CM genus 3 curves over $\mathbb{Q}$

Christophe Ritzenthaler (Rennes 1)

Banff, May 2017

An $A + B + C + D + E + F + G$ article

Pınar Kılıçer
Hugo Labrande
Reynald Lercier
Jeroen Sijsling
Marco Streng

Goal: explicit (and short) equations of all genus 3 curves over $\mathbb{Q}$ with trivial automorphism group and CM by the maximal order.

1. The list of possible (Galois) CM fields (Kılıçer and Streng);
2. Obtain the Riemann matrix (folklore + improvements);
3. Compute the Thetanullwerte (fast algorithms from Labrande);
4. Compute a model of the curve over $\mathbb{C}$ (formulas from Weber);
5. Compute the Dixmier-Ohno invariants and recognize them as rational numbers ;
6. Reconstruct the curve from its invariants (Lercier-R.-Sijsling + improvements);
7. Reduce the size of the coefficients (Stoll, Elsenhans).

Goal: explicit (and short) equations of all genus 3 curves over $\mathbb{Q}$ with trivial automorphism group and CM by the maximal order.

1. The list of possible (Galois) CM fields (Kılıçer and Streng);
2. Obtain the Riemann matrix (folklore + improvements);
3. Compute the Thetanullwerte (fast algorithms from Labrande);
4. Compute a model of the curve over $\mathbb{C}$ (formulas from Weber);
5. Compute the Dixmier-Ohno invariants and recognize them as rational numbers ;
6. Reconstruct the curve from its invariants (Lercier-R.-Sijsling + improvements);
7. Reduce the size of the coefficients (Stoll, Elsenhans).

Similar works: genus 2 (van Wamelen 1999 + Bisson-Streng 2015), genus 3 hyperelliptic (Weng 2001 + Balakrishnan et al. 2016), Picard curves $y^3 = f(x)$ (Koike-Weng 2005 + Lario-Somoza 2016).

Some examples

$$
\begin{aligned}
X_1 : & -4169\,x^4 - 956\,x^3y + 7440\,x^3z + 55770\,x^2y^2 \\
& + 43486\,x^2y\,z + 42796\,x^2z^2 - 38748\,x\,y^3 - 30668\,x\,y^2z \\
& + 79352\,x\,y\,z^2 - 162240\,x\,z^3 + 6095\,y^4 + 19886\,y^3z \\
& - 89869\,y^2z^2 - 1079572\,y\,z^3 - 6084\,z^4 = 0, \\
X_9 : & \ 96128\,x^4 + 232804\,x^3y + 5588\,x^3z + 51333\,x^2y^2 \\
& - 37020\,x^2y\,z - 5791396\,x^2z^2 - 108416\,x\,y^3 - 49056\,x\,y^2z \\
& - 6947226\,x\,y\,z^2 - 214292\,x\,z^3 - 5880\,y^4 - 581812\,y^3z \\
& + 2438436\,y^2z^2 + 1944852\,y\,z^3 + 87102093\,z^4 = 0 \\
X_{15} : & \ x^4 - x^3y + 2\,x^3z + 2\,x^2y\,z + 2\,x^2z^2 - 2\,x\,y^2z \\
& + 4\,x\,y\,z^2 - y^3z + 3\,y^2z^2 + 2\,y\,z^3 + z^4 = 0.
\end{aligned}
$$

Remark: the result is conjectural except for some examples (work in progress by Sijsling).

The list of possible cases

Theorem (Kılıçer and Streng 2016)

There are exactly 37 isomorphism classes of CM fields K for which there exist principally polarized abelian threefolds $A/\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ and $End(A) \simeq \mathcal{O}_K$.

The list of possible cases

Theorem (Kılıçer and Streng 2016)

There are exactly 37 isomorphism classes of CM fields K for which there exist principally polarized abelian threefolds $A/\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ and $End(A) \simeq \mathcal{O}_K$.

