Rationality of intersection points of a line and a quartic

Christophe Ritzenthaler
Joint work with Roger Oyono

Institut de Mathématiques de Luminy, CNRS

Istanbul, 27-30 June 2010

Initial problem

How to add points on the Jacobian of non-hyperelliptic genus 3 curves C/k ?

Initial problem

How to add points on the Jacobian of non-hyperelliptic genus 3 curves C/k ?

This problem was addressed and solved geometrically in Flon-Oyono-R. 08.

Initial problem

How to add points on the Jacobian of non-hyperelliptic genus 3 curves C/k ?

This problem was addressed and solved geometrically in Flon-Oyono-R. 08.

Summary:

- non-hyperelliptic genus 3 curves = smooth plane quartics.

Initial problem

How to add points on the Jacobian of non-hyperelliptic genus 3 curves C/k ?

This problem was addressed and solved geometrically in Flon-Oyono-R. 08.

Summary:

- non-hyperelliptic genus 3 curves = smooth plane quartics.
- points on the Jacobian are represented by the sum D of 3 points on the curve C.

Initial problem

How to add points on the Jacobian of non-hyperelliptic genus 3 curves C/k ?

This problem was addressed and solved geometrically in Flon-Oyono-R. 08.

Summary:

- non-hyperelliptic genus 3 curves = smooth plane quartics.
- points on the Jacobian are represented by the sum D of 3 points on the curve C.
- Choice of a good divisor at infinity $\rightsquigarrow$ condition $(*)$:

  There is a rational line ℓ^∞ which crosses the quartic C in four k-points $P_1^\infty, P_2^\infty, P_3^\infty, P_4^\infty$.

A geometric addition algorithm

Aim: given D_1, D_2 find D^+ such that $D^+ + D^\infty \sim D_1 + D_2$.

A geometric addition algorithm

Aim: given D_1, D_2 find D^+ such that $D^+ + D^\infty \sim D_1 + D_2$.

1. Take a cubic E which goes (with multiplicity) through the support of D_1, D_2 and $P_1^\infty, P_2^\infty, P_4^\infty$. This cubic also crosses C in the residual effective divisor D_3.

A geometric addition algorithm

Aim: given D_1, D_2 find D^+ such that $D^+ + D^\infty \sim D_1 + D_2$.

1. Take a cubic E which goes (with multiplicity) through the support of D_1, D_2 and $P_1^\infty, P_2^\infty, P_4^\infty$. This cubic also crosses C in the residual effective divisor D_3.
2. Take a conic Q which goes through the support of D_3 and P_1^∞, P_2^∞. This conic also crosses C in the residual effective divisor D^+.

