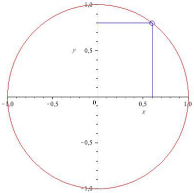
HDR defense

Christophe Ritzenthaler

Institut de Mathématiques de Luminy, CNRS

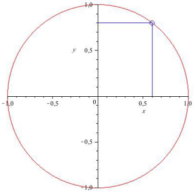
December 2, 2009

L'approche classique : genre $0, 1, 2$ et 3



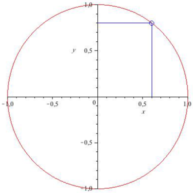
genre 0 $x^2 + y^2 = 1$

L'approche classique : genre 0, 1, 2 et 3

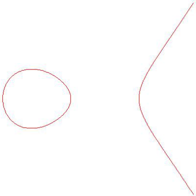


$$\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$$

L'approche classique : genre $0, 1, 2$ et 3

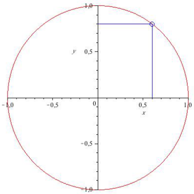


genre 0 $x^2 + y^2 = 1$

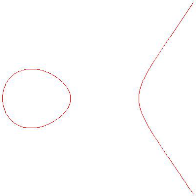


genre 1 $y^2 = x(x+1)(x+2)$

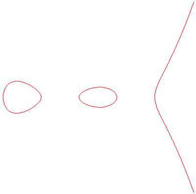
L'approche classique : genre $0, 1, 2$ et 3



genre 0 $x^2 + y^2 = 1$

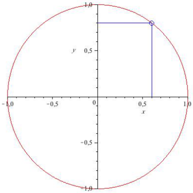


genre 1 $y^2 = x(x+1)(x+2)$

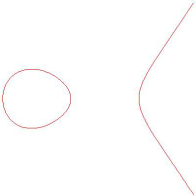


genre 2 $y^2 = x(x^2-1)(x^2-\frac{1}{4})$

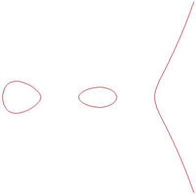
L'approche classique : genre $0, 1, 2$ et 3



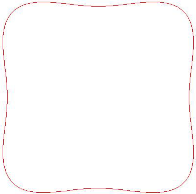
genre 0 $x^2 + y^2 = 1$



genre 1 $y^2 = x(x+1)(x+2)$



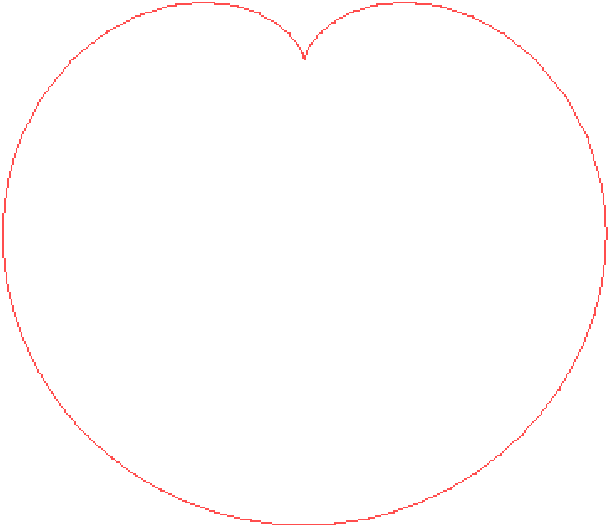
genre 2 $y^2 = x(x^2-1)(x^2-\frac{1}{4})$



genre 3 $(x^2-1)^2 + (y^2-1)^2 = 4$

Le spirographe

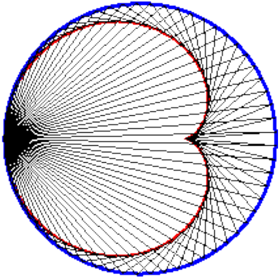
Quelques quartiques de genre 0 au quotidien



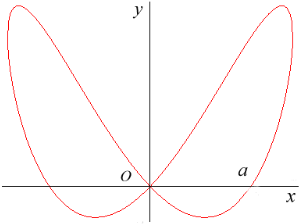
La cardioïde $(x^2 + y^2 - x)^2 = x^2 + y^2$ comme épicycloïde

au réveil

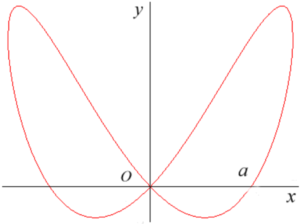
Quelques quartiques de genre 0 au quotidien

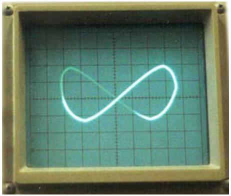
La cardioïde comme caustique



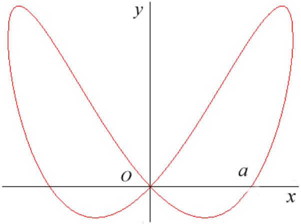
besace $(x^2 - y)^2 = (x^2 - y^2)$



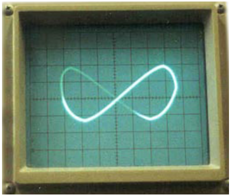
besace $(x^2 - y)^2 = (x^2 - y^2)$



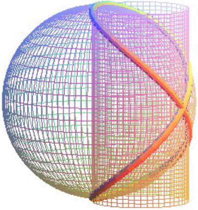
courbe de Lissajous



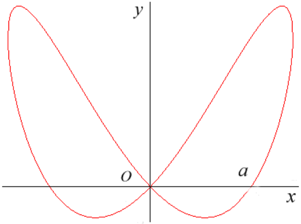
besace $(x^2 - y)^2 = (x^2 - y^2)$



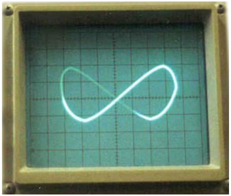
courbe de Lissajous



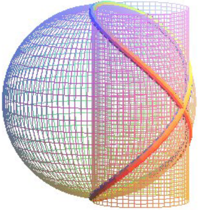
fenêtre de Vivani



besace $(x^2 - y)^2 = (x^2 - y^2)$

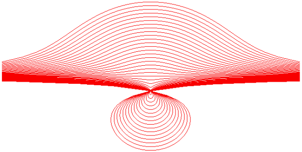


courbe de Lissajous

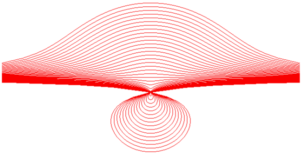


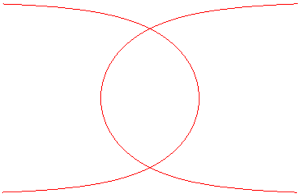
fenêtre de Vivani

musée de la marine d'Osaka

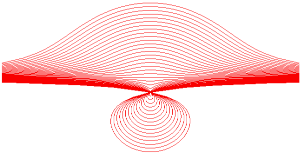
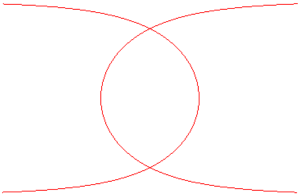


