The Fricke-Macbeath Curve

Jaap Top

Johann Bernoulli Institute
University of Groningen

BIRS, September 28th, 2016

- joint work with Carlo Verschoor (master's student in Groningen during 2014/15, currently PhD student with Frits Beukers, Utrecht)

Some history

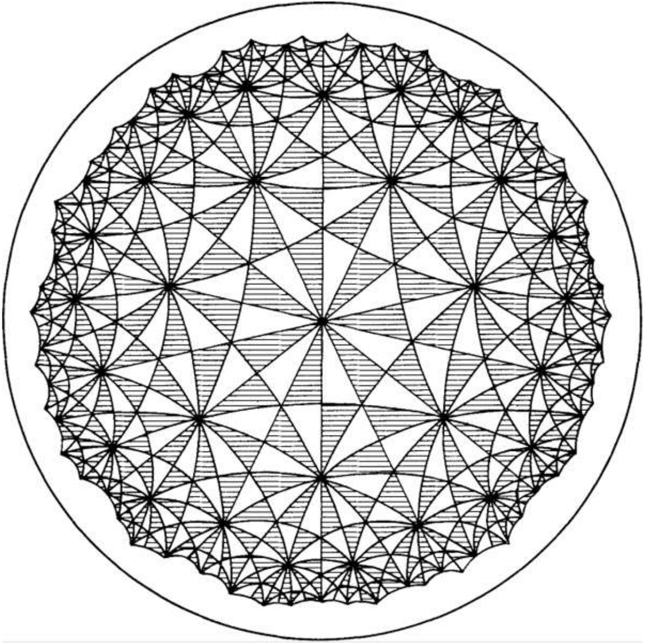
1893, result of A. Hurwitz, Math. Annalen **41**, phrased in modern terms:

- *The automorphism group of an algebraic curve of genus* $g \geq 2$ *over* $\mathbb{C}$ *is finite, of order at most* $84(g-1)$.

Some history

1893, result of A. Hurwitz, Math. Annalen **41**, phrased in modern terms:

- *The automorphism group of an algebraic curve of genus* $g \geq 2$ *over* $\mathbb{C}$ *is finite, of order at most* $84(g-1)$.
- If the automorphism group of an algebraic curve of genus $g \geq 2$ has size $84(g-1)$, then this group is generated by two elements a, b satisfying $a^2 = b^3 = (ab)^7 = 1$.



1879, F. Klein, Math. Annalen **14**

Connection of this talk to Shimura curves:
1967, G. Shimura, Annals of Math. **85**.

Brief sketch:

Connection of this talk to Shimura curves:
1967, G. Shimura, Annals of Math. **85**.

Brief sketch:

- Let $\zeta = e^{2\pi i/7} \in \mathbb{C}$, $\gamma = \zeta + \zeta^6 = 2\cos(2\pi/7) \in \mathbb{R}$, $x \in \mathbb{R}$ with $x^2 = \zeta + \zeta^6 - 1$.

Connection of this talk to Shimura curves:
1967, G. Shimura, Annals of Math. **85**.

Brief sketch:

- Let $\zeta = e^{2\pi i/7} \in \mathbb{C}$, $\gamma = \zeta + \zeta^6 = 2\cos(2\pi/7) \in \mathbb{R}$, $x \in \mathbb{R}$ with $x^2 = \zeta + \zeta^6 - 1$.
- Put $I := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $J := \begin{pmatrix} -x & 0 \\ 0 & x \end{pmatrix}$, $K := IJ = -JI$.
  Let A be the quaternion algebra over $\mathbb{Q}(\gamma)$ generated by I, J, K.

Connection of this talk to Shimura curves:
1967, G. Shimura, Annals of Math. **85**.

Brief sketch:

- Let $\zeta = e^{2\pi i/7} \in \mathbb{C}$, $\gamma = \zeta + \zeta^6 = 2\cos(2\pi/7) \in \mathbb{R}$, $x \in \mathbb{R}$ with $x^2 = \zeta + \zeta^6 - 1$.
- Put $I := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $J := \begin{pmatrix} -x & 0 \\ 0 & x \end{pmatrix}$, $K := IJ = -JI$.
  Let A be the quaternion algebra over $\mathbb{Q}(\gamma)$ generated by I, J, K.
- Put $t := I, u = -\frac{1}{2}(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + (\zeta^3 + \zeta^4)I + J) \in A$.

$$O_A := \mathbb{Z}[\gamma] \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \mathbb{Z}[\gamma]t + \mathbb{Z}[\gamma]u + \mathbb{Z}[\gamma]tu$$

is a maximal order in A. Moreover t, u, tu have order 2, 3, and 7 respectively as elements of $\mathrm{PSL}_2(\mathbb{R})$.