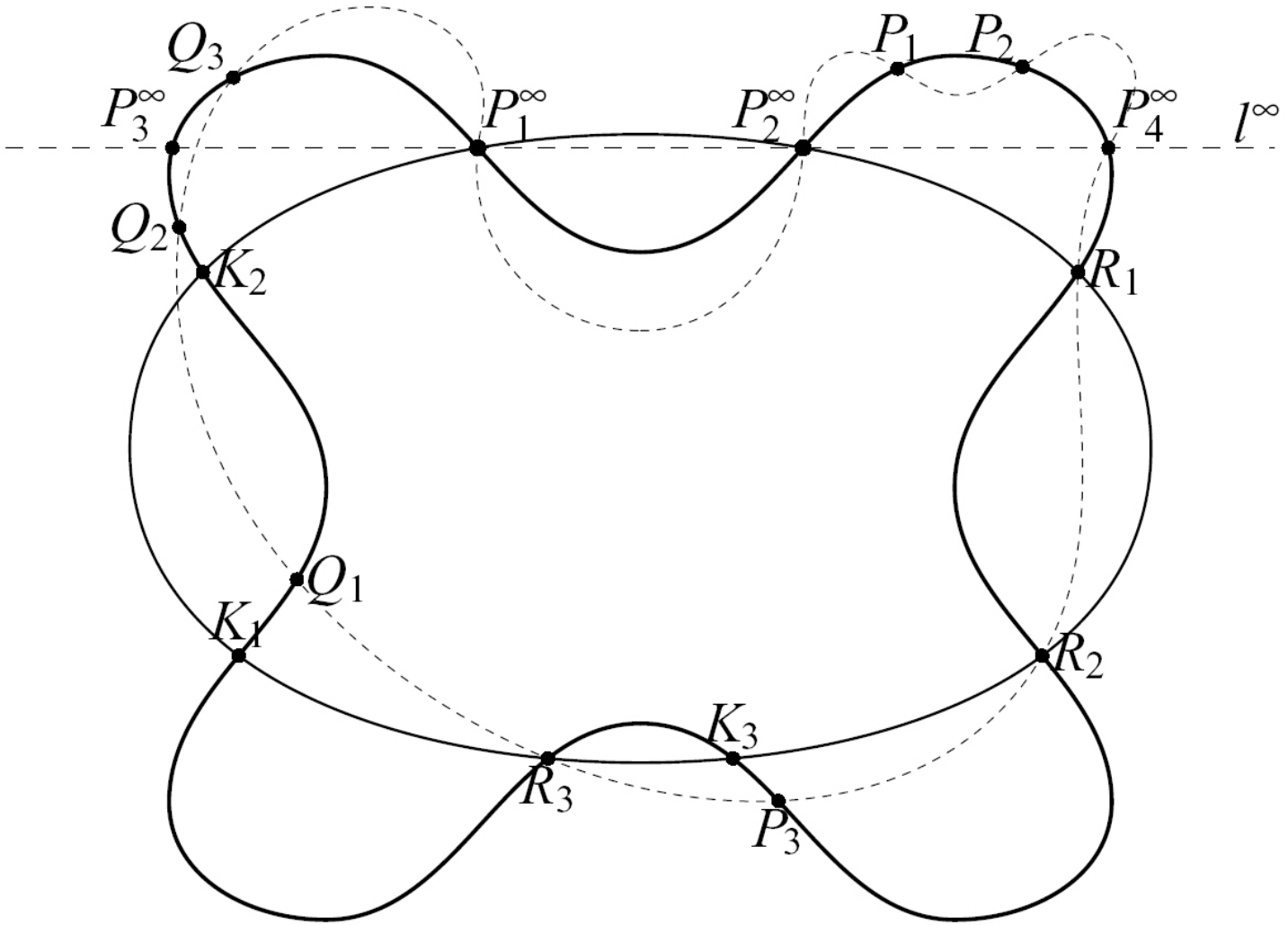
A geometric addition algorithm

Aim: given D_1, D_2 find D^+ such that $D^+ + D^\infty \sim D_1 + D_2$.

1. Take a cubic E which goes (with multiplicity) through the support of D_1, D_2 and $P_1^\infty, P_2^\infty, P_4^\infty$. This cubic also crosses C in the residual effective divisor D_3.
2. Take a conic Q which goes through the support of D_3 and P_1^∞, P_2^∞. This conic also crosses C in the residual effective divisor D^+.

Why ? Because $(\ell^\infty \cdot C) \sim \kappa$, $(Q \cdot C) \sim 2\kappa$ and $(E \cdot C) \sim 3\kappa$ where κ is the canonical divisor on C.

A chord construction



Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x), \quad \deg(f_4) \leq 4,$$

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x), \quad \deg(f_4) \leq 4,$$

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case);

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x), \quad \deg(f_4) \leq 4,$$

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case);
2. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty = P_4^\infty$ (flex case).

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x), \quad \deg(f_4) \leq 4,$$

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case);
2. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty = P_4^\infty$ (flex case).
3. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 2$ if $P_1^\infty = P_2^\infty = P_3^\infty = P_4^\infty$ (hyperflex case). These curves are the $C_{3,4}$-curves.

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x), \quad \deg(f_4) \leq 4,$$

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case);
2. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty = P_4^\infty$ (flex case).
3. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 2$ if $P_1^\infty = P_2^\infty = P_3^\infty = P_4^\infty$ (hyperflex case). These curves are the $C_{3,4}$-curves.
4. If $\mathrm{char}(k) \neq 3$, $C : y^3 = f_4(x)$ (Picard curves) iif P_1^∞ is a rational Galois point.

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x), \quad \deg(f_4) \leq 4,$$

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case);
2. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty = P_4^\infty$ (flex case).
3. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 2$ if $P_1^\infty = P_2^\infty = P_3^\infty = P_4^\infty$ (hyperflex case). These curves are the $C_{3,4}$-curves.
4. If $\mathrm{char}(k) \neq 3$, $C : y^3 = f_4(x)$ (Picard curves) iif P_1^∞ is a rational Galois point.