les conchoïdes de Nicomède,



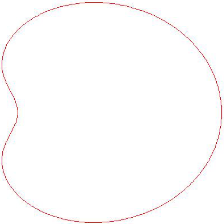


les conchoïdes de Nicomède, la trisectrice de Delanges,

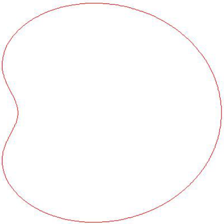
les conchoïdes de Nicomède, la trisectrice de Delanges, le bicorne, . . .

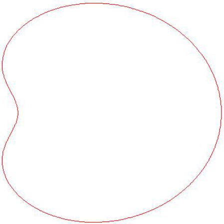
Quelques quartiques de genre 1



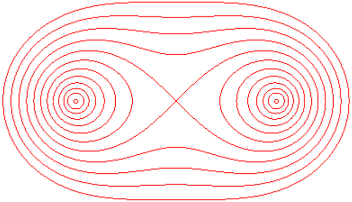
ovale de Descartes $(x^2 + y^2 - 2x + 1)^2 = 4(x^2 + y^2)$

Quelques quartiques de genre 1

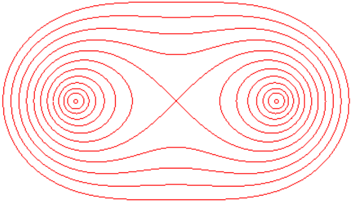




système Bélidor pour pont-levis (ici à Fort-l'Écluse)

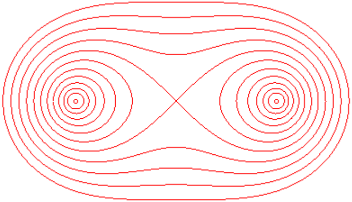


ovales de Cassini $((x-a)^2+y^2)((x+a)^2+y^2)=b^4$



ovales de Cassini

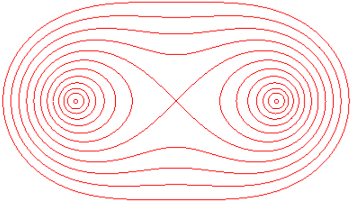
au Palais de la Découverte



ovales de Cassini

au Palais de la Découverte

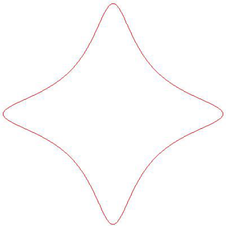
Cassini par Jean-Guillaume Moitte



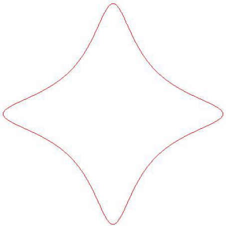
ovales de Cassini

au Palais de la Découverte

Cassini par Jean-Guillaume Moitte



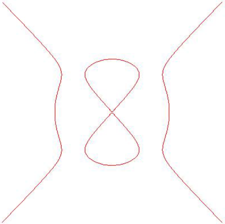
courbe d'Edwards $x^2 + y^2 = 1 - 30x^2y^2$



courbe d'Edwards $x^2 + y^2 = 1 - 30x^2y^2$

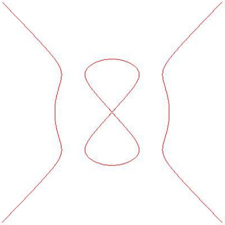
un jour dans nos cartes bleues ?

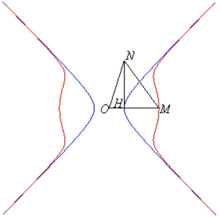
Quartique de genre 2



courbe du diable $y^4 + \frac{10}{9}x^2 = x^4 + \frac{8}{9}y^2$

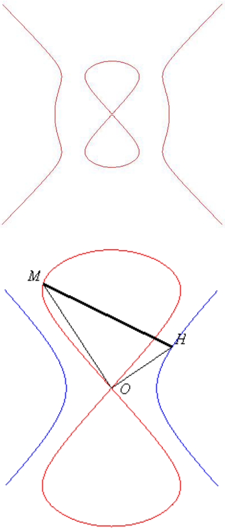
Quartique de genre 2





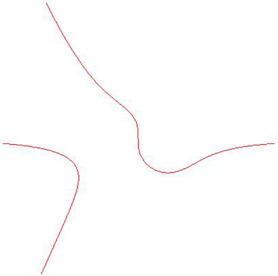
H sur l'hyperbole, $HN = 1$, $OM = ON$

Quartique de genre 2



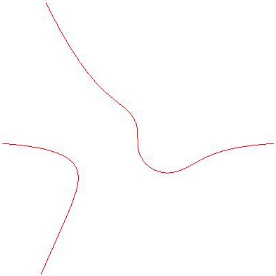
H sur l'hyperbole, rectangle en O, $HM = 1$

