Structure of elliptic curves and addition laws

David R. Kohel
Institut de Mathématiques de Luminy

Barcelona
9 September 2010

Elliptic curve models

We are interested in *explicit projective models* of elliptic curves, by which we mean E/k with given embedding $\iota : E \to \mathbb{P}^r$. Associated to this embedding we set $\mathcal{L} = \mathcal{O}_E(1) := \iota^* \mathcal{O}_{\mathbb{P}^r}(1)$.

The global sections of $\mathcal{O}_{\mathbb{P}^r}$ forms a k-vector space

$$\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1)) = \bigoplus_{i=0}^{r} kX_i,$$

and $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(n))$ is the space spanned by monomials of degree n, which maps to $\Gamma(E, \mathcal{L}^n)$ (modulo the homogeneous defining ideal for $\iota : E \to \mathbb{P}^r$).

For understanding addition laws, rather than classifying curves up to arbitrary isomorphism, we will be interested in elliptic curves up to projective linear isomorphism.

Projectively normal embeddings

As an additional condition, we require that ι is *projectively normal*, characterized by:

1. $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(n)) \to \Gamma(E, \mathcal{L}^n)$ is surjective for each $n \geq 0$,

or equivalently by the isomorphism:

2. $k[X_0, \ldots, X_r]/I_E \cong \bigoplus_{n=0}^{\infty} \Gamma(E, \mathcal{L}^n)$.

For an elliptic curve with embedding ι, it suffices to assume:

3. $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1)) \to \Gamma(E, \mathcal{L})$ is surjective.

This hypothesis allows us to reduce questions about spaces of addition laws to that of spaces of global sections of sheaves.

We assume moreover that $\mathcal{L}$ is given by an effective divisor D, with a fixed isomorphism $\mathcal{L} \cong \mathcal{L}(D)$ — this is equivalent to choosing an affine patch $\mathbb{A}^r \to \mathbb{P}^r$ with

$$(x_1, \ldots, x_r) \longmapsto (1 : x_1 : \cdots : x_r).$$

The line $X_0 = 0$ then cuts out D (and we write $\mathcal{L} = \mathcal{L}(D)$).

Projective linear isomorphism and divisors

The question of projective linear isomorphisms reduces to:

Lemma

Let $E_1 \subset \mathbb{P}^{r_1}$ and $E_2 \subset \mathbb{P}^{r_2}$ be projective normal embeddings of E/k with respect to effective D_1 and D_2. There exists a projective linear (group) isomorphism $E_1 \to E_2$ if and only if $D_2 \sim D_0 < D_1$.

And similarly for torsion subgroups acting linearly:

Lemma

Let $E \subset \mathbb{P}^r$ be projective normally embedded with respect to $D > 0$, let T be in $E(\bar{k})$, and let τ_T be the translation-by-T morphism. Then $\tau_T^*(D) \sim D$ if and only if $[\deg(D)]T = O$ if and only if τ_T is induced by a projective linear automorphism of $\mathbb{P}^r$.

Consider: $D_1 = 2(O) + (T)$ and $D_2 = 3(O)$ for T in $E[2]$; then $D_1 \not\sim D_2$ but $\tau_T^*(D_2) \sim D_1$. Construct a linear scheme $E_1 \cong E_2$.

Projective linear isomorphism and divisors

Recall that a divisor is symmetric if and only if $[-1]^*D = D$ and an invertible sheaf $\mathcal{L} = \mathcal{L}(D)$ is symmetric if and only if $[-1]^*\mathcal{L} \cong \mathcal{L}$ (if and only if $[-1]^*D \sim D$).

Lemma

$\mathcal{L}(D)$ is symmetric if and only if $\mathcal{L}(D) \cong \mathcal{L}((d-1)(O)+(T))$ for some T in $E[2]$.

Lemma

If $E \subset \mathbb{P}^r$ is a projective normal embedding with respect to $D > 0$, then $[-1]$ is induced by a projective linear automorphism if and only if $\mathcal{L}(D)$ is symmetric.

The property that D is symmetric is stronger — it implies that the automorphism inducing $[-1]$ fixes the line $X_0 = 0$ (cutting out D).

Nice elliptic curve models

Putting this all together, we consider elliptic curves E/k with given projective normal embedding in $\mathbb{P}^r$ with respect to a given effective symmetric divisor D.

Consequence: $[-1]$ is a projective linear transformation.