Case	$-d_k$	p_F	f_F	$-d_K$	#	Type
1	7	X^3+X^2-4X+1	13	$7^3 \cdot 13^4$	2	G
2	7	X^3-3X-1	3^2	$3^8 \cdot 7^3$	2	G
3	7	$X^3+8X^2-51X+27$	$7 \cdot 31$	$7^5 \cdot 31^4$	2	G
4	7	X^3+6X^2-9X+1	$3^2 \cdot 7$	$3^8 \cdot 7^5$	2	H
36	7	X^3+X^2-2X-1	7	7^5	14	H
37	3	X^3-3X-1	3^2	3^9	18	P

k: imaginary quadratic subfield of discriminant d_k

F: totally real cubic subfield with minimal polynomial p_F, conductor f_F

Computation of the Riemann matrix (van Wamelen, Shimura-Taniyama, Streng)

1. Let Φ be a CM-type for K, seen as a map $K \to \mathbb{C}^3$;
2. Let $\zeta \in K$ a generator of $\mathcal{D}_{K/\mathbb{Q}}^{-1}$ such that $\phi(\zeta)$ has a positive imaginary part for all $\phi \in \Phi$;
3. Then

$$E(\Phi(\alpha), \Phi(\beta)) = \mathrm{Tr}_{K/\mathbb{Q}}(\zeta \alpha \bar{\beta}), \quad \alpha, \beta \in K$$

   defines a principal polarization on $\mathbb{C}^3/\Phi(\mathcal{O}_K)$.
4. Deduce a Riemann matrix τ;
5. Reduce it to a fundamental domain $\mathcal{F}$? Not known but an algorithm to $\mathcal{F}_3(\{N\}) \supset \mathcal{F}$.

Computation of Thetanullwerte

$$\vartheta_i = \vartheta_{[a;b]}(\tau) = \sum_{n \in \mathbb{Z}^3} e^{i\pi({}^t(n+a)\tau(n+a)+2^t(n+a)b)}$$

with $i = 2(b_0 + 2b_1 + 4b_2) + 2^4(a_0 + 2a_1 + 4a_2)$.

Proposition

Let S_B be the partial summation of ϑ_0 with indices in $[-B, B]^3$. For $\tau \in \mathcal{F}_3(\{N\})$ and $c \geq \sqrt{3}/200$, we have

$$|\vartheta_0(\tau) - S_B| \leq 24 \left(\pi c e^{-\pi c}\right)^3 \times e^{-\pi c B^2}.$$

Taking $B = O\left(\sqrt{P}\right)$ is enough to ensure that S_B is within 10^{-P} of ϑ_0.

Fast naive algorithm (Labrande 2016)

Fast naive algorithm: Let $q_{jk} = e^{i\pi\tau_{jk}}$ and

$$t_{m,n,p} = e^{i\pi(m,n,p)\tau^t(m,n,p)}.$$

Then we have the following recursion relations:

$$\begin{aligned} t_{m+1,n,p} &= t_{m,n,p} q_{11}^{2m} q_{11} q_{12}^{2n} q_{13}^{2p} \\ t_{m,n+1,p} &= t_{m,n,p} q_{22}^{2n} q_{22} q_{12}^{2m} q_{23}^{2p} \\ t_{m,n,p+1} &= t_{m,n,p} q_{33}^{2p} q_{33} q_{23}^{2n} q_{13}^{2m} \end{aligned}$$

Complexity: $O(\mathcal{M}(P)P^{1.5})$ (450 digits in 20 seconds).

AGM style algorithm (after Dupont 2006)

Duplication formula

$$\vartheta_1(2\tau)^2 = \frac{\sqrt{\vartheta_0^2}\sqrt{\vartheta_1^2} + \sqrt{\vartheta_2^2}\sqrt{\vartheta_3^2} + \sqrt{\vartheta_4^2}\sqrt{\vartheta_5^2} + \sqrt{\vartheta_6^2}\sqrt{\vartheta_7^2}}{4}(\tau).$$

Borchardt mean

$$\mathcal{B}_3\left(1, \frac{\vartheta_1(\tau)^2}{\vartheta_0(\tau)^2}, \ldots, \frac{\vartheta_7(\tau)^2}{\vartheta_0(\tau)^2}\right) = \frac{1}{\vartheta_0(\tau)^2}.$$

$$f\left(\frac{\vartheta_1(\tau)^2}{\vartheta_0(\tau)^2}, \ldots, \frac{\vartheta_7(\tau)^2}{\vartheta_0(\tau)^2}\right) = (-i\tau_{11}, -i\tau_{22}, -i\tau_{33}, \tau_{12}^2 - \tau_{11}\tau_{22}, \tau_{13}^2 - \tau_{11}\tau_{33}, \tau_{23}^2 - \tau_{22}\tau_{33}).$$

Complexity: $O(\mathcal{M}(P)\log P)$ (2000 digits of precision in 10 seconds).