- It turns out that t, u generate the group of elements of norm 1 in $O_A^\times$. This group yields a discrete subgroup Γ in $\mathrm{PSL}_2(\mathbb{R})$.

- It turns out that t, u generate the group of elements of norm 1 in $O_A^\times$. This group yields a discrete subgroup Γ in $\mathrm{PSL}_2(\mathbb{R})$.
- In fact Γ is isomorphic to the Klein triangle group $\Delta(2,3,7)$, and $\Gamma\backslash\mathcal{H} \cong \mathbb{P}^1(\mathbb{C})$ (here $\mathcal{H} =$ upper half plane).

- It turns out that t, u generate the group of elements of norm 1 in $O_A^\times$. This group yields a discrete subgroup Γ in $\mathrm{PSL}_2(\mathbb{R})$.
- In fact Γ is isomorphic to the Klein triangle group $\Delta(2, 3, 7)$, and $\Gamma\backslash\mathcal{H} \cong \mathbb{P}^1(\mathbb{C})$ (here $\mathcal{H} =$ upper half plane).
- The subgroup $\Gamma(2) \subset \Gamma$ consisting of matrices $\equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ mod 2 yields a quotient $\Gamma(2)\backslash\mathcal{H}$ of genus 7. It has automorphisms $\Gamma/\Gamma(2) \cong \mathrm{PSL}_2(\mathbb{F}_8)$.

- It turns out that t, u generate the group of elements of norm 1 in $O_A^\times$. This group yields a discrete subgroup Γ in $\mathsf{PSL}_2(\mathbb{R})$.
- In fact Γ is isomorphic to the Klein triangle group $\Delta(2,3,7)$, and $\Gamma\backslash\mathcal{H} \cong \mathbb{P}^1(\mathbb{C})$ (here $\mathcal{H}=$ upper half plane).
- The subgroup $\Gamma(2) \subset \Gamma$ consisting of matrices $\equiv \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ mod 2 yields a quotient $\Gamma(2)\backslash\mathcal{H}$ of genus 7. It has automorphisms $\Gamma/\Gamma(2) \cong \mathsf{PSL}_2(\mathbb{F}_8)$.
- More generally (Shimura), for any maximal ideal $\mathfrak{p} \subset \mathbb{Z}[\gamma]$, the corresponding $\Gamma(\mathfrak{p})$ of matrices $\equiv \pm\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ mod $\mathfrak{p}$ yields $\Gamma(\mathfrak{p})\backslash\mathcal{H}$ of genus g with automorphism group $\mathsf{PSL}_2(\mathbb{Z}[\gamma]/\mathfrak{p})$ of order $84(g-1)$.

A curve of genus $g \geq 2$ having $84(g-1)$ automorphisms is called *Hurwitz curve*.

A curve of genus $g \geq 2$ having $84(g-1)$ automorphisms is called *Hurwitz curve*.

A Hurwitz curve C with automorphism group G is a Galois cover of $\mathbb{P}^1$ of degree $\#G$, ramified over only 3 points. The ramification index over these points is $2, 3, 7$, respectively.

A curve of genus $g \geq 2$ having $84(g-1)$ automorphisms is called *Hurwitz curve*.

A Hurwitz curve C with automorphism group G is a Galois cover of $\mathbb{P}^1$ of degree $\#G$, ramified over only 3 points. The ramification index over these points is $2, 3, 7$, respectively.

Smallest example: $G = \mathrm{PSL}_2(\mathbb{F}_7)$. The unique Hurwitz curve of genus $1 + (\#G)/84 = 3$ is the famous Klein quartic, studied both as a Riemann surface and as an algebraic curve by F. Klein (1879, Math. Annalen **14**).