Quartique de genre 3

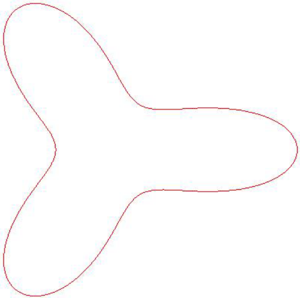


quartique de Klein
$x^3y + y^3 + x = 0$

Quartique de genre 3

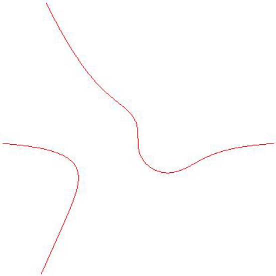


quartique de Klein
$x^3y + y^3 + x = 0$

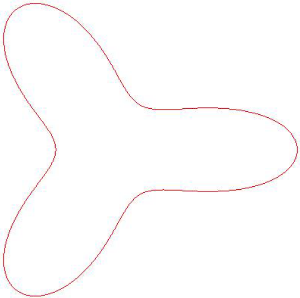


quartique de Klein (bis)
$196x^3 + 84x^2 - 588xy^2 + 84y^2 + 16 - 147x^4 - 294x^2y^2 = 147y^4$

Quartique de genre 3



quartique de Klein
$x^3y + y^3 + x = 0$



quartique de Klein (bis)
$196x^3 + 84x^2 - 588xy^2 + 84y^2 + 16 - 147x^4 - 294x^2y^2 = 147y^4$

sculpture
au MSRI

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
    - models;

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
    - models;
    - invariants;

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
    - models;
    - invariants;
    - isogeny classes of supersingular abelian threefolds which contain a Jacobian;

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
    - models;
    - invariants;
    - isogeny classes of supersingular abelian threefolds which contain a Jacobian;
    - quartics with many involutions and optimal curves.

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
   - models;
   - invariants;
   - isogeny classes of supersingular abelian threefolds which contain a Jacobian;
   - quartics with many involutions and optimal curves.
2. isogeny classes of abelian surfaces over finite fields which contain a Jacobian.

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
    - models;
    - invariants;
    - isogeny classes of supersingular abelian threefolds which contain a Jacobian;
    - quartics with many involutions and optimal curves.
2. isogeny classes of abelian surfaces over finite fields which contain a Jacobian.
3. Serre's obstruction for genus 3 curves.

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
   - models;
   - invariants;
   - isogeny classes of supersingular abelian threefolds which contain a Jacobian;
   - quartics with many involutions and optimal curves.
2. isogeny classes of abelian surfaces over finite fields which contain a Jacobian.
3. Serre's obstruction for genus 3 curves.
4. Cryptography:
   - addition law for plane quartics;

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
   - models;
   - invariants;
   - isogeny classes of supersingular abelian threefolds which contain a Jacobian;
   - quartics with many involutions and optimal curves.
2. isogeny classes of abelian surfaces over finite fields which contain a Jacobian.
3. Serre's obstruction for genus 3 curves.
4. Cryptography:
   - addition law for plane quartics;
   - Edwards curves and pairings;

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
    - models;
    - invariants;
    - isogeny classes of supersingular abelian threefolds which contain a Jacobian;
    - quartics with many involutions and optimal curves.
2. isogeny classes of abelian surfaces over finite fields which contain a Jacobian.
3. Serre's obstruction for genus 3 curves.
4. Cryptography:
    - addition law for plane quartics;
    - Edwards curves and pairings;
    - distorsion map for genus 2 curves;

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
   - models;
   - invariants;
   - isogeny classes of supersingular abelian threefolds which contain a Jacobian;
   - quartics with many involutions and optimal curves.
2. isogeny classes of abelian surfaces over finite fields which contain a Jacobian.
3. Serre's obstruction for genus 3 curves.
4. Cryptography:
   - addition law for plane quartics;
   - Edwards curves and pairings;
   - distorsion map for genus 2 curves;
   - 2-adic CM method for genus 2 curves.

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
   - models;
   - invariants;
   - isogeny classes of supersingular abelian threefolds which contain a Jacobian;
   - quartics with many involutions and optimal curves.
2. isogeny classes of abelian surfaces over finite fields which contain a Jacobian.
3. Serre's obstruction for genus 3 curves.
4. Cryptography:
   - addition law for plane quartics;
   - Edwards curves and pairings;
   - distorsion map for genus 2 curves;
   - 2-adic CM method for genus 2 curves.

Overview of the manuscript

1. Plane quartics over finite fields of characteristic 2:
   - models;
   - invariants;
   - isogeny classes of supersingular abelian threefolds which contain a Jacobian;
   - quartics with many involutions and optimal curves.
2. isogeny classes of abelian surfaces over finite fields which contain a Jacobian.
3. Serre's obstruction for genus 3 curves.
4. Cryptography:
   - addition law for plane quartics;
   - Edwards curves and pairings;
   - distorsion map for genus 2 curves;
   - 2-adic CM method for genus 2 curves.

Maximal curves and optimal curves

- $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ a finite field. K any (perfect) field;

Maximal curves and optimal curves

- $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ a finite field. K any (perfect) field;
- C/K a (smooth, projective, absolutely irreducible) curve of genus g over K;

Maximal curves and optimal curves

- $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ a finite field. K any (perfect) field;
- C/K a (smooth, projective, absolutely irreducible) curve of genus g over K;
- $m = \lfloor 2\sqrt{q} \rfloor$;

Maximal curves and optimal curves

- $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ a finite field. K any (perfect) field;
- C/K a (smooth, projective, absolutely irreducible) curve of genus g over K;
- $m = \lfloor 2\sqrt{q} \rfloor$;
- $N_q(g)$: maximal number of points on a genus g curve over $\mathbb{F}_q$.

Maximal curves and optimal curves

- $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ a finite field. K any (perfect) field;
- C/K a (smooth, projective, absolutely irreducible) curve of genus g over K;
- $m = \lfloor 2\sqrt{q} \rfloor$;
- $N_q(g) \leq 1 + q + gm$: maximal number of points on a genus g curve over $\mathbb{F}_q$.

Maximal curves and optimal curves

- $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ a finite field. K any (perfect) field;
- C/K a (smooth, projective, absolutely irreducible) curve of genus g over K;
- $m = \lfloor 2\sqrt{q} \rfloor$;
- $N_q(g) \leq 1 + q + gm$: maximal number of points on a genus g curve over $\mathbb{F}_q$.

Definition

A curve C of genus g over k is *maximal* if $\#C(k) = N_q(g)$.
It is optimal if $\#C(k) = 1 + q + gm$.

