

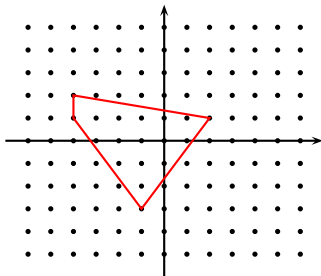
# Forms of elliptic curves

Wouter Castryck and Fré Vercauteren

Pairings in Arithmetic Geometry and Cryptography

## Lattice polytopes

- ▶ A **lattice polytope**  $\Delta$  is a convex polytope in  $\mathbb{R}^2$  with integer vertex coordinates.



- ▶ Faces of  $\Delta$  are typed by dimension:  $\Delta$  itself (2-dim), edges (1-dim), vertices (0-dim).
- ▶ Boundary of  $\Delta$  is union of edges and denoted  $\partial\Delta$ .
- ▶ The **genus** is the number of interior lattice points.

## Toric surface

- ▶ To lattice polytope  $\Delta \subset \mathbb{R}^2$ , associate toric surface  $X(\Delta)$ .
- ▶ To each point  $(i, j) \in \Delta \cap \mathbb{Z}^2$ , associate a variable  $z_{ij}$ .
- ▶ Let  $N = \#(\Delta \cap \mathbb{Z}^2) - 1$ , then  $X(\Delta)$  lives in  $\mathbb{P}^N$ .
- ▶ Divide out by **binomial relations** in  $k[z_{ij}]$ : for  $\alpha_1 + \alpha_2 = \beta_1 + \beta_2$  with  $\alpha_i, \beta_i$  integers and

$$\alpha_1(i_1, j_1) + \alpha_2(i_2, j_2) = \beta_1(k_1, l_1) + \beta_2(k_2, l_2)$$

we have the relation

$$z_{i_1 j_1}^{\alpha_1} z_{i_2 j_2}^{\alpha_2} = z_{k_1 l_1}^{\beta_1} z_{k_2 l_2}^{\beta_2}$$

- ▶ These relations define a projective surface  $X(\Delta) \subset \mathbb{P}^N$ , which is called the **toric surface associated to  $\Delta$** .

## Toric surface

- ▶ The torus  $\mathbb{T}_k^2 = (\bar{k} \setminus \{0\})^2$  can be embedded in  $X(\Delta)$  by

$$\mathbb{T}_k^2 \hookrightarrow X(\Delta) : (x, y) \mapsto (x^i \cdot y^j)_{(i,j) \in \Delta \cap \mathbb{Z}^2}$$

- ▶ To each face  $\tau \in \Delta$  associate toric orbit

$$\Theta(\tau) = \{(\alpha_{ij})_{(i,j) \in \Delta \cap \mathbb{Z}^2} \in X(\Delta) \mid \alpha_{ij} \neq 0 \Leftrightarrow (i, j) \in \tau\}$$

- ▶ Each orbit  $\Theta(\tau)$  is isomorphic to torus  $\mathbb{T}_k^{\dim \tau}$  and

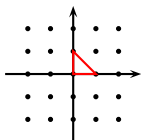
$$X(\Delta) \cong \mathbb{T}_k^2 \cup T_1 \cup \dots \cup T_r \cap P_1 \cup \dots \cup P_r,$$

with  $r$  the number of edges of  $\Delta$ .

- ▶ Points in  $X(\Delta) \setminus \Theta(\Delta)$  lie at toric infinity.

# Toric surfaces

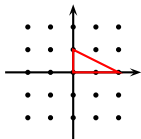
- ▶ **Example:** let  $\Delta$  be the polytope



- ▶ There are three variables:  $z_{00}, z_{10}, z_{01}$ , subject to no relations.
- ▶ Thus  $X(\Delta)$  is the projective plane  $\mathbb{P}^2$ .

## Toric surfaces

- ▶ **Example:** let  $\Delta$  be the polytope

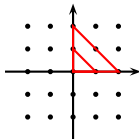


- ▶ There are four variables:  $z_{00}, z_{10}, z_{20}, z_{01}$ , subject to the single relation

$$z_{10}^2 = z_{00}z_{20}.$$

- ▶ Thus  $X(\Delta)$  is a cone in  $\mathbb{P}^3$ , which is in fact the weighted projective plane  $\mathbb{P}(1, 2, 1)$ .
- ▶ Consider  $\phi : \mathbb{P}(1, 2, 1) \rightarrow \mathbb{P}^3 : (x, y, z) \mapsto (z^2, xz, x^2, y)$  then  $\phi(\mathbb{P}(1, 2, 1)) = X(\Delta)$ .