Moreover, we will be interested in elliptic curves with torsion subgroup G stabilizing D $(= \tau_T^*(D)$ for all T in $G)$.

Consequence: G acts by projective linear transformations.

The coordinate functions $X_0, \ldots, X_r$ can be identified with sections in the k-vector space:

$$V = \Gamma(E, \mathcal{L}(D)) = \{f \in k(E) \,|\, \mathrm{div}(f) \geq -D\}.$$

Projective normality implies that their images span V.

Consequence: V is a finite $k[G]$ and $k[\langle[-1]\rangle \ltimes G]$-module.

Explicit models: Hessian model

The Hessian model H is a cubic model in $\mathbb{P}^2$ which is a universal curve over the function field of $k(X(3)) = k(d)$:

$$X^3 + Y^3 + Z^3 = dXYZ,$$

with identity $(0 : 1 : -1)$. The 3-torsion subgroup has a canonical $H[3] \cong \mu_3 \times \mathbb{Z}/3\mathbb{Z}$, such that $P = (1 : \zeta : \zeta^2)$ acts by

$$(X : Y : Z) \mapsto (X : \zeta Y : \zeta^2 Z)$$

and $Q = (1 : -1 : 0)$ acts by $(X : Y : Z) \mapsto (Y : Z : X)$. Note that H descends to $k(a) = k(d^3)$, having the model

$$aX^3 + Y^3 + Z^3 = XYZ.$$

We later generalize this to a *canonical model* of level n.

Explicit models: Jacobi model

Let J be the elliptic curve over a field of characteristic different from 2, given by the quadric intersections in $\mathbb{P}^3$:

$$\begin{aligned} aX_0^2 + X_1^2 &= X_2^2, \\ bX_0^2 + X_2^2 &= X_3^2, \\ cX_0^2 + X_3^2 &= X_1^2, \end{aligned}$$

where $a + b + c = 0$, with identity $O = (0 : 1 : 1 : 1)$ and 2-torsion points

$$T_1 = (0 : -1 : 1 : 1), \quad T_2 = (0 : 1 : -1 : 1), \quad T_3 = (0 : 1 : 1 : -1).$$

Clearly the divisor $D = (O) + (T_1) + (T_2) + (T_3)$ is that cut out by $X_0 = 0$ and satisfies $D \sim 4(O)$.

Explicit models: twisted Edwards model

The *twisted Edwards model* E/k is a degree 4 model of an elliptic curve in $\mathbb{P}^3$ given by

$$X_0^2 + dX_3^2 = aX_1^2 + X_2^2,$$
$$X_0X_3 = X_1X_2,$$

with $O = (1 : 0 : 1 : 0)$, 2-torsion point $T = (1 : 0 : -1 : 0)$, and, if $a = c^2$, there is a 4-torsion point $S = (a : 1 : 0 : 0)$.

The more typical presentation of the twisted Edwards model

$$ax^2 + y^2 = 1 + dx^2y^2,$$

is the affine patch with embedding $(x, y) \mapsto (1 : x : y : xy)$.

Explicit models: twisted Edwards model

Since x and y have degree 2 and linearly inequivalent polar divisors

$$\mathrm{div}_\infty(x) = D_1, \quad \mathrm{div}_\infty(y) = D_2,$$

it follows that $\{1, x, y, xy\}$ spans $V = \Gamma(E, \mathcal{L}(D_1 + D_2))$, and $(x, y) \mapsto (1 : x : y : xy)$ is said to be a *projective normal closure*.

Alternatively, $(x, y) \mapsto ((1 : x), (1 : y))$ is a $\mathbb{P}^1 \times \mathbb{P}^1$ embedding, and the Segre embedding :

$$((U_0 : U_1), (V_0 : V_1)) \longmapsto (U_0V_0 : U_1V_0 : U_0V_1 : U_1V_1),$$

recovers this model in $\mathbb{P}^3$. We note that D_1 $(\sim 2(O))$ and D_2 $(\sim (O) + (T))$ are nonequivalent symmetric divisors and

$$\Gamma(E, \mathcal{L}(D_1)) \otimes \Gamma(E, \mathcal{L}(D_2)) \cong \Gamma(E, \mathcal{L}(D_1 + D_2)).$$

Explicit models: Jacobi–Edwards isogeny relations

The Jacobi and Edwards models are universal models with $\Gamma(2)$ and $\Gamma_0(4)$-structures. Moreover, they represent distinct projective linear isomorphism classes, given by divisors equivalent to $4(O)$ and $3(O)+(T)$ for a 2-torsion point T, respectively, so that there is no projective linear (group) isomorphism between them.