Model of the curve over $\mathbb{C}$ (Weber 1876)

$$a_{11} := i\frac{\vartheta_{33}\vartheta_5}{\vartheta_{40}\vartheta_{12}}, \quad a_{12} := i\frac{\vartheta_{21}\vartheta_{49}}{\vartheta_{28}\vartheta_{56}}, \quad a_{13} := i\frac{\vartheta_7\vartheta_{35}}{\vartheta_{14}\vartheta_{42}},$$
$$a_{21} := i\frac{\vartheta_5\vartheta_{54}}{\vartheta_{27}\vartheta_{40}}, \quad a_{22} := i\frac{\vartheta_{49}\vartheta_2}{\vartheta_{47}\vartheta_{28}}, \quad a_{23} := i\frac{\vartheta_{35}\vartheta_{16}}{\vartheta_{61}\vartheta_{14}},$$
$$a_{31} := -\frac{\vartheta_{54}\vartheta_{33}}{\vartheta_{12}\vartheta_{27}}, \quad a_{32} := \frac{\vartheta_2\vartheta_{21}}{\vartheta_{56}\vartheta_{47}}, \quad a_{33} := \frac{\vartheta_{16}\vartheta_7}{\vartheta_{42}\vartheta_{61}}.$$

The lines

$$x_1 = 0, x_2 = 0, x_3 = 0, x_1 + x_2 + x_3 = 0$$

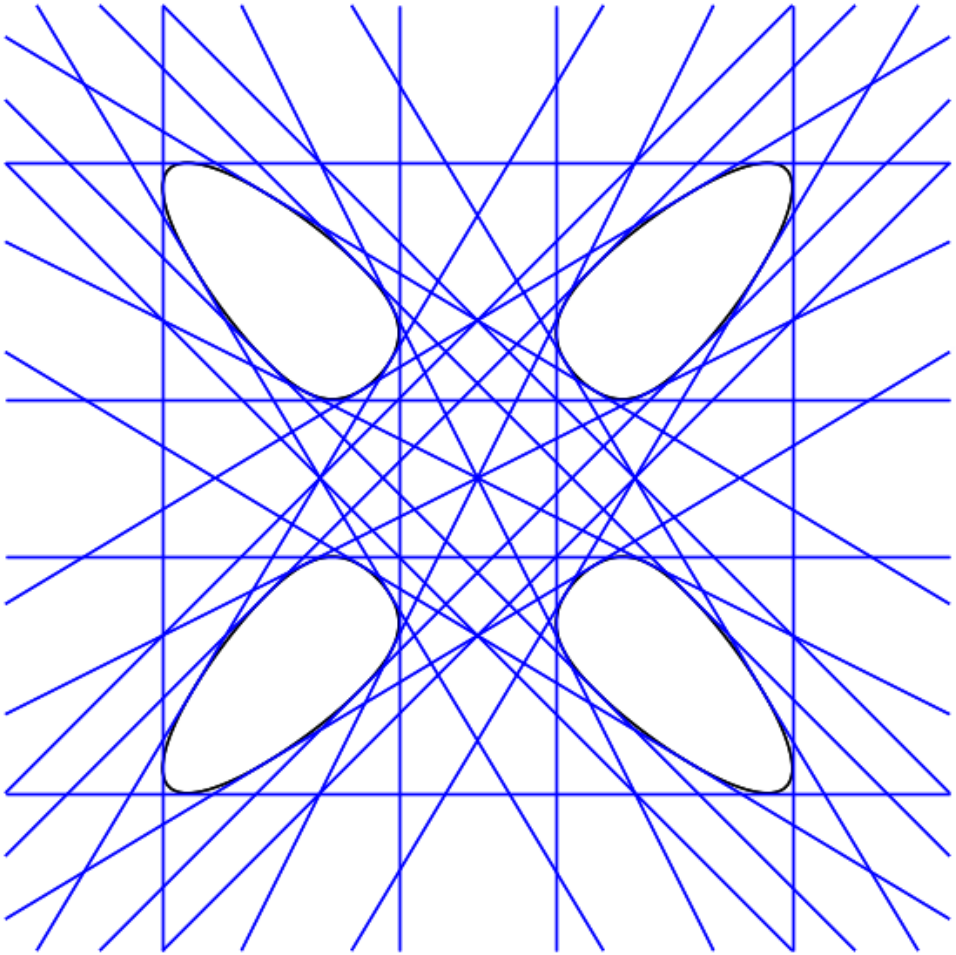
and

$$\ell_i : a_{1i}x_1 + a_{2i}x_2 + a_{3i}x_3 = 0$$

in $\mathbb{P}^2_{\mathbb{C}}$ form an *Aronhold system*.