Optimal curves of genus $0, 1, 2$ and 3

If C/k is a genus 0 curve, it is isomorphic to $\mathbb{P}^1$ so $N_q(0) = q + 1$.

Optimal curves of genus $0, 1, 2$ and 3

If C/k is a genus 0 curve, it is isomorphic to $\mathbb{P}^1$ so $N_q(0) = q + 1$.

If C is an optimal curve of genus $1 \leq g \leq 3$ then Jac $C \sim E^g$ with E an elliptic curve of trace $-m$.

Optimal curves of genus $0, 1, 2$ and 3

If C/k is a genus 0 curve, it is isomorphic to $\mathbb{P}^1$ so $N_q(0) = q + 1$.

If C is an optimal curve of genus $1 \leq g \leq 3$ then $\operatorname{Jac} C \sim E^g$ with E an elliptic curve of trace $-m$.

- Existence of the isogeny class (Deuring 1941): explained by Honda-Tate theory.

Optimal curves of genus $0, 1, 2$ and 3

If C/k is a genus 0 curve, it is isomorphic to $\mathbb{P}^1$ so $N_q(0) = q + 1$.

If C is an optimal curve of genus $1 \leq g \leq 3$ then $\mathrm{Jac}\, C \sim E^g$ with E an elliptic curve of trace $-m$.

- Existence of the isogeny class (Deuring 1941): explained by Honda-Tate theory.

Proposition

There does not exist an elliptic curve with trace $-m$ if and only if $n \geq 3$, n is odd and $p|m$.

Optimal curves of genus $0, 1, 2$ and 3

If C/k is a genus 0 curve, it is isomorphic to $\mathbb{P}^1$ so $N_q(0) = q + 1$.

If C is an optimal curve of genus $1 \leq g \leq 3$ then $\operatorname{Jac} C \sim E^g$ with E an elliptic curve of trace $-m$.

- Existence of the isogeny class (Deuring 1941): explained by Honda-Tate theory.

Proposition

There does not exist an elliptic curve with trace $-m$ if and only if $n \geq 3$, n is odd and $p|m$.

This solves the question for optimal genus 1 curves.

Optimal curves of genus $0, 1, 2$ and 3

If C/k is a genus 0 curve, it is isomorphic to $\mathbb{P}^1$ so $N_q(0) = q + 1$.

If C is an optimal curve of genus $1 \leq g \leq 3$ then $\operatorname{Jac} C \sim E^g$ with E an elliptic curve of trace $-m$.

- Existence of the isogeny class (Deuring 1941): explained by Honda-Tate theory.

Proposition

There does not exist an elliptic curve with trace $-m$ if and only if $n \geq 3$, n is odd and $p|m$.

This solves the question for optimal genus 1 curves.

- Existence of a principal polarization in the class E^g: yes (the product polarization a_0).

- Existence of an absolutely indecomposable principal polarization in the class E^g.
  This question mainly translates into existence of positive definite indecomposable (quaternion) hermitian forms on $\mathrm{End}(E)$-modules $+$ descent.

- Existence of an absolutely indecomposable principal polarization in the class E^g.
  This question mainly translates into existence of positive definite indecomposable (quaternion) hermitian forms on $\mathrm{End}(E)$-modules + descent.
  - $g = 2$ (Hayashida, Nishi 1965, Serre 1983): no if and only if $q = 4, 9$ or

$$m^2 - 4q \in \{-3, -4, -7\}.$$

- Existence of an absolutely indecomposable principal polarization in the class E^g.
  This question mainly translates into existence of positive definite indecomposable (quaternion) hermitian forms on $\mathrm{End}(E)$-modules $+$ descent.
  - $g = 2$ (Hayashida, Nishi 1965, Serre 1983): no if and only if $q = 4, 9$ or
    $$m^2 - 4q \in \{-3, -4, -7\}.$$
  - $g = 3$ (Ibukiyama 1993, Lauter, Serre 2002, Nart, R. 2008): no if and only if $q = 4, 16$ or
    $$m^2 - 4q \in \{-3, -4, -8, -11\}.$$

The case $g = 2, 3$ (Continued)

For $g \leq 3$, any absolutely indecomposable p.p.a.v. $(A, a)/K$ is the Jacobian of a curve C_0 over $\bar{K}$ (Oort, Ueno 1973).

The case $g = 2, 3$ (Continued)

For $g \leq 3$, any absolutely indecomposable p.p.a.v. $(A, a)/K$ is the Jacobian of a curve C_0 over $\bar{K}$ (Oort, Ueno 1973).

Theorem (Arithmetic Torelli theorem (Serre 1985))

There is a model C/K of C_0 such that:

1. *If C_0 is hyperelliptic, there is an isomorphism*

$$(\operatorname{Jac} C, j) \xrightarrow{\sim} (A, a).$$

The case $g = 2, 3$ (Continued)

For $g \leq 3$, any absolutely indecomposable p.p.a.v. $(A, a)/K$ is the Jacobian of a curve C_0 over $\bar{K}$ (Oort, Ueno 1973).

Theorem (Arithmetic Torelli theorem (Serre 1985))

There is a model C/K of C_0 such that:

1. *If C_0 is hyperelliptic, there is an isomorphism*

$$(\operatorname{Jac} C, j) \xrightarrow{\sim} (A, a).$$

2. *If C_0 is not hyperelliptic, there is a quadratic character ε of $\operatorname{Gal}(\bar{K}/K)$, and an isomorphism*

$$(\operatorname{Jac} C, j) \xrightarrow{\sim} (A, a)_\varepsilon$$

where $(A, a)_\varepsilon$ is the twist of A by ε.

The case $g = 2$ (end)

For $g = 2$, the previous results give the answer. Actually (Serre 1983) gives the value $N_q(2)$.

The case $g = 2$ (end)

For $g = 2$, the previous results give the answer. Actually (Serre 1983) gives the value $N_q(2)$.

Theorem (Howe, Maisner, Nart, R. 2008)

An isogeny class of Weil polynomial $x^4 + ax^3 + bx^2 + aqx + q^2$ does not contain a principally polarized abelian surface if and only if the three following conditions are fullfilled:

- $a^2 - b = q$,
- $b < 0$ *and*
- *all prime divisors of* b *are congruent to* 1 *modulo* 3.