# Toric surfaces



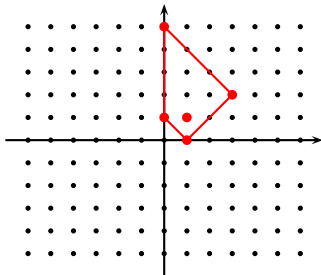
## Theorem

If  $\Delta = k\Delta'$  for some smaller lattice polytope  $\Delta'$ , then  $X(\Delta) \cong X(\Delta')$ .

- ▶ Thus for all triangles  $\Delta = (0,0)-(0,d)-(d,0)$  we have  $X(\Delta) \cong \mathbb{P}^2$ .

## The Newton polytope

- ▶ The **Newton polytope** of a bivariate Laurent polynomial is the convex hull in  $\mathbb{R}^2$  of its exponent vectors.
- ▶ Example: consider  $f = x^3y^2 + 2y^5 - x + 4xy + 8y$ .



- ▶ We denote the Newton polytope with  $\Delta(f)$ .

## Nondegenerate wrt Newton Polytope

- ▶ Let  $f(x, y) = \sum_{(i,j) \in S} f_{i,j} x^i y^j \in k[\mathbb{Z}^2]$  be a Laurent polynomial with Newton polytope  $\Delta(f)$ .
- ▶ For each face  $\tau$  of  $\Delta$ , define  $f_\tau(x, y) = \sum_{(i,j) \in \tau \cap \mathbb{Z}^2} f_{i,j} x^i y^j$ .
- ▶ Then  $f$  is called **nondegenerate** with respect to its Newton polygon if for all faces  $\tau$ , the system of equations

$$f_\tau = \frac{\partial f_\tau}{\partial x} = \frac{\partial f_\tau}{\partial y} = 0$$

has no solutions in the torus  $\mathbb{T}_k^2$ , i.e.  $(\bar{k} \setminus \{0\})^2$ .

- ▶ Implies that curve  $f(x, y) = 0$  is non-singular in  $\mathbb{T}_k^2$ , but much more!
- ▶ For every  $\Delta$ , generically chosen  $f$  with Newton polytope will be nondegenerate.

## Toric resolution

- ▶ Associate to  $\Delta(f)$  its toric surface  $X(\Delta(f))$ .
- ▶ Let  $f(x, y) = \sum_{(i,j) \in \Delta(f)} f_{i,j} x^i y^j$  be a Laurent polynomial, then we obtain linear relation in  $\mathbb{P}^N$  by

$$\sum_{(i,j) \in \Delta(f)} f_{i,j} z_{ij} = 0.$$

- ▶ Intersection with  $X(\Delta(f))$  cuts out curve  $\tilde{C}$  that satisfies:
  - ▶  $\tilde{C}$  is nonsingular,
  - ▶ Intersects the 1-dimensional orbits transversally in  $\#(\tau \cap \mathbb{Z}^2) - 1$  points,
  - ▶ Does not contain the 0-dimensional orbits,
  - ▶ Number of points at toric infinity equals  $\#(\partial\Delta \cap \mathbb{Z}^2)$ .

# Genus

- ▶ Let  $f(x, y) = \sum_{(i,j) \in \Delta(f)} f_{i,j} x^i y^j$  be a Laurent polynomial and consider the curve  $C$  defined by  $f(x, y) = 0$  in  $\mathbb{T}_k^2$ .
- ▶ **Baker's inequality**: the geometric genus  $g(\tilde{C})$  is bounded by  $\#((\Delta(f) \setminus \partial\Delta(f)) \cap \mathbb{Z}^2)$ .
- ▶ If  $f$  is **nondegenerate** with respect to  $\Delta(f)$  then

$$g(\tilde{C}) = \#((\Delta(f) \setminus \partial\Delta(f)) \cap \mathbb{Z}^2).$$

# Elliptic curves

- ▶ An elliptic curve  $E/k$  is a non-singular projective genus 1 curve with a  $k$ -rational point  $O$ .
- ▶ Weierstrass equation: elliptic curve is isomorphic over  $k$  to

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

along with the point  $(0, 1, 0)$  at infinity.