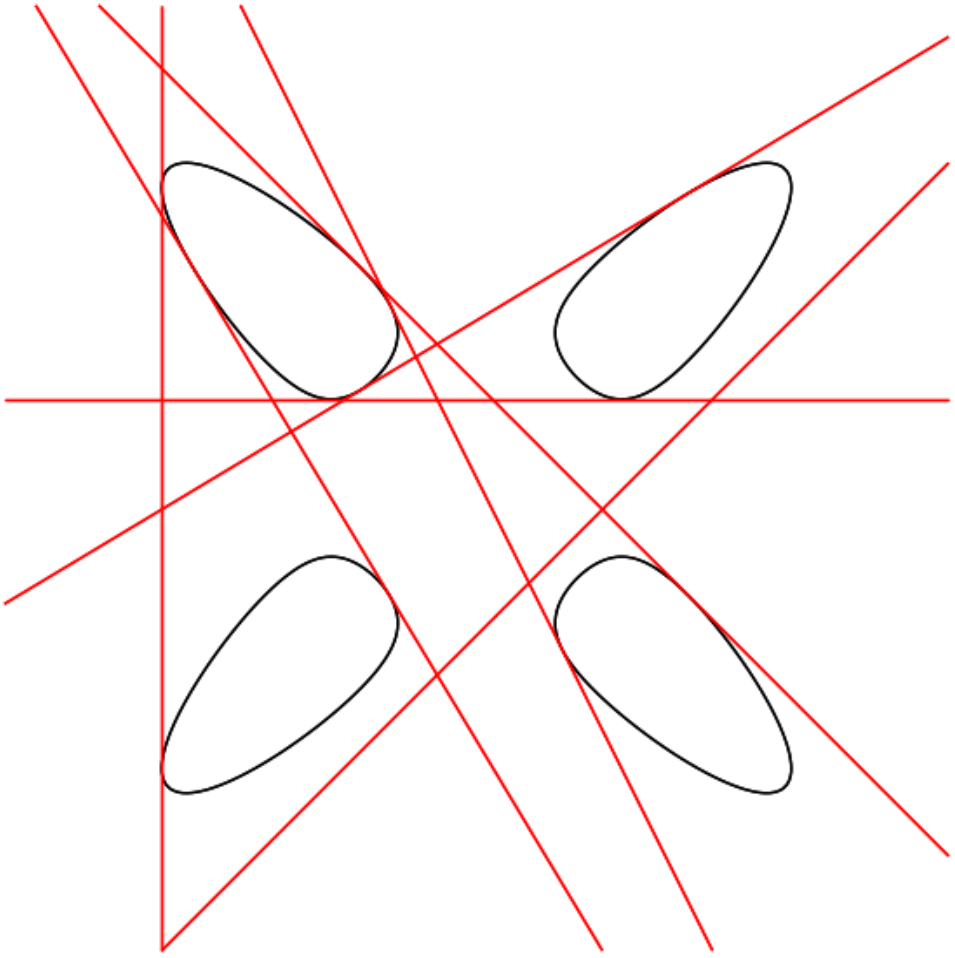
Edge quartic (Plaumann et al. 2011)

$$25(x^4 + y^4 + z^4) = 34(x^2y^2 + y^2z^2 + x^2z^2)$$



Edge quartic (Plaumann et al. 2011)

$$25(x^4 + y^4 + z^4) = 34(x^2y^2 + y^2z^2 + x^2z^2)$$



Define

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{a_{11}} & \frac{1}{a_{12}} & \frac{1}{a_{13}} \\ \frac{1}{a_{21}} & \frac{1}{a_{22}} & \frac{1}{a_{23}} \end{bmatrix}^{-1} \cdot \begin{bmatrix} 1 & 1 & 1 \\ a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}.$$

Then $X_{\mathbb{C}}$ is the curve defined by the equation

$$(x_1 u_1 + x_2 u_2 - x_3 u_3)^2 - 4 x_1 u_1 x_2 u_2 = 0.$$

Alternative: (Guardia 2009) using derivative of odd theta functions.