However, the congruence groups $\Gamma(2)$ and $\Gamma_0(4)$ are conjugate in $\mathrm{PSL}_2(\mathbb{R})$, which is explained by the existence of a 2-isogeny from J with parameters (a,b,c) to E with parameters $(c,-a)$, given by

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (X_1X_2 : X_0X_2 : X_1X_3 : X_0X_3),$$

with dual

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (2X_0X_3 : X_0^2 - aX_3^2 : X_0^2 + aX_3^2 : -cX_1^2 + X_2^2).$$

Explicit models: Canonical model of level 4

The Edwards curve, with $a = 1$,

$$X_0^2 + dX_3^2 = X_1^2 + X_2^2,$$
$$X_0X_3 = X_1X_2,$$

has 4-torsion point $S = (1 : 1 : 0 : 0)$ such that τ_S is:

$$\tau_S(X_0 : X_1 : X_2 : X_3) = (X_0 : X_2 : -X_1 : -X_3),$$

defined by the matrix

$$\begin{pmatrix} 1 & & & \\ & 0 & -1 & \\ & 1 & 0 & \\ & & & -1 \end{pmatrix}$$

which is begging to be diagonalized. First we twist by $a = -1$ so that the diagonalization descends...

Explicit models: Canonical model of level 4

...then the twisted Edwards curve, with $a = -1$,

$$X_0^2 - dX_3^2 = -(X_1 - X_2)(X_1 + X_2),\ X_0X_3 = X_1X_2,$$

is isomorphic to the *canonical curve C of level 4*:

$$\begin{aligned} X_0^2 - dX_2^2 &= X_1X_3, \\ X_1^2 - X_3^2 &= 4X_0X_2, \end{aligned}$$

via the isomorphism

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (X_0 : X_1 + X_2 : X_3 : -X_1 + X_2).$$

This curve has identity $(1 : 1 : 0 : 1)$ and the point $(i : 1 : 0 : 0)$ on E maps to $(1 : i : 0 : -i)$ on C, which acts by

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (X_0 : iX_1 : -X_2 : -iX_3).$$

Explicit models: Canonical model of level n

We can formally define a canonical model C/k to be an elliptic curve with subgroup scheme $G \cong \mu_n$, embedded in $\mathbb{P}^r$ for $r = n - 1$, such that for an n-th root of unity ζ in $\bar{k}$ there exists T in $G(k(\zeta))$ with

$$\tau_T(X_0 : X_1 : \cdots : X_r) \longmapsto (X_0 : \zeta X_1 : \cdots : \zeta^r X_r).$$

Moreover, there exists S in $C(\bar{k})$ such that $\langle S, T \rangle = C[n]$ and for some $a_0, \ldots, a_r$ in $\bar{k}$,

$$\tau_S(X_0 : X_1 : \cdots : X_r) \longmapsto (a_1 X_1 : \cdots : a_r X_r : a_0 X_0).$$

This generalizes the Hessian model and the diagonalized Edwards model (of the -1 twist).

Explicit models: Canonical model of level 5

A canonical model can be constructed by writing down a universal curve C with n-torsion point T over $k(X_1(n), \zeta_n)$, embedding with respect to the divisor with support on $\langle T \rangle$ ($\sim n(O)$ if n is odd), and diagonalizing the G-action.

Carrying this out for $n = 5$ yields the following canonical model $C/k(t)$ be the elliptic curve in $\mathbb{P}^4$ can be defined by

$$\begin{aligned} tX_0^2 + X_2X_3 &= X_1X_4, \\ tX_0X_1 + X_2X_4 &= X_3^2, \\ X_0X_2 + X_1^2 &= X_3X_4, \\ X_0X_3 + X_1X_2 &= X_4^2, \\ tX_0X_4 + X_2^2 &= X_1X_3, \end{aligned}$$

with identity $O = (0 : 1 : 1 : 1 : 1)$ and $T = (0 : \zeta : \zeta^2 : \zeta^3 : \zeta^4)$.

The genus of $X(5)$ is zero, its function field is generated by u with $u^5 = t$, and $S = (1 : u : -u^2 : u^3 : 0)$ is 5-torsion.

