Elliptic curves - Edwards curves

Robert Rolland

May 9, 2011

ACrypTA - eRISCS - IML
web: http://www.acrypta.fr/

This presentation uses the Beamer \LaTeXclass

eriscs
1 Courbes d’Edwards
- Définitions
- Singular points
- A bizarroidal correspondance
- The addition law
Courbes d’Edwards

Définitions

Singular points

A bizarroidal correspondance

The addition law
Recall that our base field is the prime finite field $\mathbb{F}_p$ where $p$ is a large prime (i.e. having a size in the order of 256, 384 or 512 bits). In the original work of Edwards, the studied curves are

$$x^2 + y^2 = c^2(1 + x^2y^2).$$

Bernstein and Lange showed that it is possible to obtain more curves by taking the following equations

$$x^2 + y^2 = c^2(1 + dx^2y^2),$$

and that in fact these curves are isomorphic to curves of the form

$$x^2 + y^2 = 1 + dx^2y^2. \quad (1)$$

From now on, curves in the form of Equation 1 will be named Edwards curves.
Courbes d’Edwards

- Définitions
- Singular points
- A bizarroidal correspondance
- The addition law
Study of Edwards curves

Let us recall the equation of the projective Edwards curve in projective coordinates

$$F(X, Y, T) = X^2 T^2 + Y^2 T^2 - T^4 - dX^2 Y^2 = 0. \quad (2)$$

Let us compute the partial derivatives in order to find the singular points

$$\frac{\partial F}{\partial X} = 2X(T^2 - dY^2)$$
$$\frac{\partial F}{\partial Y} = 2Y(T^2 - dX^2)$$
$$\frac{\partial F}{\partial T} = 2T(X^2 + Y^2 - 2T^2)$$

Hence there is two singular points, the two points at infinity

$$A_\infty = (1 : 0 : 0) \quad B_\infty = (0 : 1 : 0).$$
Singular points

We will denote by $\alpha$ a square root of $d$ in $\overline{K} = \overline{\mathbb{F}}_p$. Let us study the curve near $A_\infty$. Choose the affine plane $X = 1$. Its equation is

$$t^2 + y^2 t^2 - t^4 - dy^2 = 0.$$ 

The point $A_\infty$ is now an affine point of affine coordinates $(0, 0)$. Let us study the tangents to the curve at this point and to do that, let us set for $t \neq 0$

$$z = y/t \quad y = tz.$$ 

Using the equation of the curve we get for any point such that $t \neq 0$

$$z^2(t^2 - d) - (t^2 - 1) = 0.$$
This last relation gives for \( t = 0 \) two different values of \( z \) (in the algebraically closure of \( k \)) which are the slopes of the tangents to \( \mathcal{E}_d \) at the point \( A_\infty \). More precisely, the curve has the two distinct tangent slopes \( 1/\alpha \) and \( -1/\alpha \), at the point \( A_\infty \). In conclusion, the curve has two ordinary singular points \( A_\infty \) and \( B_\infty \), and then the genus can be computed by the formula

\[
g = \frac{(n-1)(n-2)}{2} - \sum_s \frac{r_s(r_s-1)}{2}
\]

\[
g = \frac{(4-1)(3-1)}{2} - \frac{2(2-1)}{2} - \frac{2(2-1)}{2} = 1.
\]

We conclude that the associated function field of the curve is an elliptic function field and consequently, the curve is birationally equivalent to a cubic given in Weierstrass form.
The affine trace $C'$ of the curve on the affine plane $X + Y = 1$ gives an affine model of the curve where the coordinates are $(X, T)$:

$$T^2 - 2X(1 - X)T^2 - T^4 - dX^2(1 - X)^2.$$

Now the points $A_\infty = (1, 0)$ and $B_\infty = (0, 0)$ are affine points. Then let us consider the curve $C''$ in $\mathbb{A}^3$ defined by the two equations

$$\begin{cases}
1 - 2ZT - T^2 - dZ^2 = 0 \\
X(1 - X) - TZ = 0
\end{cases}$$

The map $(X, T) \mapsto (X, T, X(1 - X)/T)$ is a birational map between the two affine curves with birational inverse $(X, T, Z) \mapsto (X, T)$. 
The curve $C''$ has no singular points. The singular point $A_{\infty} = (1, 0)$, (respectively $B_{\infty} = (0, 0)$) of the curve $C'$ is under the two points $(1, 0, 1/\alpha)$, $(1, 0, -1/\alpha)$ (respectively $(0, 0, 1/\alpha)$, $(0, 0, -1/\alpha)$). Hence if $d$ is not a square these four points are not rational points of the curve. In this case we can forgot the 2 singular points at infinity.
Plan

1 Courbes d’Edwards
   - Définitions
   - Singular points
   - A bizarroidal correspondance
   - The addition law
From now on we suppose that $d$ is not a square in $\mathbb{F}_p$. Let us consider two particular points of the affine Edwards curve:

$$O = (0, 1) \text{ and } Q = (0, -1)$$

that are the only points such that $x = 0$ or $y = 1$. Let $\phi$ the following map:

$$\phi : \mathcal{E}_d \setminus \{O, Q\} \to \mathbb{A}^2$$

$$(x, y) \mapsto \begin{cases} u &= (1 - d)\frac{1+y}{1-y} \\ v &= 2(1 - d)\frac{1+y}{(1-y)x} \end{cases}$$
Theorem

