# Completeness

Christophe Ritzenthaler

Institut de Mathématiques de Luminy, CNRS

Montréal 04-10

e-mail: ritzenth@iml.univ-mrs.fr
web: http://iml.univ-mrs.fr/∼ritzenth/

# Edwards curves

## Definition

Let $k$ be a field of char. $\neq 2$ and $d \in k, d \neq 0, 1$. An Edwards curve is defined by

$$E_d : x^2 + y^2 = 1 + dx^2y^2.$$

Elliptic curve: $(1 : 0 : 0)$ and $(0 : 1 : 0)$ singular.

## Theorem (Edwards 07)

*Let $P = (x, y), P' = (x', y') \in E_d$ two affine points. The group law is defined by*

$$P + P' = \left( \frac{xy' + x'y}{1 + dxx'yy'}, \frac{yy' - xx'}{1 - dxx'yy'} \right)$$

*as soon as the denominators are defined.*
*Neutral element: $O := (0, 1)$.*
*Inverse: $-(x, y) = (-x, y)$.*

# Why is this model interesting ?

**Theorem (Bernstein, Lange 07)**

*The addition law is defined for every affine rational couple of points on $E_d$ if and only if $d$ is not a square or $E_d(k) = \{(\pm 1, 0), (0, \pm 1)\}$.*

- Avoid side channel attacks.
- Operations are fast (the fastest ?).
- Fast pairing (the fastest ?).
- Cover all group orders of elliptic curves divisible by 4.

Was it designed in this way ?
No! It was found analytically. And the geometric interpretation doesn't help.
Rem: New interesting genus 1 examples have been found since (Bernstein, Kohel, Lange work in progress).

Institut de Mathématiques de Luminy

# Generalization: the notion of addition laws

Let $A$ be an abelian variety over a field $k$ embedded in $\mathbb{P}^n$ by a morphism $\iota$.
Let $m : A \times A \to A$, $(x, y) \mapsto x + y$ be the group law.

## Definition

An addition law of bi-degree $(\mu, \nu)$ $\mathfrak{p} : \mathbb{P}^n \times \mathbb{P}^n \to \mathbb{P}^n$ is an $(n+1)$-tuple of polynomials

$$p_0, \ldots, p_n \in k[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$$

not all zero, bihomogenous of degree $\mu$ in $X_0, \ldots, X_n$ and of degree $\nu$ in $Y_0, \ldots, Y_n$ such that on a nonempty open set $U \subset A \times A$

$$\iota(x + y) = (p_0(\iota(x), \iota(y)) : \ldots : p_n(\iota(x), \iota(y))), \ \forall (x, y) \in U(\bar{k}).$$

# Generalization: the notion of complete

**Definition**

We say that $\mathfrak{p}$ is complete if $(A \times A)(k) \subset U$.

We can extend the definition to complete set of addition laws. Moreover if $A$ is considered over $\bar{k}$ we say that the law (or set of laws) is geometrically complete.

# Example (Kohel)

$$\begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \longrightarrow & \mathbb{A}^2 = \{z=1\} \times \{w=1\} \subset \mathbb{P}^1 \times \mathbb{P}^1 \\ (x:z) \times (y:w) & \mapsto & (xw)^2 + (yz)^2 = (zw)^2 + d(xy)^2 \\ & & x^2 \quad + \; y^2 \; = \quad 1 \quad + d(xy)^2 \end{array}$$

$$\downarrow$$

$$\begin{cases} X_0 X_3 = X_1 X_2, \\ X_1^2 + X_2^2 = X_3^2 + d X_0^2, \end{cases} \quad \subset \quad \mathbb{P}^3$$

with $X_0 = xy, X_1 = xw, X_2 = yz, X_3 = zw$.
The addition law associate to $((u_0 : u_1 : u_2 : u_3), (v_0 : v_1 : v_2 : v_3))$ the point with coordinates

$$\begin{array}{ll} \big[(u_1 v_2 + v_1 u_2) \cdot (u_2 v_2 - u_1 v_1) : & (u_1 v_2 + v_1 u_2) \cdot (u_3 v_3 - d u_0 v_0) : \\ (u_2 v_2 - u_1 v_1) \cdot (u_3 v_3 + d u_0 v_0) : & (u_3 v_3 + d u_0 v_0) \cdot (u_3 v_3 - d u_0 v_0) \big]. \end{array}$$

Completeness has nothing to do with singularities!

Institut de Mathématiques de Luminy

# Our main results (Arène, Kohel, R.)

For simplicity and the purpose of the conference, assume $k = \mathbb{F}_q$ is a finite field (but, under mild assumptions, everything works for a global field).

**Theorem**

*Every abelian variety over $k$ has an embedding for which there exists a complete addition law of bi-degree $(2, 2)$.*

Rem: for $g = 1$, this result has also been obtained over finite fields by Bernstein and Lange using explicit formulae.

**Theorem**

- *For genus 1 and $q \geq 5$, this embedding can be the Weierstrass model;*
- *For genus 2 and $q \geq 5$, this embedding is the classical embedding in $\mathbb{P}^{15}$ given by ThetaNullwerte.*

Rem: so far we cannot give them explicitly. . . and they are probably very ugly!

Institut de Mathématiques de Luminy

# How to understand group laws ?

We assume that the embedding $\iota : A \hookrightarrow \mathbb{P}^n$ is given by a complete linear system $|L|$ for some very ample line bundle $L$ on $A$ . Let $p_1, p_2 : A \times A \to A$ be the projection maps on the first and second factor.