Addition law structure

Let $E \subset \mathbb{P}^r$ be projectively normal and let $\mu : E \times E \to E$ be the group morphism. An *addition law* of bidegree (m, n) for E is an $r+1$-tuple $(p_0, \ldots, p_r)$ of polynomials in

$$k[X_0, \ldots, X_r]/I_E \otimes k[X_0, \ldots, X_r]/I_E.$$

such that each p_j is bihomogeneous of bidegree (m, n), and

$$(x, y) \mapsto (p_0(x, y) : \cdots : p_n(x, y))$$

determines μ on an open subset. The *exceptional set* on $E \times E$ $p_0 = \cdots = p_r = 0$, is an effective divisor on $E \times E$ for any nonzero addition law. The set of addition laws of bidegree (m, n) is a finite dimensional vector space.

Interlude: definitions and notation

Let $\pi_i : E \times E \to E$, be the projection onto the i-th component, $\mu : E \times E \to$ be the group morphism, and $\delta : E \times E \to E$ the difference morphism. Moreover we define divisors on $E \times E$ by

$$\pi_1^*((P)) = V_P \quad \pi_2^*((P)) = H_P$$
$$\mu^*((P)) = \nabla_P \quad \delta^*((P)) = \Delta_P$$

When $P = O$ (the group identity) we drop the subscript.
More generally we define the graphs

$$\Gamma_{a,b} = \{(aP, bP) : P \in E\},$$

and note that

$$V = \Gamma_{0,1}, \quad H = \Gamma_{1,0}, \quad \nabla = \Gamma_{1,-1}, \quad \Delta = \Gamma_{1,1}.$$

Addition laws as sections of sheaves

In order to understand the spaces of addition laws on abelian varieties, Lange & Ruppert interpret these spaces as

$$\mathrm{Hom}(\mu^*\mathcal{L}, \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n),$$

and observe that this space is isomorphic to the global sections:

$$\Gamma(E \times E, \mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n).$$

Note. If $\mathcal{L} = \mathcal{L}(d(O))$, then

$$\mathcal{M}_{m,n} := \mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n = \mathcal{L}(-d\nabla + mdV + ndH).$$

In order to determine the existence and dimensions of the spaces of addition laws, we want to find $\mathcal{M}_{m,n} \cong \mathcal{L}(D)$ for an effective divisor D on $E \times E$, and for $(m, n) = (2, 2)$ we have $D = d\Delta$.

Lange & Ruppert Theorem

A set of addition laws is *geometrically complete* or *complete* if the intersection of their exceptional sets is the empty scheme in $E \times E$. A set is *arithmetically complete* or *k-complete* if the intersection contains no k-rational point. **Remark.** A set S of addition laws is complete if and only the vector space spanned by S is complete.

Theorem (Lange & Ruppert)

The sets of addition laws of bidegree $(2,3)$ *and* $(3,2)$ *are complete. If* $\mathcal{L}$ *is symmetric, then the set of addition laws of bidegree* $(2,2)$ *is complete, and otherwise empty.*

This suggests that, for a symmetric sheaf $\mathcal{L}$, the sheaf

$$\mathcal{M} = \mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^2 \otimes \pi_2^*\mathcal{L}^2.$$

associated to the critical bidegree $(2,2)$ plays an important role.

Addition laws of bidegree $(2,2)$

The following theorem is a generalization of a result in Bosma & Lenstra for the divisor $D = 3(O)$, following Lange & Ruppert.

Theorem

Let $\mathcal{L}$ be a symmetric divisor and $\mathcal{M} = \mu^*\mathcal{L} \otimes \pi_1^*\mathcal{L}^2 \otimes \pi_2^*\mathcal{L}^2$.

1. *$\delta^* : \Gamma(E, \mathcal{L}) \to \Gamma(E \times E, \mathcal{M})$ is an isomorphism.*
2. *The exceptional divisor of an addition law of bidegree $(2,2)$ is an effective divisor of the form $\delta^* D$ for D effective such that $\mathcal{L} \cong \mathcal{L}(D)$.*

In particular, the dimension of the space of addition laws is $\deg(\mathcal{L})$ and the components of the exceptional divisor are of the form Δ_P.