Next smallest example: $G = \mathrm{PSL}_2(\mathbb{F}_8)$, of order 504, so $g = 7$.

Next smallest example: $G = \mathrm{PSL}_2(\mathbb{F}_8)$, of order 504, so $g = 7$.

The unique Riemann surface of genus 7 with this automorphism group was studied by R. Fricke, 1899, Math. Annalen **52**; see also Shimura's 1967 paper discussed above.

Next smallest example: $G = \mathrm{PSL}_2(\mathbb{F}_8)$, of order 504, so $g = 7$.

The unique Riemann surface of genus 7 with this automorphism group was studied by R. Fricke, 1899, Math. Annalen **52**; see also Shimura's 1967 paper discussed above.

The first to publish an algebraic model of this $g = 7$ example, was the Scottish mathematician A.M. (Murray) Macbeath, 1965, Proc. LMS **15**. We call this *the Fricke-Macbeath curve*.

Alexander Murray Macbeath, 1923–2014.

Idea of Macbeath: In $\mathrm{PGL}_7(\mathbb{Q}) \subset \mathrm{Aut}(\mathbb{P}^6)$, the elements $T =$

$$\begin{pmatrix} -1 & 0 & 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 & -1 \\ 0 & 1 & -1 & 1 & 0 & 1 & 0 \\ -1 & -1 & -1 & 0 & -1 & 0 & 0 \\ -1 & 1 & 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 & -1 & -1 & -1 \end{pmatrix}, \ W = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

satisfy $T^3 = W^7 = (TW)^2 = id$ and they generate a group $\cong \mathrm{PSL}_2(\mathbb{F}_8)$.
So any curve in $\mathbb{P}^6$ fixed by T and W will have an automorphism group containing $\mathrm{PSL}_2(\mathbb{F}_8)$.

Macbeath constructs a canonically embedded genus 7 curve with this property.

It is the zero locus of

$$
\begin{aligned}
&x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2, \\
&x_0^2 + \zeta x_1^2 + \zeta^2 x_2^2 + \zeta^3 x_3^2 + \zeta^4 x_4^2 + \zeta^5 x_5^2 + \zeta^6 x_6^2, \\
&x_0^2 + \zeta^6 x_1^2 + \zeta^5 x_2^2 + \zeta^4 x_3^2 + \zeta^3 x_4^2 + \zeta^2 x_5^2 + \zeta x_6^2, \\
&\left(\zeta^5 - \zeta^2\right) x_1 x_4 + \left(\zeta^6 - \zeta\right) x_3 x_5 + \left(-\zeta^4 + \zeta^3\right) x_0 x_6, \\
&\left(-\zeta^4 + \zeta^3\right) x_0 x_1 + \left(\zeta^5 - \zeta^2\right) x_2 x_5 + \left(\zeta^6 - \zeta\right) x_4 x_6, \\
&\left(-\zeta^4 + \zeta^3\right) x_1 x_2 + \left(\zeta^6 - \zeta\right) x_0 x_5 + \left(\zeta^5 - \zeta^2\right) x_3 x_6, \\
&\left(-\zeta^4 + \zeta^3\right) x_2 x_3 + \left(\zeta^5 - \zeta^2\right) x_0 x_4 + \left(\zeta^6 - \zeta\right) x_1 x_6, \\
&\left(\zeta^6 - \zeta\right) x_0 x_2 + \left(-\zeta^4 + \zeta^3\right) x_3 x_4 + \left(\zeta^5 - \zeta^2\right) x_1 x_5, \\
&\left(\zeta^6 - \zeta\right) x_1 x_3 + \left(-\zeta^4 + \zeta^3\right) x_4 x_5 + \left(\zeta^5 - \zeta^2\right) x_2 x_6, \\
&\left(\zeta^5 - \zeta^2\right) x_0 x_3 + \left(\zeta^6 - \zeta\right) x_2 x_4 + \left(-\zeta^4 + \zeta^3\right) x_5 x_6.
\end{aligned}
$$

Here as earlier $\zeta = e^{2\pi i/7}$.

This model is defined over $\mathbb{Q}(\zeta)$.

More accurately: denoting the defining ideal by I, then $I \cap \mathbb{Q}[x_0, x_1, \ldots, x_6]$ defines (over $\mathbb{Q}(\zeta)$) the union of three (Galois conjugate, isomorphic) algebraic curves.