## Theorem (Lange, Ruppert 85)

*Let $\mu, \nu$ be positive integers and*

$$M := m^* L^{-1} \otimes p_1^* L^{\mu} \otimes p_2^* L^{\nu}.$$

- *There is an addition law of bidegree $(\mu, \nu)$ on $A$ with respect to the embedding $\iota$ if and only if $H^0(A \times A, M) \neq \{0\}$;*
- *There is a geometrically complete set of addition laws of bidegree $(\mu, \nu)$ with respect to the embedding $\iota$ if and only if $|M|$ is base point-free.*

# Geometric consequences

**Corollary**

*Assume that $A$ is principally polarized (for instance a Jacobian). There exists an embedding of $A$ for which there exists a geometrically complete set of addition laws (of bidegree $(2,2)$) of order less than or equal to $3^g$.*

On the contrary, using intersection arguments:

**Proposition (Arène, Kohel, R.)**

*If $S$ is a geometrically complete set of addition laws, then $\#S > g$.*

Rem (Bosma, Lenstra 95): for $g = 1$, there exists an explicit geometrically complete set of order 2.

Institut de Mathématiques de Luminy

# Ingredients of the proof: main observation

**Lemma**

*If $M \simeq \mathcal{L}(D)$ where $D$ is an effective divisor on $A \times A$, then the section of $H^0(A \times A, M)$ with zero locus $D$ defines an addition law on the open set $U = A \times A \setminus D$.*

$\Rightarrow$ To have a complete addition law, it is then sufficient (and necessary) to construct an ample rational divisor $D$ on $A \times A$ such that $D$ has no rational point.

# The case $(2,2)$

Let $\pi : A \times A \to A$ is $(x,y) \mapsto x - y$ and let $L = \mathcal{L}(D_0)$.

**Lemma (Lange, Ruppert 85)**

*If the bidegree is* $(2,2)$ *then*

- *if* $L$ *is symmetric (i.e.* $-D_0 \sim D_0$*), then* $M \simeq \pi^* L$*;*
- *if not, then* $H^0(A \times A, M) = \{0\}$*.*

$\Rightarrow$ To have a complete addition law of bidegree $(2,2)$ it is then sufficient (and necessary) to construct a very ample rational divisor $D_0$ on $A$ such that $D_0$ has no rational point and $L = \mathcal{L}(D_0)$ is symmetric.

$\Rightarrow$ construct $D_0$ irreductible but not absolutely irreducible!

# Construction: the genus 1 case

**Lemma**

*If $q \geq 5$, there is a point $P \in E(\mathbb{F}_{q^3}) \setminus E(\mathbb{F}_q)$ such that $P_0 + P_1 + P_2 = O$.*

The divisor $D_0 = P_0 + P_1 + P_2$ is

- rational;
- without rational point;
- very ample;
- and $L = \mathcal{L}(D_0)$ is symmetric (since $-D_0 \sim -3O \sim 3O \sim D_0$).

Moreover since $D_0 \sim 3O$, the embedding is the Weierstrass model.

# Construction: the genus 2 case

Let $C : y^2 = f(x)$ be a genus 2 curve over $k = \mathbb{F}_q$ and $\bar{}$ be the canonical involution. Let $K$ be the canonical divisor on $C$.

## Lemma

- *There exists a degree* 1 *divisor* $\kappa$ *such that* $2\kappa \sim K$. *If* $\deg f = 5$, *one can take* $\kappa = \infty$.
- *For all* $z \in \mathbf{Jac}(C)(\bar{k})$ *there exists* $P, Q \in C(\bar{k})$ *such that* $z \sim P - Q$.
- *Let* $\Theta = C \subset \mathbf{Pic}^1(C)$. *If* $z \sim P - Q \in \mathbf{Jac}(C)(\bar{k})$ *then*

$$\Theta \cap (z + \Theta) = \{P, \overline{Q}\}.$$

- If $q \geq 5$, there exists $x_0 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $y^2 = f(x_0)$ has no solution in $\mathbb{F}_{q^2}$. Let $y_0$ be a solution in $\mathbb{F}_{q^4}$.
- Let $P_0 = (x_0, y_0), P_1 = (x_1, y_1), P_2 = (x_0, -y_0), P_3 = (x_1, -y_1)$ be the Galois orbit.
- Let $\alpha_0 = P_0 + P_1 - K, \alpha_1 = P_1 + P_2 - K$, $\alpha_2 = P_2 + P_3 - K$ and $\alpha_3 = P_3 + P_0 - K$.
- We can check that

$$(\Theta + \alpha_0) \cap (\Theta + \alpha_1) = \{P_2 + \alpha_0\}, \quad (\Theta + \alpha_0) \cap (\Theta + \alpha_3) = \{P_3 + \alpha_0\}.$$

- Hence $D_0 = \sum(\Theta - \kappa + \alpha_i) \subset \mathbf{Jac}(C)$ is very ample, symmetric, rational but without any rational points.

Rem: one can show that the translation divisors have to be general (*i.e.* not on $\mathbf{Sym}^r C \subset \mathbf{Pic}^r(C)$ for $r < g$).

# Construction: the general case

- Let $\phi : A \to \mathbb{P}^{n_0}$ be a finite map. By Noether's normalization theorem we may take $n_0 = g$.
- Let $\alpha$ be a primitive element in an extension of $k$ of degree $r > n_0$ and $\alpha = \alpha_0, \ldots, \alpha_{r-1}$ its conjugates.
- Let $D_1 = \phi^*(\sum H_i)$ where

$$\forall\, i \leq r-1,\ H_i : X_0 + \alpha_i X_1 + \ldots \alpha_i^{n_0} X_{n_0} = 0.$$

- $D_1$ is rational, ample but without any rational point.
- take $D_0 = 2(-D_1 + D_1)$: very ample and symmetric.

Thanks!