Explicit addition laws: Hessian model

Theorem

The space of addition laws of bidegree $(2,2)$ *on* H *is spanned by:*

$$(X_1^2Y_2Z_2 - Y_1Z_1X_2^2,\ Z_1^2X_2Y_2 - X_1Y_1Z_2^2,\ Y_1^2X_2Z_2 - X_1Z_1Y_2^2),$$
$$(X_1Y_1Y_2^2 - Z_1^2X_2Z_2,\ X_1Z_1X_2^2 - Y_1^2Y_2Z_2,\ Y_1Z_1Z_2^2 - X_1^2X_2Y_2),$$
$$(X_1Z_1Z_2^2 - Y_1^2X_2Y_2,\ Y_1Z_1Y_2^2 - X_1^2X_2Z_2,\ X_1Y_1X_2^2 - Z_1^2Y_2Z_2).$$

This is all consistent with expectations in the theory of Lange & Ruppert, and the structure of the exceptional divisors is exactly as described in Bosma & Lenstra.

Explicit addition laws: Jacobi model

Theorem

The space of addition laws of bidegree $(2,2)$ *for* J *is spanned by :*

$$\begin{array}{ll}
(X_0^2Y_1^2 - X_1^2Y_0^2, & (X_0X_2Y_1Y_3 + X_1X_3Y_0Y_2,\\
X_0X_1Y_2Y_3 - X_2X_3Y_0Y_1, & -aX_0X_3Y_0Y_3 + X_1X_2Y_1Y_2,\\
X_0X_2Y_1Y_3 - X_1X_3Y_0Y_2, & abX_0^2Y_0^2 + X_2^2Y_2^2,\\
X_0X_3Y_1Y_2 - X_1X_2Y_0Y_3) & bX_0X_1Y_0Y_1 + X_2X_3Y_2Y_3)\\
\\
(X_0X_1Y_2Y_3 + X_2X_3Y_0Y_1, & (a(X_0X_3Y_1Y_2 + X_1X_2Y_0Y_3),\\
acX_0^2Y_0^2 + X_1^2Y_1^2, & a(cX_0X_2Y_0Y_2 + X_1X_3Y_1Y_3),\\
aX_0X_3Y_0Y_3 + X_1X_2Y_1Y_2, & a(-bX_0X_1Y_0Y_1 + X_2X_3Y_2Y_3),\\
-cX_0X_2Y_0Y_2 + X_1X_3Y_1Y_3) & -bX_1^2Y_1^2 - cX_2^2Y_2^2).
\end{array}$$

Explicit addition laws: Canonical model of level 4

Theorem

The space of addition laws of bidegree $(2,2)$ *for* C *is spanned by :*

$$\begin{pmatrix} -(X_1^2Y_3^2 - X_3^2Y_1^2)/4, \\ X_0X_3Y_1Y_2 - X_1X_2Y_0Y_3, \\ X_0^2Y_2^2 - X_2^2Y_0^2, \\ X_0X_1Y_2Y_3 - X_2X_3Y_0Y_1), \end{pmatrix} \quad \begin{pmatrix} X_0X_1Y_0Y_3 + dX_2X_3Y_1Y_2, \\ 4dX_0X_2Y_2^2 + X_1^2Y_1Y_3, \\ X_0X_3Y_2Y_3 + X_1X_2Y_0Y_1, \\ X_1X_3Y_3^2 - 4dX_2^2Y_0Y_2) \end{pmatrix}$$

$$\begin{pmatrix} X_0^2Y_0^2 - e^8X_2^2Y_2^2, \\ X_0X_1Y_0Y_1 - e^4X_2X_3Y_2Y_3, \\ (X_1^2Y_1^2 - X_3^2Y_3^2)/4, \\ X_0X_3Y_0Y_3 - dX_1X_2Y_1Y_2) \end{pmatrix} \quad \begin{pmatrix} X_0X_3Y_0Y_1 + e^4X_1X_2Y_2Y_3, \\ X_1X_3Y_1^2 + 4dX_2^2Y_0Y_2, \\ X_0X_1Y_1Y_2 + X_2X_3Y_0Y_3, \\ -4dX_0X_2Y_2^2 + X_3^2Y_1Y_3) \end{pmatrix}$$