- ▶ A plane curve  $C \subset \mathbb{P}^2$  along with a base point  $O \in C(k)$  is elliptic if and only if it is nonsingular and of degree 3.

## Finding new forms of elliptic curves

- ▶ Consider all lattice polytopes  $\Delta$  with 1 interior point.
- ▶ Any generic equation  $f$  with such Newton polytope and rational point defines an elliptic curve.
- ▶ To limit possibilities, consider  $\mathbb{Z}$ -affine equivalence, i.e.

$$e : \mathbb{R}^2 \rightarrow \mathbb{R}^2 : \begin{bmatrix} i \\ j \end{bmatrix} \mapsto A \cdot \begin{bmatrix} i \\ j \end{bmatrix} + \begin{bmatrix} a \\ b \end{bmatrix}$$

for  $a, b \in \mathbb{Z}$  and  $A \in GL_2(\mathbb{Z})$ .

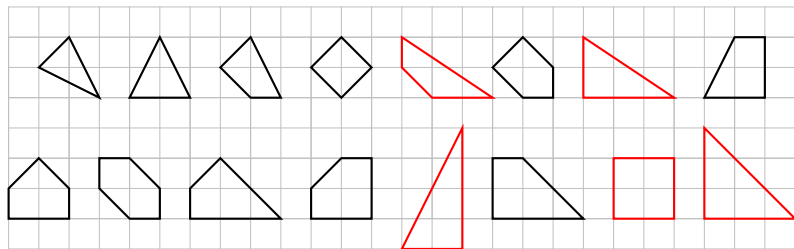
- ▶  $\Delta$  is equivalent with  $\Delta'$  iff exists  $e$  with  $\Delta = e(\Delta')$ .
- ▶ Two polynomials  $f$  and  $f'$  are equivalent if  $f_{i,j} = f'_{e(i,j)}$ .
- ▶ Defines isomorphic curves in  $\mathbb{T}_2$ .
- ▶ Nondegenerateness invariant under equivalence.

# Lattice polytopes of genus one

## Theorem

Up to affine equivalence, for every genus  $g$  there is a finite number of lattice polytopes.

The lattice polytopes of genus 1 ([Poonen/Rodriguez-Villegas](#)):



## Weierstrass equation revisited

- ▶ Short Weierstrass equation  $y^2 = x^3 + Ax + B$ .
- ▶ Can consider curve in  $\mathbb{P}^2$ , then obtain

$$y^2z = x^3 + Axz^2 + Bz^3,$$

with  $O = (0, 1, 0)$ .

- ▶ Weighted projective coordinates in  $\mathbb{P}(2, 3, 1)$ , then

$$y^2 = x^3 + Axz^4 + Bz^6,$$

with  $O = (1, 1, 0)$ .

- ▶ Often called **Jacobian form**.
- ▶ Equivalence relation in  $\mathbb{P}(2, 3, 1)$  is

$$(x, y, z) \cong (\lambda^2x, \lambda^3y, \lambda z).$$

## Weierstrass equation revisited

- ▶ Recover these by looking at  $X(\Delta(f)) \cong \mathbb{P}(2, 3, 1)$ .

- ▶  $X(\Delta(f)) \subset \mathbb{P}_k^6$  defined by binomial relations

$$z_{00}z_{20} = z_{10}^2, z_{10}z_{20} = z_{00}z_{30}, z_{11}z_{00} = z_{01}z_{10}, z_{02}z_{00} = z_{01}^2$$

- ▶ Consider  $\phi : \mathbb{P}(2, 3, 1) \rightarrow \mathbb{P}^6$  defined as

$$\phi(x, y, z) = (z^6, xz^4, x^2z^2, x^3, yz^3, xyz, y^2)$$

then  $\phi(\mathbb{P}(2, 3, 1)) = X(\Delta(f))$ .

- ▶ Elliptic curve is then the hyperplane section

$$z_{02} = z_{30} + A_1z_{10} + A_2z_{00}$$

and  $O$  corresponds to  $(0; 0; 0; 1; 0; 0; 1)$ .

Edwards form  $x^2z^2 + y^2z^2 = A^2(z^4 + x^2y^2)$ 

- ▶ An **Edwards** form is a curve in  $\mathbb{P}^3$  given by

$$\begin{cases} xy = zw \\ x^2 + y^2 = A^2(z^2 + w^2), \end{cases}$$

where  $A^5 - A \neq 0$  and  $O = (0, A, 1, 0)$ .