The case $g = 2$ (end)

For $g = 2$, the previous results give the answer. Actually (Serre 1983) gives the value $N_q(2)$.

Theorem (Howe, Maisner, Nart, R. 2008)

An isogeny class of Weil polynomial $x^4 + ax^3 + bx^2 + aqx + q^2$ does not contain a principally polarized abelian surface if and only if the three following conditions are fullfilled:

- $a^2 - b = q$,
- $b < 0$ *and*
- *all prime divisors of b are congruent to* 1 *modulo* 3.

Theorem (Howe, Nart, R. 2009)

One characterizes the isogeny classes which contains a Jacobian in terms of their Weil polynomials.

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

1. Explicit quotients by isogeny

Serre's obstruction for genus 3 curve

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée ...)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

1. Explicit quotients by isogeny (Partial results);

Serre's obstruction for genus 3 curve

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

1. Explicit quotients by isogeny (Partial results);
2. Serre's analytic strategy, also followed by S. Meagher

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

1. Explicit quotients by isogeny (Partial results);
2. Serre's analytic strategy, also followed by S. Meagher (Well understood);

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

1. Explicit quotients by isogeny (Partial results);
2. Serre's analytic strategy, also followed by S. Meagher (Well understood);
3. Algebraic interpretation of this strategy

Serre's obstruction for genus 3 curve

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

1. Explicit quotients by isogeny (Partial results);
2. Serre's analytic strategy, also followed by S. Meagher (Well understood);
3. Algebraic interpretation of this strategy (Work in progress);

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

1. Explicit quotients by isogeny (Partial results);
2. Serre's analytic strategy, also followed by S. Meagher (Well understood);
3. Algebraic interpretation of this strategy (Work in progress);
4. Geometric strategy

Serre's obstruction for genus 3 curve

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée ...)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

1. Explicit quotients by isogeny (Partial results);
2. Serre's analytic strategy, also followed by S. Meagher (Well understood);
3. Algebraic interpretation of this strategy (Work in progress);
4. Geometric strategy (Work in progress).

Quotients by isogeny

Key idea: use families with explicit elliptic isogeny factors and reverse the process to see when you can glue them together in this way.

Quotients by isogeny

Key idea: use families with explicit elliptic isogeny factors and reverse the process to see when you can glue them together in this way.

Using families with geometric automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$.

- (Howe, Leprevost, Poonen 2002) in characteristic different from 2 (but no general results for maximal curves);

Quotients by isogeny

Key idea: use families with explicit elliptic isogeny factors and reverse the process to see when you can glue them together in this way.

Using families with geometric automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$.

- (Howe, Leprevost, Poonen 2002) in characteristic different from 2 (but no general results for maximal curves);
- (Nart, R. 2008): if $n \geq 6$ is even then there is an optimal curve over $\mathbb{F}_{2^n}$.

Quotients by isogeny

Key idea: use families with explicit elliptic isogeny factors and reverse the process to see when you can glue them together in this way.

Using families with geometric automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$.

- (Howe, Leprevost, Poonen 2002) in characteristic different from 2 (but no general results for maximal curves);
- (Nart, R. 2008): if $n \geq 6$ is even then there is an optimal curve over $\mathbb{F}_{2^n}$.
- (Nart, R. 2009) : if n is odd and $m = \lfloor 2\sqrt{2^n} \rfloor \equiv 1, 5, 7 \pmod 8$ there is an optimal curve over $\mathbb{F}_{2^n}$.

Quotients by isogeny

Key idea: use families with explicit elliptic isogeny factors and reverse the process to see when you can glue them together in this way.

Using families with geometric automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$.

- (Howe, Leprevost, Poonen 2002) in characteristic different from 2 (but no general results for maximal curves);
- (Nart, R. 2008): if $n \geq 6$ is even then there is an optimal curve over $\mathbb{F}_{2^n}$.
- (Nart, R. 2009) : if n is odd and $m = \lfloor 2\sqrt{2^n} \rfloor \equiv 1, 5, 7 \pmod 8$ there is an optimal curve over $\mathbb{F}_{2^n}$.

Rem: (Mestre 2009) works with the family with geometric automorphism group S_3.

Quotients by isogeny

Key idea: use families with explicit elliptic isogeny factors and reverse the process to see when you can glue them together in this way.

Using families with geometric automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$.

- (Howe, Leprevost, Poonen 2002) in characteristic different from 2 (but no general results for maximal curves);
- (Nart, R. 2008): if $n \geq 6$ is even then there is an optimal curve over $\mathbb{F}_{2^n}$.
- (Nart, R. 2009) : if n is odd and $m = \lfloor 2\sqrt{2^n} \rfloor \equiv 1, 5, 7 \pmod 8$ there is an optimal curve over $\mathbb{F}_{2^n}$.

Rem: (Mestre 2009) works with the family with geometric automorphism group S_3.

This works quite well for small values of q: see `www.manypoints.org` (van der Geer, Howe, Lauter, R.).

Main result (Lachaud, R., Zykin 2009)

Let $A = (A, a)/K$ be a p.p.a.t. defined over a field K with char $K \neq 2$. Assume that a is absolutely indecomposable. There exists a unique geometric Siegel modular form of weight 18 defined over $\mathbb{Z}$, denoted χ_{18}, such that

Main result (Lachaud, R., Zykin 2009)

Let $A = (A, a)/K$ be a p.p.a.t. defined over a field K with char $K \neq 2$. Assume that a is absolutely indecomposable. There exists a unique geometric Siegel modular form of weight 18 defined over $\mathbb{Z}$, denoted χ_{18}, such that

1. (A, a) is a hyperelliptic Jacobian if and only if $\chi_{18}(A, a) = 0$.

Main result (Lachaud, R., Zykin 2009)

Let $A = (A, a)/K$ be a p.p.a.t. defined over a field K with char $K \neq 2$. Assume that a is absolutely indecomposable. There exists a unique geometric Siegel modular form of weight 18 defined over $\mathbb{Z}$, denoted χ_{18}, such that

1. (A, a) is a hyperelliptic Jacobian if and only if $\chi_{18}(A, a) = 0$.
2. (A, a) is a non hyperelliptic Jacobian if and only if $\chi_{18}(A, a)$ is a non-zero square.

