 67\}$. Since $\mathbb{F}_3^\times = \{1, 2\}$ has order 2, $2^2 = 4 \equiv 1 \pmod 3$. □

Theorem 8 (Confinement). *Let $S \subseteq \mathbb{F}_3^\times \times \mathbb{Z}_{\geq 0}$ be the reachable set*

$$S \;=\; \big\{\, \delta\big((1,0), w\big) \;:\; w \in (\Sigma^*)^* \,\big\}.$$

Then $S = \mathbb{F}_3^\times \times \mathbb{Z}_{\geq 0}$, but the subset $\{(r, 0) : r \in \mathbb{F}_3^\times\}$ (the matter *or boundary sector) is reachable only by words containing no shift gate. Once T_{11} or T_{19} has been applied, the trajectory enters the* vacuum *sector $\mathbb{F}_3^\times \times \mathbb{Z}_{\geq 1}$ and never returns. Equivalently: the 3-adic ideal $\mathfrak{m} = 3\mathbb{Z}_3$ is forward-invariant under Σ^*, and the matter complement $\mathbb{Z}_3^\times$ is forward-absorbing into $\mathfrak{m}$.*

Proof. Reachability: T_7 realises both residues from $r = 1$, and T_{11}^k reaches every shell $k \geq 0$. Forward invariance of $\mathfrak{m}$: by Theorem 6, the shell coordinate never decreases, so once $k \geq 1$ it remains ≥ 1. Absorption: both shift gates have $v_3 = 1 > 0$, so a single application sends $k = 0$ to $k = 1$. □

Corollary 9. *The annihilator T_3 is the unique gate that exits both sectors into* VAC*. Removing T_3 from the alphabet yields a deterministic automaton on $\mathbb{F}_3^\times \times \mathbb{Z}_{\geq 0}$ in which the matter sector is one-way and the vacuum sector is closed.*

5 The five numbers, revisited

Proposition 10. *The following identities hold for the gate set $\{T_3, T_7, T_{11}, T_{19}, T_{43}, T_{67}\}$ at conductor* 163*:*

(i) $\sum_p a_p^2 = 129 = 3 \cdot 43$.

(ii) $\mathrm{SWAP}^2 = \mathrm{ID}$ *on residues.*

(iii) Exactly one annihilator, exactly one swap, exactly two shifts, exactly two identities.

(iv) The kernel of the residue action $\Sigma^* \to \mathbb{F}_3^\times$ is the submonoid generated by $\{T_{11}, T_{19}, T_{43}, T_{67}\}$, with $\sum_{p \in \ker} a_p^2 = 36 + 36 + 49 + 4 = 125 = 5^3$.

(v) The two shift primes contribute equally: $a_{11}^2 = a_{19}^2 = 36 = 4 \cdot 3^2$.

Proof. (i) Lemma 1. (ii) Theorem 7. (iii) Proposition 3. (iv) The four primes acting trivially on residues are $\{11, 19, 43, 67\}$ by Proposition 3; $36+36+49+4 = 125 = 5^3$. (v) $(-6)^2 = 36 = 4 \cdot 9$. □

Remark 11. Items (iv) and (v) are stated as observations on the gate table, not as structural theorems. Whether $125 = 5^3$ is meaningful (e.g. as a degree of an associated congruence) or coincidental is open.

6 What is *not* proved here

This paper makes only the claims stated above. In particular:

- We do *not* claim the formal-group orbit of the Mordell–Weil generator $P \in E(\mathbb{Q})$ is monotone under multiplication-by-n. Numerical data show the shell pattern $v_3(z(nP))$ is not monotone in n beyond the first few rungs. The monotonicity proved here is a property of *gate sequences acting on the state space*, not of the integer orbit on the curve.
- We do *not* prove the automaton is universal among curves with similar Hecke data. The empirical universality classes observed across ten conductors are deferred.
- The connection to the singularity category $D_{\mathrm{sg}}(R)$ for $R = \mathbb{Z}_3[\eta]/(\eta^2 - 3\eta)$ is sketched only as motivation; the $\mathbb{Z}/2\mathbb{Z}$ of Theorem 7 is established here purely as a property of residue arithmetic.

Reproducibility

The gate classification of Proposition 3 and the arithmetic of Lemma 1 are reproduced by `src/heegner/heegner_ga` which uses Sage to compute $a_p(E)$ from the curve equation directly and applies Definition 2. The full transition table of $\mathcal{A}_{163}$ truncated to shell depth 4 is emitted as `heegner_gate_automaton.json`.