This model is defined over $\mathbb{Q}(\zeta)$.

More accurately: denoting the defining ideal by I, then $I \cap \mathbb{Q}[x_0, x_1, \ldots, x_6]$ defines (over $\mathbb{Q}(\zeta)$) the union of three (Galois conjugate, isomorphic) algebraic curves.

Since only one (up to isomorphism!) Hurwitz curve of genus 7 exists, an obvious problem is to look for a model defined over $\mathbb{Q}$. It exists, and to find one is an exercise in explicit Galois descent (from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}$):

Theorem

(Maxim Hendriks, PhD thesis, Eindhoven Univ., 2013)

A model of the Fricke-Macbeath $/\mathbb{Q}$ is defined by the polynomials

$$
\begin{aligned}
&-x_1x_2 + x_1x_0 + x_2x_6 + x_3x_4 - x_3x_5 - x_3x_0 - x_4x_6 - x_5x_6,\\
&x_1x_3 + x_1x_6 - x_2^2 + 2x_2x_5 + x_2x_0 - x_3^2 + x_4x_5 - x_4x_0 - x_5^2,\\
&x_1^2 - x_1x_3 + x_2^2 - x_2x_4 - x_2x_5 - x_2x_0 - x_3^2 + x_3x_6 + 2x_5x_0 - x_0^2,\\
&x_1x_4 - 2x_1x_5 + 2x_1x_0 - x_2x_6 - x_3x_4 - x_3x_5 + x_5x_6 + x_6x_0,\\
&x_1^2 - 2x_1x_3 - x_2^2 - x_2x_4 - x_2x_5 + 2x_2x_0 + x_3^2 + x_3x_6 + x_4x_5 + x_5^2 - x_5x_0 - x_6^2,\\
&x_1x_2 - x_1x_5 - 2x_1x_0 + 2x_2x_3 - x_3x_0 - x_5x_6 + 2x_6x_0,\\
&-2x_1x_2 - x_1x_4 - x_1x_5 + 2x_1x_0 + 2x_2x_3 - 2x_3x_0 + 2x_5x_6 - x_6x_0,\\
&2x_1^2 + x_1x_3 - x_1x_6 + 3x_2x_0 + x_4x_5 - x_4x_0 - x_5^2 + x_6^2 - x_0^2,\\
&2x_1^2 - x_1x_3 + x_1x_6 + x_2^2 + x_2x_0 + x_3^2 - 2x_3x_6 + x_4x_5 - x_4x_0 + x_5^2 - 2x_5x_0 + x_6^2 + x_0^2,\\
&x_1^2 + x_1x_3 - x_1x_6 + 2x_2x_5 - 3x_2x_0 + 2x_3x_6 + x_4^2 + x_4x_5 - x_4x_0 + x_6^2 + 3x_0^2.
\end{aligned}
$$

A beautiful alternative way to construct a model of the Fricke-Macbeath curve, was proposed by J-P. Serre in a July 1990 letter to S.S. Abhyankar:

A beautiful alternative way to construct a model of the Fricke-Macbeath curve, was proposed by J-P. Serre in a July 1990 letter to S.S. Abhyankar:

- $\mathrm{PSL}_2(\mathbb{F}_8)$ permutes the set $\mathbb{P}^1(\mathbb{F}_8)$ transitively.

A beautiful alternative way to construct a model of the Fricke-Macbeath curve, was proposed by J-P. Serre in a July 1990 letter to S.S. Abhyankar:

- $\mathrm{PSL}_2(\mathbb{F}_8)$ permutes the set $\mathbb{P}^1(\mathbb{F}_8)$ transitively.
- Hence the stabilizer of any point in this set is a subgroup H of index 9.

A beautiful alternative way to construct a model of the Fricke-Macbeath curve, was proposed by J-P. Serre in a July 1990 letter to S.S. Abhyankar:

- $\mathrm{PSL}_2(\mathbb{F}_8)$ permutes the set $\mathbb{P}^1(\mathbb{F}_8)$ transitively.
- Hence the stabilizer of any point in this set is a subgroup H of index 9.
- The quotient of the curve by H has genus 0, hence one obtains a Belyi map $\beta: \mathbb{P}^1 \to \mathbb{P}^1$ of degree 9.