The map $\phi$ is a bijection from $E_d \setminus \{O, Q\}$ onto the affine points of the Weierstrass curve $W_{2(1+d),(1-d)^2}$:

$$v^2 = u^3 + 2(1 + d)u^2 + (1 - d)^2u,$$

(3)

minus the points $Z_1 = (0, 0)$ and the reciprocal map is given by

$$\phi^{-1} : W_{2(1+d),(1-d)^2} \setminus \{Z_1\} \rightarrow E_d \setminus \{O, Q\}$$

$$(u, v) \mapsto \left\{ \begin{array}{l}
x = 2\frac{u}{v} \\
y = 2\frac{u^2-1+d}{u+1-d} \
\end{array} \right.$$

(It is not true if $d$ is a square, in this case we must consider other special points). Then if we extend $\phi$ by setting $\phi(O) = P_\infty$ and $\phi(Q) = (0, 0)$ we obtain a bijection between the set of rational points of the affine Edwards curve onto the set of rational points of the complete (projective) Weierstrass curve. Very bizarroidal!!
Plan

1 Courbes d’Edwards
   • Définitions
   • Singular points
   • A bizarroidal correspondance
   • The addition law
We transport the addition on the Projective Weierstrass curve to the Edwards curve by the bijection. The obtained operation is given by only one formula (complete unified operation - when $d$ is not a square)

**Theorem**

This group structure on $\mathcal{E}_d(k)$ is given by the addition

$$(x_3, y_3) = \left( \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

the point $(0, 1)$ is the neutral point. The point $(0, -1)$ has order 2 the points $(1, 0), (-1, 0)$ have order 4.

Now we can conclude that

**Theorem**

If a Weierstrass curve over $k$ is birationally equivalent over $k$ to an Edwards curve, its associated group has a subgroup of order 4.
Requirements

- $p$ a large prime (256, 384 or 512 bits);
- $p \equiv 3 \pmod{4}$;
- equation $x^2 + y^2 = 1 + dx^2y^2$ (Edwards curve);
- $d \neq 0$ and $d \neq 1$ so that the curve is irreducible of genus one;
- $d$ is not a square in $\mathbb{F}_p$; and
- the number $n$ of $\mathbb{F}_p$-rational points is four times a prime.

The second last condition is required to obtain a complete set of addition laws on the curve, namely an addition formula with no exceptional points. In this case, the equations for addition take the particularly elegant form

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3),$$

where

$$x_3 = \frac{(x_1y_2 + x_2y_1)}{(1 + dx_1x_2y_1y_2)} \quad \text{and} \quad y_3 = \frac{(y_1y_2 - x_1x_2)}{(1 - dx_1x_2y_1y_2)}.$$
Similar to the case of Weierstrass curves, we wrote two PARI scripts to generate the database of Edwards curves. The first generates Edwards curves defined over a prime finite field $p$ whose coefficient $d$ is not a square in $\mathbb{F}_p$ and whose group of $\mathbb{F}_p$-rational points has order four times a prime. To prove that the curve is not specially chosen, we do not select $d$ directly, but rather generate a number $r_d$ which is hashed to give $d$. To compute the number of rational points we use the SEA algorithm after transforming the Edwards curve into Weierstrass form (not the short Weierstrass form).
We apply SEA to this last curve and we test if the number of rational points is of the right form. Unfortunately, the standard early-abort procedure cannot be used here because the order of group of rational points of an Edwards curve is a multiple of 4. On the other hand, for efficiency reasons we cannot deactivate the early-abort capability. To circumvent this problem we applied a patch to the PARI implementation of SEA in order to disable the early-abort when a factor of 2 is found. As in the case Weierstrass curves, when a candidate curve is found we test if the curve is of a type known to be insecure. We also compute a point on the curve which is not of order 1, 2 or 4. To do that we draw a random number \( r \), compute the hash \( g_x \) of \( r \), and test if \( z = (1 - g_x^2)/(1 - dg_x^2) \) is a square. If \( z \) is square, we compute \( g_y \) to be a square root of \( z \), otherwise we repeat the process with a new \( r \).
The second script verifies whether a curve is correctly generated and computes the exact order of the chosen point on the curve. We know that the point \((0, 1)\) is always the neutral element on an Edwards curve. The opposite of \((x, y)\) is \((-x, y)\). There is an element of order two: \((0, -1)\) and two elements of order four: \((1, 0), (-1, 0)\). So it is very easy to detect elements of order 1, 2 and 4. If we exclude these four elements, the other elements are of order \(n = 4u, n/2 = 2u\) or \(n/4 = u\) where \(u\) is prime. For each accepted curve, we choose a point \((g_x, g_y)\) of order \(u, 2u\) or \(4u\). We fill in a field \(t\) in the descriptor file of the curve such that \(t = 0\) if the order is \(n\), \(t = 1\) if the order is \(n/2\), and \(t = 2\) if the order is \(n/4\). In fact, knowing an element \((g_x, g_y)\) on the curve and its \(t\)-value, we can deduce elements of any order. More precisely, if \(g\) has order \(n\), then \(2g\) has order \(n/2\) and \(4g\) has order \(n/4\); if \(g\) has order \(n/2\), \(2g\) has order \(n/4\) and \(g + (0, -1)\) has order \(n\); and if \(g\) has order \(n/4\), \(g + (0, -1)\) has order \(n/2\) and \(g + (1, 0)\) has order \(n\).