Computation of the invariants

Dixmier-Ohno invariants

$$\underline{I} = (I_3 : I_6 : I_9 : J_9 : I_{12} : J_{12} : I_{15} : J_{15} : I_{18} : J_{18} : I_{21} : J_{21} : I_{27})$$

are homogeneous expressions in the coefficients of $X_{\mathbb{C}}$ of degree

$$\underline{d} = (3, 6, 9, 9, 12, 12, 15, 15, 18, 18, 21, 21, 27).$$

$$\underline{I}^{\mathrm{norm}} = \left(1, \frac{I_6}{I_3^2}, \frac{I_9}{I_3^3}, \frac{J_6}{I_3^3}, \frac{I_{12}}{I_3^4}, \frac{J_{12}}{I_3^4}, \frac{I_{15}}{I_3^5}, \frac{J_{15}}{I_3^5}, \frac{I_{18}}{I_3^6}, \frac{J_{18}}{I_3^6}, \frac{J_{21}}{I_3^7}, \frac{J_{21}}{I_3^7}, \frac{I_{27}}{I_3^9}\right) \in \mathbb{Q}^{13}.$$

Use `BestApproximation` at less than 1000 decimal digits to observe convergence to a rational.

Reconstruction from the invariants

Problems: The basic reconstruction algorithm produces a quartic over a quadratic extension with huge coefficients

- Mestre reconstruction involves finding a rational point on a conic (which does not necessarily exists)
- A Shioda invariant of degree d is of degree $9d$ in the Dixmier-Ohno invariants
- The Galois descent blows up coefficients even more

The conic trick

- Mestre reconstruction algorithm starts with three (covariant) quadratic binary forms $q_1, q_2, q_3 \in k[x, z]$.
- Construct a conic C and a degree $g + 1$ curve H which intersections are the ramification points of the hyperelliptic curve.
- Clebsch's identity: $2 \cdot \mathrm{disc}(C) = \left(\det(q_1, q_2, q_3)_{(x^2, xz, z^2)}\right)^2$.
- Use another q_3' to minimize

$$\det(q_1, q_2, \lambda q_3 + \mu q_3') = \lambda \det(q_1, q_2, q_3) + \mu \det(q_1, q_2, q_3').$$

- Find the corresponding C and H with interpolation techniques.

Leads to big speed-ups to reconstruct a hyperelliptic curve in general. Here we observe that $\mathrm{disc}(C) \approx I_{12}$.

Descent over the field of moduli

Our quartic $X : F = 0$ over a quadratic extension $K/\mathbb{Q}$ has $\mathrm{Aut}(X) = \{\mathrm{Id}\}$.

- There exists $M \in \mathrm{PGL}_3(K)$ such that $F.M = F^\sigma$ up to a scalar (Van Rijnswou 2001).
- $MM^\sigma = \pi\,\mathrm{Id}$, $\pi \in \mathbb{Q}$.
- Let $M_0 = \frac{\pi}{\det(M)} \cdot M$. Then $M_0 M_0^\sigma = \mathrm{Id}$.
- Hilbert 90 to define a coboundary $N = R + MR^\sigma$, R random matrix in $\mathrm{GL}_3(K)$.
- $X_0 : F.N = 0$ is defined over $\mathbb{Q}$.

Problem: in general N is large and the primes dividing $\det(N)$ add to the discriminant of X_0.

In worst case, X_0 has 1500-digits coefficients. One needs to reduce further

1. use action of $\mathrm{GL}_3(\mathbb{Q})$ to minimize discriminant (Elsenhans 2016);
2. use action of $\mathrm{SL}_3(\mathbb{Q})$ to reduce the heights (Stoll 2011).

Complexity (heuristically): factorization of I_{12} and I_{27}.

Question: can we avoid (partially) the factorizations as in (Bouyer-Streng 2015) for hyperelliptic curves?