- ▶ Projecting from  $(0, 0, 0, 1)$  onto  $\mathbb{P}^2$  corresponds to substituting

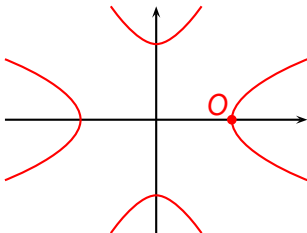
$$\begin{pmatrix} x & y & z & w \\ xz & yz & z^2 & xy \end{pmatrix},$$

from which we retrieve the plane Edwards equation

$$x^2z^2 + y^2z^2 = A^2(z^4 + x^2y^2).$$

Edwards form  $x^2z^2 + y^2z^2 = A^2(z^4 + x^2y^2)$ 

- ▶ The plane form is **not** an elliptic curve  $\rightsquigarrow$  2 singularities at infinity, which represent 4 points on the nonsingular model.



- ▶ Space curve is isomorphic to plane cubic

$$y^2 = (2Ax - 1)((1 - A^2)x + A)((1 + A^2)x - A).$$

Edwards form  $x^2z^2 + y^2z^2 = A^2(z^4 + x^2y^2)$ 

- ▶ Linear functions  $\alpha x + \beta y + \gamma$  on cubic form read

$$\frac{\alpha y(1 - A^2x^2)(A + x)^3 + \beta + \gamma(A + x)}{A + x}$$

on the Edwards form...

- ▶ Yet miraculously, the addition law in the affine part reads

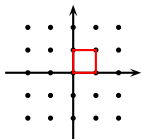
$$(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1y_2 + y_1x_2}{A(1 + x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{A(1 - x_1x_2y_1y_2)} \right)$$

(both for **addition** and **doubling**) and

$$-(x_1, y_1) = (-x_1, y_1).$$

# The Newton polytope

- ▶ **Example:** consider  $f(x, y) = x^2 + y^2 - A^2(1 + x^2y^2)$ , whose Newton polytope equals  $2\Delta$ , where  $\Delta$  is



- ▶  $X(\Delta) \subset \mathbb{P}^3$  is defined by

$$z_{00}z_{11} = z_{10}z_{01}.$$

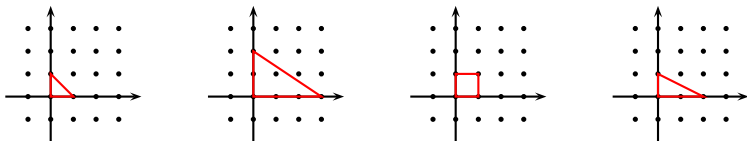
- ▶  $f$  defines the additional degree **2** relation

$$z_{10}^2 + z_{01}^2 = A^2(z_{00}^2 + z_{11}^2).$$

- ▶ We find the nonsingular Edwards model in  $\mathbb{P}^3$ !

# Observation

- ▶ **Observation:** all nonsingular forms of elliptic curves that have proven to be useful, canonically lie in a toric surface.
- ▶ Plane cubics (e.g. Hessian) lie in  $\mathbb{P}^2$ .
- ▶ Weighted Weierstrass curves lie in  $\mathbb{P}(2, 3, 1)$ .
- ▶ Edwards curves lie in  $\mathbb{P}^1 \times \mathbb{P}^1$ .
- ▶ Quartic Jacobian forms lie in  $\mathbb{P}(1, 2, 1)$ .



## Searching for efficient forms

- ▶ Look at the 16 equivalence classes and derive addition/doubling formulae for all
  - ▶  $O$  chosen as point at toric infinity
  - ▶ Canonical projective coordinate system coming from  $X(\Delta(f))$
- ▶ Exhaustive strategy:
  - ▶ For a degree bound  $B$ , list all genus 1 lattice polygons of total degree less than  $B$
  - ▶ For each of these possibilities, find the best addition/doubling formulae possible

## Finding the most efficient group law

For each genus 1 lattice polytope: repeat

- ▶ Choose base face  $\sigma \subset \Delta$ , and set coefficient of outer vertices 1 and  $-1$  and the others 0
- ▶ The point  $O$  then corresponds to a rational point on  $\mathbb{T}_\sigma$ .
- ▶ Choose vertex not on face, and assign parametrised coefficient  $c$
- ▶ Assign 1 to other vertices
- ▶ Assign 0 or 1 to other points not on  $\sigma$
- ▶ Results in a 1-parameter family of curves, e.g.

$$cx^2y^2 + x^4 - x^2 + y^2$$

with base face  $[\langle 0, 2 \rangle, \langle 1, 1 \rangle, \langle 2, 0 \rangle]$ .