Main result (Lachaud, R., Zykin 2009)

Let $A = (A, a)/K$ be a p.p.a.t. defined over a field K with char $K \neq 2$. Assume that a is absolutely indecomposable. There exists a unique geometric Siegel modular form of weight 18 defined over $\mathbb{Z}$, denoted χ_{18}, such that

1. (A, a) is a hyperelliptic Jacobian if and only if $\chi_{18}(A, a) = 0$.
2. (A, a) is a non hyperelliptic Jacobian if and only if $\chi_{18}(A, a)$ is a non-zero square.

Moreover, if $K \subset \mathbb{C}$, let

- $(\omega_1, \omega_2, \omega_3)$ be a basis of $\Omega^1_K[A]$;

Main result (Lachaud, R., Zykin 2009)

Let $A = (A, a)/K$ be a p.p.a.t. defined over a field K with char $K \neq 2$. Assume that a is absolutely indecomposable. There exists a unique geometric Siegel modular form of weight 18 defined over $\mathbb{Z}$, denoted χ_{18}, such that

1. (A, a) is a hyperelliptic Jacobian if and only if $\chi_{18}(A, a) = 0$.
2. (A, a) is a non hyperelliptic Jacobian if and only if $\chi_{18}(A, a)$ is a non-zero square.

Moreover, if $K \subset \mathbb{C}$, let

- $(\omega_1, \omega_2, \omega_3)$ be a basis of $\Omega^1_K[A]$;
- $\gamma_1, \ldots \gamma_6$ be a symplectic basis (for a);

Main result (Lachaud, R., Zykin 2009)

Let $A = (A, a)/K$ be a p.p.a.t. defined over a field K with char $K \neq 2$. Assume that a is absolutely indecomposable. There exists a unique geometric Siegel modular form of weight 18 defined over $\mathbb{Z}$, denoted χ_{18}, such that

1. (A, a) is a hyperelliptic Jacobian if and only if $\chi_{18}(A, a) = 0$.
2. (A, a) is a non hyperelliptic Jacobian if and only if $\chi_{18}(A, a)$ is a non-zero square.

Moreover, if $K \subset \mathbb{C}$, let

- $(\omega_1, \omega_2, \omega_3)$ be a basis of $\Omega^1_K[A]$;
- $\gamma_1, \ldots \gamma_6$ be a symplectic basis (for a);
- $\Omega_a := [\Omega_1 \ \Omega_2] = [\int_{\gamma_j} \omega_i]$ with $\tau_a := \Omega_2^{-1}\Omega_1 \in \mathbb{H}_3$.

Main result (Lachaud, R., Zykin 2009)

Let $A = (A, a)/K$ be a p.p.a.t. defined over a field K with char $K \neq 2$. Assume that a is absolutely indecomposable. There exists a unique geometric Siegel modular form of weight 18 defined over $\mathbb{Z}$, denoted χ_{18}, such that

1. (A, a) is a hyperelliptic Jacobian if and only if $\chi_{18}(A, a) = 0$.
2. (A, a) is a non hyperelliptic Jacobian if and only if $\chi_{18}(A, a)$ is a non-zero square.

Moreover, if $K \subset \mathbb{C}$, let

- $(\omega_1, \omega_2, \omega_3)$ be a basis of $\Omega^1_K[A]$;
- $\gamma_1, \dots \gamma_6$ be a symplectic basis (for a);
- $\Omega_a := [\Omega_1 \ \Omega_2] = [\int_{\gamma_j} \omega_i]$ with $\tau_a := \Omega_2^{-1}\Omega_1 \in \mathbb{H}_3$.

Then (A, a) is a Jacobian if and only if

$$\frac{(2\pi)^{54}}{2^{28}} \cdot \frac{\prod_{[\varepsilon] \text{ even}} \theta[\varepsilon](\tau_a)}{\det(\Omega_2)^{18}}$$

is a square in K.

Main result (Lachaud, R., Zykin 2009)

Let $A = (A, a)/K$ be a p.p.a.t. defined over a field K with char $K \neq 2$. Assume that a is absolutely indecomposable. There exists a unique geometric Siegel modular form of weight 18 defined over $\mathbb{Z}$, denoted χ_{18}, such that

1. (A, a) is a hyperelliptic Jacobian if and only if $\chi_{18}(A, a) = 0$.
2. (A, a) is a non hyperelliptic Jacobian if and only if $\chi_{18}(A, a)$ is a non-zero square.

Moreover, if $K \subset \mathbb{C}$, let

- $(\omega_1, \omega_2, \omega_3)$ be a basis of $\Omega^1_K[A]$;
- $\gamma_1, \ldots \gamma_6$ be a symplectic basis (for a);
- $\Omega_a := [\Omega_1 \ \Omega_2] = [\int_{\gamma_j} \omega_i]$ with $\tau_a := \Omega_2^{-1}\Omega_1 \in \mathbb{H}_3$.

Then (A, a) is a Jacobian if and only if

$$\chi_{18}((A, a), \omega_1 \wedge \omega_2 \wedge \omega_3) := \frac{(2\pi)^{54}}{2^{28}} \cdot \frac{\prod_{[\varepsilon] \text{ even}} \theta[\varepsilon](\tau_a)}{\det(\Omega_2)^{18}}$$

is a square in K.

Ingredients of the proof and consequences

- Result of (Ichikawa 1996): let $t : \mathsf{M}_3 \to \mathsf{A}_3$ be the Torelli map. There exists a Teichmüller modular form of weight 9 defined over $\mathbb{Z}$, denoted μ_9, such that $t^*(\chi_{18}) = \mu_9^2$.

- Result of (Ichikawa 1996): let $t : \mathsf{M}_3 \to \mathsf{A}_3$ be the Torelli map. There exists a Teichmüller modular form of weight 9 defined over $\mathbb{Z}$, denoted μ_9, such that $t^*(\chi_{18}) = \mu_9^2$.
- General result on the action of twists on geometric Siegel modular forms.