A beautiful alternative way to construct a model of the Fricke-Macbeath curve, was proposed by J-P. Serre in a July 1990 letter to S.S. Abhyankar:

- $\mathrm{PSL}_2(\mathbb{F}_8)$ permutes the set $\mathbb{P}^1(\mathbb{F}_8)$ transitively.
- Hence the stabilizer of any point in this set is a subgroup H of index 9.
- The quotient of the curve by H has genus 0, hence one obtains a Belyi map $\beta : \mathbb{P}^1 \to \mathbb{P}^1$ of degree 9.
- The Fricke-Macbeath curve is the normal closure (geometrically) of this covering.

A beautiful alternative way to construct a model of the Fricke-Macbeath curve, was proposed by J-P. Serre in a July 1990 letter to S.S. Abhyankar:

- $\mathrm{PSL}_2(\mathbb{F}_8)$ permutes the set $\mathbb{P}^1(\mathbb{F}_8)$ transitively.
- Hence the stabilizer of any point in this set is a subgroup H of index 9.
- The quotient of the curve by H has genus 0, hence one obtains a Belyi map $\beta : \mathbb{P}^1 \to \mathbb{P}^1$ of degree 9.
- The Fricke-Macbeath curve is the normal closure (geometrically) of this covering.
- The ramification of the degree 9 map is as follows: one point with $e = 7$ over ∞, three points with $e = 3$ over 0, and four points with $e = 2$ over 1.

A beautiful alternative way to construct a model of the Fricke-Macbeath curve, was proposed by J-P. Serre in a July 1990 letter to S.S. Abhyankar:

- $\mathrm{PSL}_2(\mathbb{F}_8)$ permutes the set $\mathbb{P}^1(\mathbb{F}_8)$ transitively.
- Hence the stabilizer of any point in this set is a subgroup H of index 9.
- The quotient of the curve by H has genus 0, hence one obtains a Belyi map $\beta : \mathbb{P}^1 \to \mathbb{P}^1$ of degree 9.
- The Fricke-Macbeath curve is the normal closure (geometrically) of this covering.
- The ramification of the degree 9 map is as follows: one point with $e = 7$ over ∞, three points with $e = 3$ over 0, and four points with $e = 2$ over 1.
- This determines the map β as

$$x \mapsto \beta(x) := (x^3 + 4x^2 + 10x + 6)^3/(27x^2 + \frac{351}{4}x + 216).$$

Note (as remarked by Serre) that $\mathbb{Q}$ is not algebraically closed in the normal closure of $\mathbb{Q}(x)/\mathbb{Q}(\beta(x))$.

So Serre's construction does not define a model over $\mathbb{Q}$ of the Fricke-Macbeath.

Note (as remarked by Serre) that $\mathbb{Q}$ is not algebraically closed in the normal closure of $\mathbb{Q}(x)/\mathbb{Q}(\beta(x))$.

So Serre's construction does not define a model over $\mathbb{Q}$ of the Fricke-Macbeath.

An alternative simple model which *is* over $\mathbb{Q}$, was discovered by Bradley Brock ($\approx$ 2013): the normalization of the plane curve given by

$$1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0$$

is a model of the Fricke-Macbeath curve.

To see that this is correct:

To see that this is correct:

- The plane curve has degree 8;

To see that this is correct:

- The plane curve has degree 8;
- The singular locus consists of 14 ODP's; one orbit under the action of $(x, y) \mapsto (y, x)$ and $(x, y) \mapsto (\zeta^n x, \zeta^{-n} y)$.

To see that this is correct:

- The plane curve has degree 8;
- The singular locus consists of 14 ODP's; one orbit under the action of $(x, y) \mapsto (y, x)$ and $(x, y) \mapsto (\zeta^n x, \zeta^{-n} y)$.
- (In fact: this holds in every characteristic $\neq 2, 7$.)

To see that this is correct:

- The plane curve has degree 8;
- The singular locus consists of 14 ODP's; one orbit under the action of $(x, y) \mapsto (y, x)$ and $(x, y) \mapsto (\zeta^n x, \zeta^{-n} y)$.
- (In fact: this holds in every characteristic $\neq 2, 7$.)
- Hence genus $(8-1)(8-2)/2 - 14 = 7$.