$\rightsquigarrow$: the more special, the faster.

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x), \quad \deg(f_4) \leq 4,$$

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case);
2. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty = P_4^\infty$ (flex case).
3. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 2$ if $P_1^\infty = P_2^\infty = P_3^\infty = P_4^\infty$ (hyperflex case). These curves are the $C_{3,4}$-curves.
4. If $\mathrm{char}(k) \neq 3$, $C : y^3 = f_4(x)$ (Picard curves) iif P_1^∞ is a rational Galois point.

$\rightsquigarrow$: the more special, the faster.

Remark: Quartics with a hyperflex form a sub-variety of codimension 1. So generically the two last cases do not occur.

Study of the condition $(*)$ over $\mathbb{F}_q$ (Oyono-R.)

Theorem

Let C be a smooth plane quartic over the finite field $\mathbb{F}_q$ with $q = p^n$ elements. If $q \geq 127$, then there exists a line ℓ which intersects C at rational points only.

Study of the condition $(*)$ over $\mathbb{F}_q$ (Oyono-R.)

Theorem

Let C be a smooth plane quartic over the finite field $\mathbb{F}_q$ with $q = p^n$ elements. If $q \geq 127$, then there exists a line ℓ which intersects C at rational points only.

Theorem

Let C be a smooth plane quartic over $\mathbb{F}_q$. If $q \geq 66^2 + 1$, then there exists a tangent to C which intersects C at rational points only.

Study of the condition $(*)$ over $\mathbb{F}_q$ (Oyono-R.)

Theorem

Let C be a smooth plane quartic over the finite field $\mathbb{F}_q$ with $q = p^n$ elements. If $q \geq 127$, then there exists a line ℓ which intersects C at rational points only.

Theorem

Let C be a smooth plane quartic over $\mathbb{F}_q$. If $q \geq 66^2 + 1$, then there exists a tangent to C which intersects C at rational points only.

Moreover, under a certain conjecture, the probability for a plane smooth quartic over a finite field to have a rational flex is about 0.63.

Proof of the generic case

Follow an idea of (Diem-Thomé 08).

Proof of the generic case

Follow an idea of (Diem-Thomé 08).

1. Let $P \in C(k)$. Consider the separable geometric cover $\phi : C \to |\kappa - P| = \mathbb{P}^1$ of degree 3 induced by the linear system $|\kappa - P|$. This parametrizes lines through the point P.

Proof of the generic case

Follow an idea of (Diem-Thomé 08).

1. Let $P \in C(k)$. Consider the separable geometric cover $\phi : C \to |\kappa - P| = \mathbb{P}^1$ of degree 3 induced by the linear system $|\kappa - P|$. This parametrizes lines through the point P.
2. Using effective Chebotarev's density theorem for function fields, one gets estimation on the number of completely split divisors in $|\kappa - P|$.

Proof for the tangent case

Let $T : C \to \mathrm{Sym}^2(C)$, $P \mapsto T_P(C) \cdot C - 2P$ be the tangential correspondence. We associate to it its correspondence curve

$$X_C = \{(P, Q) \in C \times C : Q \in T(P)\}$$

which is defined over k.

Proof for the tangent case

Let $T : C \to \mathrm{Sym}^2(C)$, $P \mapsto T_P(C) \cdot C - 2P$ be the tangential correspondence. We associate to it its correspondence curve

$$X_C = \{(P, Q) \in C \times C : Q \in T(P)\}$$

which is defined over k.

We want to prove that there is a rational point on X_C when q is big enough.

Proof for the tangent case

Let $T : C \to \mathrm{Sym}^2(C)$, $P \mapsto T_P(C) \cdot C - 2P$ be the tangential correspondence. We associate to it its correspondence curve

$$X_C = \{(P, Q) \in C \times C : Q \in T(P)\}$$

which is defined over k.

We want to prove that there is a rational point on X_C when q is big enough.

Proposition (Aubry, Perret 95)

Let $X/\mathbb{F}_q$ be a geometrically irreducible curve of arithmetic genus π_X. Then

$$|\#X(\mathbb{F}_q) - (q+1)| \leq 2\pi_X\sqrt{q}.$$

In particular if $q \geq (2\pi_X)^2$ then X has a rational point.