## Finding the most efficient doubling law

For each such family do the following:

- ▶ Affine doubling formulae can be written as

$$D(x, y) = \left( \frac{f_1(x, y)}{g_2(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right)$$

- ▶ Choose set  $S$  such that support of  $f_i, g_i$  is limited to  $S$
- ▶ Consider  $U = S \cup cS$ , then we can express  $f_i, g_i$  on  $U$  using  $8|S|$  unknowns
- ▶ Find all possible doubling laws using interpolation

## Finding the most efficient doubling law

- ▶ Choose large finite field  $\mathbb{F}_p$
- ▶ Choose random coefficient  $\bar{c} \in \mathbb{F}_p$  defining curve  $C_{\bar{c}}$
- ▶ Find a random point  $P$  on  $C_{\bar{c}}$  and compute

$$P = (x_0, y_0), [2]P = (x_1, y_1), \dots, [2^k]P = (x_k, y_k)$$

for  $k \gg 4|S|$

- ▶ Each doubling gives rise to two linear equations

$$f_1(x_i, y_i) = g_1(x_i, y_i)x_{i+1} \quad \text{and} \quad f_2(x_i, y_i) = g_2(x_i, y_i)y_{i+1}$$

- ▶ **Kernel** describes **all** doubling laws **over**  $\mathbb{F}_p$  defined on  $U$
- ▶ Practice: consider two linear systems for  $x$  and  $y$  separately

## Finding the most efficient doubling law

- ▶ Let  $\{b_1, \dots, b_n\}$  be a basis of one kernel, with  $b_i \in \mathbb{F}_p^{|U|}$
- ▶ Consider the lattice  $L$  spanned by the columns of

$$[b_1, b_2, \dots, b_n, pI_{|U|}]$$

- ▶ Short vectors in  $L$  give **efficient parametrised** group laws over any field (including characteristic 0)
- ▶ Lattice reduction should use weights to express the fact that some monomials are cheaper to compute than others

## Example: x-coordinate of double

Family of curves:  $cx^2y^2 + x^2 + y^2 - 1$  with base face  
 $[\langle 0, 2 \rangle, \langle 0, 1 \rangle, \langle 0, 0 \rangle]$

$$\begin{aligned} & (-x^2y^2 - 1/cx^2 - 2/cxy - 1/cy^2 + 1/c)/(x^2y^2 - 1/c) \\ & \quad -2/cxy/(x^2y^2 - 1/c) \\ & \quad (-cx^2y^2 - x^2 + 2xy - y^2 + 1)/(x^2 + y^2) \\ & \quad \quad 2xy/(x^2 + y^2) \\ & \quad (x^2y^2 + 1/cx^2 + 2xy + 1/cy^2 - 1/c)/(x^2 + y^2) \\ & \quad \quad (2c - 2)/cxy/(x^2y^2 + x^2 + y^2 - 1/c) \\ & \quad \quad (-2c - 2)/cxy/(x^2y^2 - x^2 - y^2 - 1/c) \\ & (x^2y^2 + 1/cx^2 - 2/cxy + 1/cy^2 - 1/c)/(x^2y^2 - 1/c) \\ & \quad 2xy/(x^2y^2 + (c + 1)/cx^2 + (c + 1)/cy^2 - 1/c) \end{aligned}$$

## More applications ...

- ▶ Decide if certain formulae can exist or not
- ▶ x-only arithmetic: find most efficient doubling formulae with only x-coordinates used (à la Montgomery)
- ▶ Uniform group laws: same formula for adding and doubling
- ▶ Exists for any form of elliptic curve since adding is morphism
- ▶ Example: for short Weierstrass equation  $y^2 = x^3 + Ax + B$ , then x-coordinate of sum/double given by:

$$\frac{(x_1 x_2 - 2A)x_1 x_2 - 4B(x_1 + x_2) + A_2}{(x_1 x_2 + A)(x_1 + x_2) + 2y_1 y_2 + 2B}$$

# Questions?