To see that this is correct:

- The plane curve has degree 8;
- The singular locus consists of 14 ODP's; one orbit under the action of $(x, y) \mapsto (y, x)$ and $(x, y) \mapsto (\zeta^n x, \zeta^{-n} y)$.
- (In fact: this holds in every characteristic $\neq 2, 7$.)
- Hence genus $(8-1)(8-2)/2 - 14 = 7$.
- To verify the curve is indeed isomorphic to the Fricke-Macbeath, compute its canonical embedding:

Defining ideal of Brock's model, canonically embedded:

$$
\begin{aligned}
&x_0x_2 + 12x_3^2 - x_4x_6,\\
&-x_1^2 + x_0x_3 - 2x_5x_6,\\
&x_0x_4 + 16x_3x_5 + 8x_6^2,\\
&-x_1x_3 + x_0x_5 + \tfrac{1}{2}x_2x_6,\\
&-x_2x_3 + 2x_5^2 + x_0x_6,\\
&x_1x_2 + 12x_3x_5 + 4x_6^2,\\
&-2x_2x_3 + x_1x_4 - 8x_5^2,\\
&-x_3^2 + x_1x_5 + \tfrac{1}{4}x_4x_6,\\
&-\tfrac{1}{2}x_3x_4 - \tfrac{1}{2}x_2x_5 + x_1x_6,\\
&x_2^2 + 2x_4x_5 + 8x_3x_6.
\end{aligned}
$$

Defining ideal of Brock's model, canonically embedded:

$$
\begin{aligned}
&x_0x_2 + 12x_3^2 - x_4x_6,\\
&-x_1^2 + x_0x_3 - 2x_5x_6,\\
&x_0x_4 + 16x_3x_5 + 8x_6^2,\\
&-x_1x_3 + x_0x_5 + \tfrac{1}{2}x_2x_6,\\
&-x_2x_3 + 2x_5^2 + x_0x_6,\\
&x_1x_2 + 12x_3x_5 + 4x_6^2,\\
&-2x_2x_3 + x_1x_4 - 8x_5^2,\\
&-x_3^2 + x_1x_5 + \tfrac{1}{4}x_4x_6,\\
&-\tfrac{1}{2}x_3x_4 - \tfrac{1}{2}x_2x_5 + x_1x_6,\\
&x_2^2 + 2x_4x_5 + 8x_3x_6.
\end{aligned}
$$

Using that a linear isomorphism between the two given canonical models over $\mathbb{Q}$ conjugates the known automorphisms, it is not hard to find one explicitly. There exists one over $\mathbb{Q}(\sqrt{-7})$, not over $\mathbb{Q}$.

Corollary

The canonical curves over $\mathbb{Q}$ described by Hendriks and by Brock both have good reduction at every prime $p \neq 2, 7$.

Corollary

The canonical curves over $\mathbb{Q}$ described by Hendriks and by Brock both have good reduction at every prime $p \neq 2, 7$.

Proof: we observed this for Brock's model; since the models are isomorphic over $\mathbb{Q}(\sqrt{-7})$ and this field only ramifies at 7, it is true for the other model as well.

One more algebraic model, over $\mathbb{Q}(\zeta)$, described by A.M. Macbeath and by Everett Howe:

the Fricke-Macbeath curve is the $(\mathbb{Z}/2\mathbb{Z})^3$-cover of $\mathbb{P}^1$ defined by

$$\begin{cases} u^2 = (x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^4), \\ v^2 = (x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^5), \\ w^2 = (x-\zeta^2)(x-\zeta^3)(x-\zeta^4)(x-\zeta^6). \end{cases}$$

Using the Macbeath/Howe model, visibly the function field of the Fricke-Macbeath curve contains 7 elliptic subfields (namely, the ones generated over $\mathbb{C}(x)$ by respectively u, v, w, uv, uw, vw, and uvw; they correspond to the 7 subgroups of $(\mathbb{Z}/2\mathbb{Z})^3$ of index 2).

Using the Macbeath/Howe model, visibly the function field of the Fricke-Macbeath curve contains 7 elliptic subfields (namely, the ones generated over $\mathbb{C}(x)$ by respectively u, v, w, uv, uw, vw, and uvw; they correspond to the 7 subgroups of $(\mathbb{Z}/2\mathbb{Z})^3$ of index 2).