The question of the absolute irreducibility of X_C

- The case of $p \neq 2$.

Let $\pi_i : X_C \to C$ be the projections on the first and second factors.

The question of the absolute irreducibility of X_C

- The case of $p \neq 2$.

Let $\pi_i : X_C \to C$ be the projections on the first and second factors. The morphism π_1 a degree 2-cover which ramification points are the bitangency points.

The question of the absolute irreducibility of X_C

- The case of $p \neq 2$.

Let $\pi_i : X_C \to C$ be the projections on the first and second factors. The morphism π_1 a degree 2-cover which ramification points are the bitangency points. Moreover if a bitangency point P is not a hyperflex, then the points in the fiber of $\pi_1^{-1}(P)$ are smooth points on X_C.

The question of the absolute irreducibility of X_C

- The case of $p \neq 2$.

Let $\pi_i : X_C \to C$ be the projections on the first and second factors. The morphism π_1 a degree 2-cover which ramification points are the bitangency points. Moreover if a bitangency point P is not a hyperflex, then the points in the fiber of $\pi_1^{-1}(P)$ are smooth points on X_C.This implies that X_C is absolutely irreducible.

The question of the absolute irreducibility of X_C

- The case of $p \neq 2$.

Let $\pi_i : X_C \to C$ be the projections on the first and second factors. The morphism π_1 a degree 2-cover which ramification points are the bitangency points. Moreover if a bitangency point P is not a hyperflex, then the points in the fiber of $\pi_1^{-1}(P)$ are smooth points on X_C.This implies that X_C is absolutely irreducible.

- The case $p = 2$ (not in the article, see Arxiv).

We prove that if X_C is not absolutely irreducible, then X_C is reducible and each component is isomorphic to C.

The question of the absolute irreducibility of X_C

- The case of $p \neq 2$.

Let $\pi_i : X_C \to C$ be the projections on the first and second factors. The morphism π_1 a degree 2-cover which ramification points are the bitangency points. Moreover if a bitangency point P is not a hyperflex, then the points in the fiber of $\pi_1^{-1}(P)$ are smooth points on X_C.This implies that X_C is absolutely irreducible.

- The case $p = 2$ (not in the article, see Arxiv).

We prove that if X_C is not absolutely irreducible, then X_C is reducible and each component is isomorphic to C.Apply the previous bound to a component.

The question of the absolute irreducibility of X_C

• The case of $p \neq 2$.
Let $\pi_i : X_C \to C$ be the projections on the first and second factors. The morphism π_1 a degree 2-cover which ramification points are the bitangency points. Moreover if a bitangency point P is not a hyperflex, then the points in the fiber of $\pi_1^{-1}(P)$ are smooth points on X_C.This implies that X_C is absolutely irreducible.

• The case $p = 2$ (not in the article, see Arxiv).
We prove that if X_C is not absolutely irreducible, then X_C is reducible and each component is isomorphic to C.Apply the previous bound to a component.

Remark: the only case where X_C is reducible is when C is geometrically isomorphic to the Klein quartic $x^3y + y^3z + z^3x = 0$ (in particular Conjecture 1 in the paper is false).

Computation of the arithmetic genus of X_C

If $p \neq 2$ and there is no hyperflex on C, one can use Riemann-Hurwitz formula with the degree 2-cover $\pi_1 : X_C \to C$ to get g_{X_C}.

Computation of the arithmetic genus of X_C

If $p \neq 2$ and there is no hyperflex on C, one can use Riemann-Hurwitz formula with the degree 2-cover $\pi_1 : X_C \to C$ to get g_{X_C}. Then one uses a flat family argument to get π_{X_C} in general.

Computation of the arithmetic genus of X_C

If $p \neq 2$ and there is no hyperflex on C, one can use Riemann-Hurwitz formula with the degree 2-cover $\pi_1 : X_C \to C$ to get g_{X_C}. Then one uses a flat family argument to get π_{X_C} in general.

When $p = 2$, wild ramification prevents to use Riemann-Hurwitz formula so easily. We use instead intersection theory in $C \times C$.

Computation of the arithmetic genus of X_C

If $p \neq 2$ and there is no hyperflex on C, one can use Riemann-Hurwitz formula with the degree 2-cover $\pi_1 : X_C \to C$ to get g_{X_C}. Then one uses a flat family argument to get π_{X_C} in general.