Ingredients of the proof and consequences

- Result of (Ichikawa 1996): let $t : \mathsf{M}_3 \to \mathsf{A}_3$ be the Torelli map. There exists a Teichmüller modular form of weight 9 defined over $\mathbb{Z}$, denoted μ_9, such that $t^*(\chi_{18}) = \mu_9^2$.
- General result on the action of twists on geometric Siegel modular forms.
- Link between analytic and geometric Siegel modular forms.

Ingredients of the proof and consequences

- Result of (Ichikawa 1996): let $t : \mathrm{M}_3 \to \mathrm{A}_3$ be the Torelli map. There exists a Teichmüller modular form of weight 9 defined over $\mathbb{Z}$, denoted μ_9, such that $t^*(\chi_{18}) = \mu_9^2$.
- General result on the action of twists on geometric Siegel modular forms.
- Link between analytic and geometric Siegel modular forms.

By-products:

- Klein's formula: $\mu_9 = \pm \,\mathrm{Disc}$;

Ingredients of the proof and consequences

- Result of (Ichikawa 1996): let $t : \mathrm{M}_3 \to \mathrm{A}_3$ be the Torelli map. There exists a Teichmüller modular form of weight 9 defined over $\mathbb{Z}$, denoted μ_9, such that $t^*(\chi_{18}) = \mu_9^2$.
- General result on the action of twists on geometric Siegel modular forms.
- Link between analytic and geometric Siegel modular forms.

By-products:

- Klein's formula: $\mu_9 = \pm\,\mathrm{Disc}$;
- cannot work for g even;

Ingredients of the proof and consequences

- Result of (Ichikawa 1996): let $t : \mathsf{M}_3 \to \mathsf{A}_3$ be the Torelli map. There exists a Teichmüller modular form of weight 9 defined over $\mathbb{Z}$, denoted μ_9, such that $t^*(\chi_{18}) = \mu_9^2$.
- General result on the action of twists on geometric Siegel modular forms.
- Link between analytic and geometric Siegel modular forms.

By-products:

- Klein's formula: $\mu_9 = \pm\,\mathrm{Disc}$;
- cannot work for g even;
- need forms of weight h such that $h/2$ is odd;

Ingredients of the proof and consequences

- Result of (Ichikawa 1996): let $t : \mathrm{M}_3 \to \mathrm{A}_3$ be the Torelli map. There exists a Teichmüller modular form of weight 9 defined over $\mathbb{Z}$, denoted μ_9, such that $t^*(\chi_{18}) = \mu_9^2$.
- General result on the action of twists on geometric Siegel modular forms.
- Link between analytic and geometric Siegel modular forms.

By-products:

- Klein's formula: $\mu_9 = \pm \mathrm{Disc}$;
- cannot work for g even;
- need forms of weight h such that $h/2$ is odd;
- cannot take χ_h.

How to use it for optimal curves ?

R. 2009 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

How to use it for optimal curves ?

R. 2009 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

- $\exists$? optimal curve $C/\mathbb{F}_{47}$: $A = \operatorname{Jac} C \sim E^3$ with E CM by $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1+\sqrt{-19})/2$.

How to use it for optimal curves ?

R. 2009 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

- $\exists$? optimal curve $C/\mathbb{F}_{47}$: $A = \operatorname{Jac} C \sim E^3$ with E CM by $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1+\sqrt{-19})/2$.
- $Cl(\mathcal{O}) = 1 \Rightarrow A = E^3$.

How to use it for optimal curves ?

R. 2009 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

- $\exists$? optimal curve $C/\mathbb{F}_{47}$: $A = \text{Jac}\, C \sim E^3$ with E CM by $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1 + \sqrt{-19})/2$.
- $Cl(\mathcal{O}) = 1 \Rightarrow A = E^3$.
- a_0 the product polarization on A:

$$\{a \text{ p.p. on } A\} \longleftrightarrow \{M = a_0^{-1} a \in M_3(\mathcal{O}) \text{ hermitian positive definite of determinant } 1\}.$$

How to use it for optimal curves ?

R. 2009 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

- $\exists$? optimal curve $C/\mathbb{F}_{47}$: $A = \text{Jac}\, C \sim E^3$ with E CM by $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1+\sqrt{-19})/2$.
- $Cl(\mathcal{O}) = 1 \Rightarrow A = E^3$.
- a_0 the product polarization on A:

$$\{a \text{ p.p. on } A\} \longleftrightarrow \{M = a_0^{-1} a \in M_3(\mathcal{O}) \text{ hermitian positive definite of determinant } 1\}.$$

- computation by (Schiemann 1998) of such matrices. There is only one –up to equivalence–, which is indecomposable:

$$M = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\overline{\tau} & 3 \end{pmatrix}.$$

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;
- find a period matrix associated to $(\tilde{E}^3, a_0 M)$ w.r.t. wedge product ω_0 of the pull back of the differential $dx/(2y)$ on each $\tilde{E}$ of $\tilde{E}^3$:

$$c_1(a_0 M) = \frac{1}{\mathrm{Im}(\omega_1 \overline{\omega_2})} {}^t M$$

where $[\omega_1, \omega_2]$ is a period matrix of $\tilde{E}$ w.r.t. $dx/(2y)$;

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;
- find a period matrix associated to $(\tilde{E}^3, a_0 M)$ w.r.t. wedge product ω_0 of the pull back of the differential $dx/(2y)$ on each $\tilde{E}$ of $\tilde{E}^3$:

$$c_1(a_0 M) = \frac{1}{\mathrm{Im}(\omega_1 \overline{\omega_2})} {}^t M$$

  where $[\omega_1, \omega_2]$ is a period matrix of $\tilde{E}$ w.r.t. $dx/(2y)$;
- compute an analytic approximation of

$$\chi_{18}((\tilde{E}^3, a_0 M), \omega_0) = (2^{19} \cdot 19^7)^2;$$

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;
- find a period matrix associated to $(\tilde{E}^3, a_0 M)$ w.r.t. wedge product ω_0 of the pull back of the differential $dx/(2y)$ on each $\tilde{E}$ of $\tilde{E}^3$:

$$c_1(a_0 M) = \frac{1}{\mathrm{Im}(\omega_1 \overline{\omega_2})} {}^t M$$

where $[\omega_1, \omega_2]$ is a period matrix of $\tilde{E}$ w.r.t. $dx/(2y)$;
- compute an analytic approximation of

$$\chi_{18}((\tilde{E}^3, a_0 M), \omega_0) = (2^{19} \cdot 19^7)^2;$$

- since it is a square (over $\mathbb{F}_{47}$), such an optimal curve C exists.