More precisely, in this way one verifies that over $\mathbb{Q}(\zeta)$ the Jacobian of this curve is isogenous to a product of 7 elliptic curves.

Moreover, the elliptic curves can be taken to be isomorphic over $\mathbb{Q}(\zeta)$.
(At least over $\mathbb{C}$, this result is attributed to Kevin Berry and Marvin Tretkoff, 1990.)

To describe the Jacobian of a Fricke-Macbeath model over $\mathbb{Q}$, we start from the description given by Hendriks. Denote this curve by H.

To describe the Jacobian of a Fricke-Macbeath model over $\mathbb{Q}$, we start from the description given by Hendriks. Denote this curve by H.

Consider the curve X of genus 3 defined as $X = \pi(H)$, the image of H under $\pi : (x_0 : x_1 : x_2 : x_3 : x_4 : x_5 : x_6) \mapsto (x_0 : x_2 : x_5)$.

Equation for X:

$$
\begin{aligned}
&5x^4 + 12x^3y + 6x^2y^2 - 4xy^3 + 4y^4 - 28x^3z + 16x^2yz \\
&-24xy^2z + 16y^3z + 24x^2z^2 - 10y^2z^2 - 12xz^3 + 8yz^3 + 3z^4 = 0
\end{aligned}
$$

The genus 3 curve X inherits from H a group of automorphisms $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The involutions in this group are defined over $\mathbb{Q}(\zeta + \zeta^{-1})$. The quotient by such an involution is a genus one curve over this field, with Jacobian an elliptic curve E'.

The genus 3 curve X inherits from H a group of automorphisms $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The involutions in this group are defined over $\mathbb{Q}(\zeta + \zeta^{-1})$. The quotient by such an involution is a genus one curve over this field, with Jacobian an elliptic curve E'.

Corollary: $\mathrm{Jac}(X)$ *is isogenous over* $\mathbb{Q}$ *to* $\mathrm{Res}_{\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}} E'$.

The genus 3 curve X inherits from H a group of automorphisms $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The involutions in this group are defined over $\mathbb{Q}(\zeta + \zeta^{-1})$. The quotient by such an involution is a genus one curve over this field, with Jacobian an elliptic curve E'.

Corollary: $\mathrm{Jac}(X)$ *is isogenous over* $\mathbb{Q}$ *to* $\mathrm{Res}_{\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}} E'$.

Using an appropriate $\iota \in \mathrm{Aut}(H)$ and

$$(\pi, \pi \circ \iota) : H \to X \times X$$

one shows:

Lemma: *There is an elliptic curve* $E/\mathbb{Q}$ *such that* $\mathrm{Jac}(H)$ *is isogenous over* $\mathbb{Q}$ *to* $E \times \mathrm{Res}_{\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}} E' \times \mathrm{Res}_{\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}} E'$.

Two ways to determine such $E/\mathbb{Q}$:

Two ways to determine such $E/\mathbb{Q}$:

(1). It turns out that $\mathrm{Aut}(H)$ contains an element of order 3 defined over $\mathbb{Q}$. The quotient has genus 1, and the Jacobian of this curve is the desired E.

Two ways to determine such $E/\mathbb{Q}$:

(1). It turns out that $\mathrm{Aut}(H)$ contains an element of order 3 defined over $\mathbb{Q}$. The quotient has genus 1, and the Jacobian of this curve is the desired E.

(2). Since H has good reduction away from $2, 7$, so has E. Moreover, over any finite field $\mathbb{F}_q$ of characteristic $\neq 2, 7$, we have

$$\#E(\mathbb{F}_q) = 2q + 2 + \#H(\mathbb{F}_q) - 2\#X(\mathbb{F}_q).$$

Using this it is easy to find an E as desired.

Result: E given by $y^2 = x^3 + x^2 - 114x - 127$ works. (Conductor 14^2, j-invariant $1792 = 2^8 \cdot 7$, no CM!)