Exotic addition laws: Hessian model

Let's consider the Hessian model again. If we take the projections to coordinates

$$(X, X - T), \quad (Y, Y - T), \text{ and } (Z, Z - T),$$

where $T = X + Y + Z$, we find addition laws of bidegree $(2, 1)$

$$\begin{aligned}
&(Y_1 Z_1 X_2 + X_1 Y_1 Y_2 + X_1 Z_1 Z_2,\ X_1^2 X_2 + Z_1^2 Y_2 + Y_1^2 Z_2),\\
&(X_1 Z_1 X_2 + Y_1 Z_1 Y_2 + X_1 Y_1 Z_2,\ Y_1^2 X_2 + X_1^2 Y_2 + Z_1^2 Z_2),\\
&(X_1 Y_1 X_2 + X_1 Z_1 Y_2 + Y_1 Z_1 Z_2,\ Z_1^2 X_2 + Y_1^2 Y_2 + X_1^2 Z_2),
\end{aligned}$$

and of bidegree $(1, 2)$:

$$\begin{aligned}
&(X_1 Y_2 Z_2 + Y_1 X_2 Y_2 + Z_1 X_2 Z_2,\ X_1 X_2^2 + Y_1 Z_2^2 + Z_1 Y_2^2),\\
&(X_1 X_2 Z_2 + Y_1 Y_2 Z_2 + Z_1 X_2 Y_2,\ X_1 Y_2^2 + Y_1 X_2^2 + Z_1 Z_2^2),\\
&(X_1 X_2 Y_2 + Y_1 X_2 Z_2 + Z_1 Y_2 Z_2,\ X_1 Z_2^2 + Z_1 X_2^2 + Y_1 Y_2^2).
\end{aligned}$$

Each of these addition laws spans a unique one-dimensional space.

Additional tools needed

The previous example requires us to understand addition law projections: a tuple of polynomials which interpolate the composition of the group law with a projection $\phi : E \to \mathbb{P}^1$:

$$E \times E \to E \to \mathbb{P}^1.$$

If the projection ϕ is given by an effective divisor D_1 then we are led to the global sections of the sheaves:

$$\mathcal{M}_{\phi,m,n} = \mu^{-1}\mathcal{L}(D_1) \otimes \pi_1^*\mathcal{L}(D)^m \otimes \pi_2^*\mathcal{L}(D)^n.$$

For $\deg(D_1) < \deg(D)$ we find more sections, of lower bidegrees, than for the global problem.

The Euler-Poincaré characteristic

For a projective variety X/k and a sheaf $\mathcal{F}$, and let $\chi(X, \mathcal{F})$ be the Euler-Poincaré characteristic:

$$\chi(X, \mathcal{F}) = \sum_{i=0}^{\infty} (-1)^i \dim_k(H^i(X, \mathcal{F})).$$

For the classification of divisors or invertible sheaves of X, we have considered the *linear equivalence* classes in $\mathrm{Pic}(X)$. In order to determine the dimensions of spaces of addition laws, it suffices to consider the coarser *algebraic equivalence* class in the *Néron-Severi group* of X, defined as

$$\mathrm{NS}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X).$$

The coarsest equivalence class is numerical, but...

Lemma

If X is an abelian variety then $\mathrm{NS}(X) = \mathrm{Num}(X)$.

The Euler-Poincaré characteristic

We've expressed addition laws in terms of global sections of a sheaf, and the Euler-Poincaré characteristic is a tool for understanding the dimension of the space of global sections

$$H^0(X, \mathcal{F}) = \Gamma(X, \mathcal{F}),$$

provided we can establish the vanishing of all other $H^i(X, \mathcal{F})$. For the surfaces $E \times E$, we can compute $\chi(E \times E, \mathcal{L})$:

Theorem

Let E *be an elliptic curve and* $\mathcal{L}$ *be an invertible sheaf on* $E \times E$. *The Euler-Poincaré characteristic* $\chi(E \times E, \mathcal{L})$ *depends only on the numerical equivalence class of* $\mathcal{L}$, *and in particular*

$$\chi(E \times E, \mathcal{L}(D)) = \frac{1}{2} D.D.$$

If $\mathcal{L}$ *is ample, then* $\chi(E \times E, \mathcal{L}) = \dim_k(\Gamma(E \times E, \mathcal{L})$.

The Neron-Serveri group

Lemma

The following diagram is exact.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \mathrm{Pic}^0(E) \times \mathrm{Pic}^0(E) & \longrightarrow & \mathrm{Pic}^0(E \times E) & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Pic}(E) \times \mathrm{Pic}(E) & \xrightarrow{\pi_1^* \times \pi_2^*} & \mathrm{Pic}(E \times E) & \longrightarrow & \mathrm{End}(E) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{NS}(E) \times \mathrm{NS}(E) & \longrightarrow & \mathrm{NS}(E \times E) & \longrightarrow & \mathrm{End}(E) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

In particular if $\mathrm{End}(E) \cong \mathbb{Z}$ then $\mathrm{NS}(E) \cong \mathbb{Z}^3$.