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;
- find a period matrix associated to $(\tilde{E}^3, a_0 M)$ w.r.t. wedge product ω_0 of the pull back of the differential $dx/(2y)$ on each $\tilde{E}$ of $\tilde{E}^3$:

$$c_1(a_0 M) = \frac{1}{\mathrm{Im}(\omega_1 \overline{\omega_2})} {}^t M$$

  where $[\omega_1, \omega_2]$ is a period matrix of $\tilde{E}$ w.r.t. $dx/(2y)$;
- compute an analytic approximation of

$$\chi_{18}((\tilde{E}^3, a_0 M), \omega_0) = (2^{19} \cdot 19^7)^2;$$

- since it is a square (over $\mathbb{F}_{47}$), such an optimal curve C exists.

(Guàrdia 2009):

$$\tilde{C} : x^4 + \frac{1}{9} y^4 + \frac{2}{3} x^2 y^2 - 190 y^2 - 570 x^2 + \frac{152}{9} y^3 - 152 x^2 y = 1083.$$

Values of $\chi = \chi_{18}((\tilde{E}^3, a_0 M), \omega_0)$

$\tilde{E}$: Gross' models with discriminant d^3 (when the class number is 1).

d	$M, \tau = (1+\sqrt{d})/2$	χ	$\#\,\mathrm{Aut}(\tilde{E}^3, a)$
-7	$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & \overline{\tau} \\ 1 & \tau & 2 \end{pmatrix}$	$(7^7)^2$	$2 \cdot 168$
-19	$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\overline{\tau} & 3 \end{pmatrix}$	$(2^5 \cdot 19^7)^2 \cdot (-2)$	$2 \cdot 6$
-43	$\begin{pmatrix} 3 & 1 & 1-\overline{\tau} \\ 1 & 4 & 2 \\ 1-\tau & 2 & 5 \end{pmatrix}$	$(2^6 \cdot 43^7)^2 \cdot (-47 \cdot 79 \cdot 107 \cdot 173)$	$2 \cdot 1$
-67	$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 3 & -2+\overline{\tau} \\ -1 & -2+\tau & 7 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 67^7)^2 \cdot (-2 \cdot 7 \cdot 31)$	$2 \cdot 6$
-163	$\begin{pmatrix} 2 & 1 & -\overline{\tau} \\ 1 & 2 & 1-\overline{\tau} \\ -\tau & 1-\tau & 28 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 11^4 \cdot 163^7)^2 \cdot (-2 \cdot 7 \cdot 11 \cdot 19 \cdot 127)$	$2 \cdot 6$
-15	$\begin{pmatrix} 2 & -1 & -1+\overline{\tau} \\ -1 & 2 & 1-\overline{\tau} \\ -1+\tau & 1-\tau & 3 \end{pmatrix}$	$22769095299822142340569171645771726299/4+$ $10182522603020834484863085151244322675 \cdot \sqrt{5}/4+$ $44626409093538218819956956474294768 69 \cdot \sqrt{-15}/4$ $+9978330617922886443823982755114202445 \cdot \sqrt{-3}$	$2 \cdot 24$

Algebraic interpretation of χ

Idea: interpret $\mathfrak{p} | \chi$ in terms of the geometric nature of $(\tilde{E}^3, a_0 M) \pmod{\mathfrak{p}}$.

Algebraic interpretation of χ

Idea: interpret $\mathfrak{p} | \chi$ in terms of the geometric nature of $(\tilde{E}^3, a_0 M) \pmod{\mathfrak{p}}$.

So far, very basic results about primes that appear because of decomposable polarizations.

Algebraic interpretation of χ

Idea: interpret $\mathfrak{p}|\chi$ in terms of the geometric nature of $(\tilde{E}^3, a_0 M) \pmod{\mathfrak{p}}$.

So far, very basic results about primes that appear because of decomposable polarizations.

Question: how to detect hyperelliptic reduction ?
Ex. for $d = -15$ with $\mathfrak{p}|19$:

$\sqrt{-3}$	$\sqrt{5}$	$(\tilde{E}^3, a_0 M) \pmod{\mathfrak{p}}$ is the Jacobian of a
-4	9	non hyperelliptic curve with $1+q+3m-3$ points
-4	-9	non hyperelliptic curve with $1+q+3m-3$ points
4	-9	non hyperelliptic curve with $1+q-3m+3$ points
4	9	hyperelliptic curve

Algebraic interpretation of χ

Idea: interpret $\mathfrak{p} | \chi$ in terms of the geometric nature of $(\tilde{E}^3, a_0 M) \pmod{\mathfrak{p}}$.

So far, very basic results about primes that appear because of decomposable polarizations.

Question: how to detect hyperelliptic reduction ?
Ex. for $d = -15$ with $\mathfrak{p} | 19$:

$\sqrt{-3}$	$\sqrt{5}$	$(\tilde{E}^3, a_0 M) \pmod{\mathfrak{p}}$ is the Jacobian of a
-4	9	non hyperelliptic curve with $1 + q + 3m - 3$ points
-4	-9	non hyperelliptic curve with $1 + q + 3m - 3$ points
4	-9	non hyperelliptic curve with $1 + q - 3m + 3$ points
4	9	hyperelliptic curve

Worse: how to control the (parity of the) exponents ?

References for introduction material

- Mainly: `http://www.mathcurve.com/`
- Spirograph: `http://fr.wikipedia.org/wiki/Spirographe_(jeu)`
- Osaka museum: `http://fr.wikipedia.org/wiki/Fenêtre_de_Viviani`
- "Ovales de Cassini" : picture from G. Lachaud
- "Cassini statue": `http://home.nordnet.fr/~ajuhel/Obs_Paris/Cassini/cassini.html`
- The eightfold way. The beauty of Klein's quartic curve. Edited by Silvio Levy. Mathematical Sciences Research Institute Publications, **35**. Cambridge University Press, Cambridge, 1999, p. 325
- Video of Klein quartic: `http://www.gregegan.net/SCIENCE/KleinQuartic/KleinQuartic.html`