When $p = 2$, wild ramification prevents to use Riemann-Hurwitz formula so easily. We use instead intersection theory in $C \times C$.

In both cases, we find that $\pi_{X_C} = 33$.

Computation of the arithmetic genus of X_C

If $p \neq 2$ and there is no hyperflex on C, one can use Riemann-Hurwitz formula with the degree 2-cover $\pi_1 : X_C \to C$ to get g_{X_C}. Then one uses a flat family argument to get π_{X_C} in general.

When $p = 2$, wild ramification prevents to use Riemann-Hurwitz formula so easily. We use instead intersection theory in $C \times C$.

In both cases, we find that $\pi_{X_C} = 33$.

Remark : unfortunately, there is a mistake in a remark of our paper (corrected in the Arxiv version). We claimed that $\pi_{X_C} = 9$ when $p = 2$. This is due to a confusion between the degree of the dual curve and the degree of the dual map π_2 (which is inseparable in this case).

The case of flexes

Let $\mathbb{P}^{14}$ be the linear system of all plane quartics over a field K and $I_0 = \{(P, \ell),\ P \in \ell\} \subset \mathbb{P}^2 \times (\mathbb{P}^2)^*$.

The case of flexes

Let $\mathbb{P}^{14}$ be the linear system of all plane quartics over a field K and $I_0 = \{(P, \ell),\ P \in \ell\} \subset \mathbb{P}^2 \times (\mathbb{P}^2)^*$. Let $I_4 \subset \mathbb{P}^{14} \times I_0$ be the locus

$$I_4 = \{(C, (P, \ell)),\ C \text{ is smooth and } P \text{ is a flex of } C \text{ with tangent line } \ell\}.$$

The case of flexes

Let $\mathbb{P}^{14}$ be the linear system of all plane quartics over a field K and $I_0 = \{(P, \ell),\ P \in \ell\} \subset \mathbb{P}^2 \times (\mathbb{P}^2)^*$. Let $I_4 \subset \mathbb{P}^{14} \times I_0$ be the locus

$$I_4 = \{(C, (P, \ell)),\ C \text{ is smooth and } P \text{ is a flex of } C \text{ with tangent line } \ell\}.$$

Theorem (Harris 79)

The Galois group of the cover $I_4 \to \mathbb{P}^{14}$ over $\mathbb{C}$ is the full symmetric group S_{24}.

The case of flexes

Let $\mathbb{P}^{14}$ be the linear system of all plane quartics over a field K and $I_0 = \{(P, \ell),\ P \in \ell\} \subset \mathbb{P}^2 \times (\mathbb{P}^2)^*$. Let $I_4 \subset \mathbb{P}^{14} \times I_0$ be the locus

$$I_4 = \{(C, (P, \ell)),\ C \text{ is smooth and } P \text{ is a flex of } C \text{ with tangent line } \ell\}.$$

Theorem (Harris 79)

The Galois group of the cover $I_4 \to \mathbb{P}^{14}$ over $\mathbb{C}$ is the full symmetric group S_{24}.

If this result is still true over $\bar{\mathbb{F}}_p$, using Chebotarev density theorem, one gets that the probability to have a plane quartic with a rational flex tends to

$$1 - \frac{1}{2!} + \frac{1}{3!} - \ldots - \frac{1}{24!} \approx 1 - \exp(-1) \approx 0.63$$

when q tends to infinity.

Harris' result over finite fields

General reduction arguments show that the Galois group remains S_{24} for almost all p.

Harris' result over finite fields

General reduction arguments show that the Galois group remains S_{24} for almost all p.However

Proposition

The Galois group over $\bar{\mathbb{F}}_3$ is S_8.

Harris' result over finite fields

General reduction arguments show that the Galois group remains S_{24} for almost all p.However

Proposition

The Galois group over $\bar{\mathbb{F}}_3$ is S_8.

This is due to the fact that the flexes of C are on a conic, which is not the case when $p \neq 3$.

Harris' result over finite fields

General reduction arguments show that the Galois group remains S_{24} for almost all p.However

Proposition

The Galois group over $\bar{\mathbb{F}}_3$ is S_8.

This is due to the fact that the flexes of C are on a conic, which is not the case when $p \neq 3$.

We conjecture that $p = 3$ is the only exception.