A small computation shows (no great surprise, given the Macbeath/Howe model): *the elliptic curves E' and E are isogenous over $\mathbb{Q}(\zeta + \zeta^{-1})$.* Hence:

Main Theorem: *For any finite field $\mathbb{F}_q$ of characteristic $\neq 2, 7$ one has*

$$\#H(\mathbb{F}_q) = \begin{cases} \#E(\mathbb{F}_q) & \text{if } q \not\equiv \pm 1 \bmod 7; \\ 7\#E(\mathbb{F}_q) - 6q - 6 & \text{if } q \equiv \pm 1 \bmod 7. \end{cases}$$

Example: $\#H(\mathbb{F}_{27}) = 84$. This improves a previous record found in 2000 by Stéphan Sémirat, see the website `manypoints.org` maintained by Gerard van der Geer, Everett W. Howe, Kristin E. Lauter, and Christophe Ritzenthaler.

We have several such examples, often involving twists by elements of $H^1(\mathrm{Gal}_{\mathbb{F}_q}, Aut(H \otimes \overline{\mathbb{F}_q}))$.

Example: $\#H(\mathbb{F}_{27}) = 84$. This improves a previous record found in 2000 by Stéphan Sémirat, see the website `manypoints.org` maintained by Gerard van der Geer, Everett W. Howe, Kristin E. Lauter, and Christophe Ritzenthaler.

We have several such examples, often involving twists by elements of $H^1(\mathrm{Gal}_{\mathbb{F}_q}, Aut(H \otimes \overline{\mathbb{F}_q}))$.

Easy: p supersingular, then H is maximal over $\mathbb{F}_{p^2}$. This occurs for 71, 251, 503, 2591, 3527, 5867, 7307, 20663, ...

Motivated by the Fricke-Macbeath example:

- Everett Howe this summer searched over finite fields for tuples $(a_0, \ldots, a_6) \in \mathbb{F}_q^7$ defining a genus 7 curve

$$\begin{cases} u^2 = (x - a_0)(x - a_1)(x - a_2)(x - a_4), \\ v^2 = (x - a_1)(x - a_2)(x - a_3)(x - a_5), \\ w^2 = (x - a_2)(x - a_3)(x - a_4)(x - a_6) \end{cases}$$

  with many rational points.

  For example, $u^2 = 2x^3 + 11x, v^2 = x^3 + 11x^2 + 3, w^2 = x^3 + x$ defines the current record over $\mathbb{F}_{13}$, having 52 rational points.

- Observing that the Fricke-Macbeath curve is a double cover of a smooth plane quartic, Carlo Verschoor and I searched for more such double covers:

- Observing that the Fricke-Macbeath curve is a double cover of a smooth plane quartic, Carlo Verschoor and I searched for more such double covers:

  Starting from a smooth plane quartic X and points $P, Q \in X$, consider the tangent lines $L = 0$ resp. $M = 0$ at these points, and the function $f := L/M$ on X.

- Observing that the Fricke-Macbeath curve is a double cover of a smooth plane quartic, Carlo Verschoor and I searched for more such double covers:

  Starting from a smooth plane quartic X and points $P, Q \in X$, consider the tangent lines $L = 0$ resp. $M = 0$ at these points, and the function $f := L/M$ on X.

  The double cover of X defined by $\sqrt{f}$ is the curve we consider.

- Observing that the Fricke-Macbeath curve is a double cover of a smooth plane quartic, Carlo Verschoor and I searched for more such double covers:

  Starting from a smooth plane quartic X and points $P, Q \in X$, consider the tangent lines $L = 0$ resp. $M = 0$ at these points, and the function $f := L/M$ on X.

  The double cover of X defined by $\sqrt{f}$ is the curve we consider.

  Example: $c, u \in \mathbb{F}_{17^2}$ with $c^2 + 3c + 1 = 0$, $u^2 - u + 3 = 0$.
  Plane quartic defined by $x^4 + y^4 + z^4 + c(x^2y^2 + x^2z^2 + y^2z^2)$.
  (Bi)tangent $x + u^{188}y - z = 0$ and $-x - y + u^{44}z = 0$.
  This results in a genus 5 curve C reaching the
  Hasse-Weil-Serre upper bound:
  $\#C(\mathbb{F}_{289}) = 460 = 17^2 + 1 + 10 \cdot 17$.

Congratulations to Noriko,
for being today
back into prime age . . .