The Neron-Serveri group

Lemma

The Neron-Severi group $\mathrm{NS}(E \times E)$ *is a finitely generated free abelian group, and if* $\mathrm{End}(E) \cong \mathbb{Z}$, *it is generated by* V, H, Δ, *and* ∇, *modulo the relation* $\Delta + \nabla \equiv 2V + 2H$. *The intersection product is nondegenerate on* $\mathrm{NS}(E \times E)$ *and given by*

	V	H	Δ	∇
V	0	1	1	1
H	1	0	1	1
Δ	1	1	0	4
∇	1	1	4	0

Euler-Poincaré characteristic on $\mathrm{NS}(E \times E)$

Theorem (Lange-Ruppert)

Let E be an elliptic curve, then

$$\chi(E \times E, \mathcal{L}(x_0\nabla + x_1 V + x_2 H)) = x_0x_1 + x_0x_2 + x_1x_2.$$

Corollary

If $\mathcal{L}$ is an invertible sheaf of degree $d > 0$ on E, then

$$\chi(E \times E, \mathcal{M}_{m,n}) = d^2(mn - m - n).$$

and if $\deg(\phi)$ is a projection to $\mathbb{P}^1$ then

$$\chi(E \times E, \mathcal{M}_{\phi,m,n}) = d(dmn - d_1(m + n)).$$

Trivial Euler-Poincaré characteristic

Roughly, if $\chi(E \times E, \mathcal{M}_{\phi,m,n})$ is positive, then $\mathcal{M}_{\phi,m,n})$ is ample and the Euler-Poincaré characteristic gives us the dimension of the space of addition laws. The critical cases, for which

$$\chi(E \times E, \mathcal{M}_{\phi,m,n}) = 0$$

are:

d	d_1	(m,n)	$\dim(\Gamma(E \times E, \mathcal{M})^\dagger$
3	2	$(1,2),(2,1)$	1
4	2	$(1,1)$	2
$2d_1$	d_1	$(1,1)$	d_1
d	d	$(2,2)$	d

$\dagger =$ or 0 — we still need to address the gap between linear and algebraic (= numerical) equivalence.

Fortunately, in the case of zero Euler-Poincaré characteristic, we can exactly parametrize the numerical equivalence classes.

Numerical equivalence for $\chi = 0$

Lemma

The divisor $\Gamma_{(a,b)}$ is numerically equivalent to

$$-ab\nabla + (a^2 + ab)V + (ab + b^2)H.$$

Theorem

A divisor D on $E \times E$ satisfies $\chi(E \times E, \mathcal{L}(D) = 0$ if and only if D is numerically equivalent to $n\,\Gamma_{(a,b)}$ for integers n, a and b.

In the case of our exotic linear equivalence we can now explain the one-dimensional spaces of addition laws by isomorphisms

$$\mathcal{L}(\Gamma_{1,2}) \cong \mathcal{L}(-2\nabla + 3V + 6H) \text{ and } \mathcal{L}(\Gamma_{2,1}) \cong \mathcal{L}(-2\nabla + 6V + 3H),$$

first established up to numerical equivalence, then by constructing a linear equivalence.

Magical factorization of Edwards

A similar construction for $(d, d_1) = (4, 2)$ explains the magical factorizations (first observed by Hisil) of the Edwards addition laws through $\mathbb{P}^1 x \mathbb{P}^1$:

Theorem

The space of addition laws projections $E \times E \to \mathbb{P}^1$ of bidegree $(1,1)$ is spanned (for $(X_0 : X_1)$) by

$$(X_0 Y_0 + dX_3 Y_3, X_1 Y_2 + X_2 Y_1),$$
$$(aX_1 Y_1 + X_2 Y_2, X_0 Y_3 + X_3 Y_0),$$

and (for $(X_0 : X_2)$) by

$$(X_0 Y_0 - dX_3 Y_3,\ -aX_1 Y_2 + X_2 Y_1),$$
$$(-X_1 Y_2 + X_2 Y_1,\ X_0 Y_3 - X_3 Y_0).$$