Primes dividing the discriminant

Primes of potentially good non-hyperelliptic reduction

$$X_9 : 96128\,x^4 + 232804\,x^3y + 5588\,x^3z + 51333\,x^2y^2 - 37020\,x^2y\,z - 5791396\,x^2z^2$$
$$- 108416\,x\,y^3 - 49056\,x\,y^2z - 6947226\,x\,y\,z^2 - 214292\,x\,z^3 - 5880\,y^4$$
$$- 581812\,y^3z + 2438436\,y^2z^2 + 1944852\,y\,z^3 + 87102093\,z^4 = 0$$

$$I_{27} = -2^{15} \cdot 5^{12} \cdot 7^{14} \cdot 13^{18} \cdot 79^{14} \cdot 233^{14} \cdot 857^{14}\,.$$

Primes dividing the discriminant

Primes of potentially good non-hyperelliptic reduction

$$X_9 : 96128\,x^4+232804\,x^3y+5588\,x^3z+51333\,x^2y^2-37020\,x^2y\,z-5791396\,x^2z^2 - 108416\,x\,y^3-49056\,x\,y^2z-6947226\,x\,y\,z^2-214292\,x\,z^3-5880\,y^4 - 581812\,y^3z+2438436\,y^2z^2+1944852\,y\,z^3+87102093\,z^4=0$$

$$I_{27} = -2^{15}\cdot 5^{12}\cdot 7^{14}\cdot 13^{18}\cdot 79^{14}\cdot 233^{14}\cdot 857^{14}\,.$$

Change of variables

$$x = \sqrt[3]{13}^2 x_1 + 5\sqrt[3]{13}x_2,\ y = \sqrt[3]{13}x_2,\ z = x_3$$

$$\begin{aligned} X_9 \simeq\ & -96128\,\sqrt[3]{13}^2\,x_1^4 - 2155364\,\sqrt[3]{13}\,x_1^3\,x_2 - 5588\,x_1^3\,x_3 - 17962593\,x_1^2\,x_2^2 \\ & - 3600\,\sqrt[3]{13}^2\,x_1^2\,x_2\,x_3 + 445492\,\sqrt[3]{13}\,x_1^2\,x_3^2 - 5071478\,\sqrt[3]{13}^2\,x_1\,x_2^3 \\ & + 12\,\sqrt[3]{13}\,x_1\,x_2^2\,x_3 + 4989322\,x_1\,x_2\,x_3^2 + 1268\,\sqrt[3]{13}^2\,x_1\,x_3^3 - 6916605\,\sqrt[3]{13}\,x_2^4 \\ & + 81084\,x_2^3\,x_3 + 1047826\,\sqrt[3]{13}^2\,x_2^2\,x_3^2 - 5168\,\sqrt[3]{13}\,x_2\,x_3^3 - 515397\,x_3^4 \\ =\ & 0 \end{aligned}$$

$$I_{27} = -2^{15}\cdot 5^{12}\cdot 7^{14}\cdot 79^{14}\cdot 233^{14}\cdot 857^{14}\,.$$

Criterion for potentially good reduction

Proposition

Let $A = \operatorname{Jac} C$ be an abelian variety over a number field k and suppose that A has CM by $\mathcal{O}_K$ for a sextic cyclic CM field K.
Let n be the number of prime factors of $p\mathcal{O}_K$.
If $n = 2, 6$, A is absolutely simple and C has potential good reduction.
If $n = 1, 3$ then A is supersingular.

For genus 2, this leads to the characterization of primes dividing the discriminant (Goren-Lauter 2007, Lauter-Viray 2015).

For genus 3, only an upper bound for the bad primes (Kılıçer et al. 2016) and an algorithm for the bad primes of Picard curves (Kılıçer et al. 2017).

Proving hyperelliptic reduction (Clemens 1980)

Proposition

Let $C : F = 0$ be an equation of a plane smooth quartic with coefficients in $\mathbb{Z}$ and p be a prime.
If $F = Q^2 + pG$ where, modulo p, $Q = 0$ is a smooth conic intersecting the quartic $G = 0$ in 8 distinct points then C has hyperelliptic reduction modulo p with equation $\{Q = 0, t^2 = G\}$.

Problem: this can happen after an extension:
$x^3y + y^3z + z^3x = 0$ is not of this form for $p = 7$ but the curve is isomorphic over $\mathbb{Q}(\sqrt{-7})$ to

$$(x^2 + y^2 + z^2)^2 + \sqrt{-7} \cdot \frac{3 + \sqrt{-7}}{2} \left(x^2y^2 + y^2z^2 + z^2x^2\right) = 0$$

Work in progress: characterization in terms of valuations of invariants.