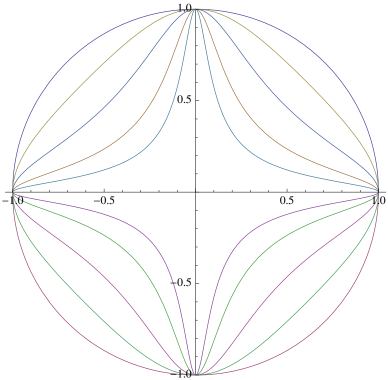
Edwards Curves

Çetin Kaya Koç

koc@cs.ucsb.edu



Edwards Curves

- Harold Edwards introduced a new normal form for elliptic curves and gave an addition law which is remarkably symmetric and much simpler
- The original form the equation Edwards studied was

$$x^2 + y^2 = c^2 + c^2x^2y^2$$

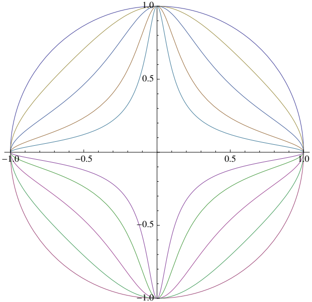
  solved over a field $\mathcal{F}$ whose characteristic is not equal to 2
- Studies on such groups go as far back as to Gauss
- Bernstein and Lange gave a slightly simpler form

$$x^2 + y^2 = 1 + dx^2y^2$$

  where d is not a square in $\mathcal{F}$

Edwards Curves

- For values of $d \in \mathcal{F} - \{0, 1\}$ in a non-binary field $\mathcal{F}$, Edward curves are within the unit circle
- Edwards curves for $d = 0, -2, -10, -50, -200$ over $\mathcal{R}$



Edwards Curves for $d = 0$

- When $d = 0$, the equation defines the unit circle: $x^2 + y^2 = 1$
- Let $x_i = \sin(\alpha_i)$ and $y_i = \cos(\alpha_i)$
- The angle α_i is measured with the respect to the y axis
- The addition of (x_1, y_1) and (x_2, y_2) is "addition on a clock"

$$
\begin{aligned}
x_3 &= \sin(\alpha_1 + \alpha_2) \\
&= \sin(\alpha_1)\cos(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2) \\
&= x_1 y_2 + y_1 x_2
\end{aligned}
$$

$$
\begin{aligned}
y_3 &= \cos(\alpha_1 + \alpha_2) \\
&= \cos(\alpha_1)\cos(\alpha_2) - \sin(\alpha_1)\sin(\alpha_2) \\
&= y_1 y_2 - x_1 x_2
\end{aligned}
$$

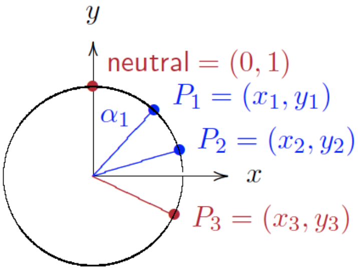
Edwards Curves for $d = 0$

- Addition of angles defines the commutative group law
- The zero (neutral) element of the group is $(0, 1)$

$$P_3 = P_1 \oplus P_2$$

$$(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$$

$$(x_1 y_2 + x_2 y_1 \ , \ y_1 y_2 - x_1 x_2)$$



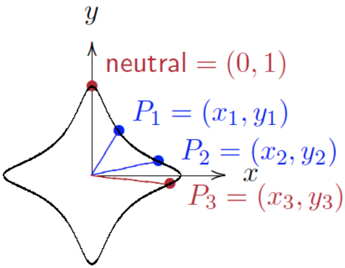
Edwards Curves for $d \neq 0, 1$

- $x^2 + y^2 = 1 + dx^2y^2$ for $d \in \mathcal{F} - \{0, 1\}$
- The zero (neutral) element is $(0, 1)$
- The inverse of (x, y) is $(-x, y)$

$$P_3 = P_1 \oplus P_2$$

$$(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$$

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



Edwards Curve Arithmetic Properties

- The zero element $(0, 1)$ is of order 1
- The point $(0, -1)$ has order 2, since

$$(0, -1) \oplus (0, -1) \quad = \quad (0, 1)$$

- The points $(1, 0)$ and $(-1, 0)$ have orders 4, since

$$\begin{aligned} (1, 0) \oplus (1, 0) &= (0, -1) \\ (-1, 0) \oplus (-1, 0) &= (0, -1) \end{aligned}$$

- The negative of $P = (x, y)$ is $-P = (-x, y)$
- The addition law applies to doubling as well

Edwards Curve Arithmetic Properties

- d needs to be a non-square in the field $\mathcal{F}$
- For $\mathcal{F} = \mathrm{GF}(p)$, d needs to be quadratic non-residue
- Question: Since

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2} \, , \, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

can denominators be 0 in $\mathcal{F}$?

Theorem

The denominators is never 0 if d is non-square in $\mathcal{F}$.

Edwards Curve Arithmetic Properties

- Let (x_1, y_1) and (x_2, y_2) be on the curve
- That is: $x_i^2 + y_i^2 = 1 + dx_i^2 y_i^2$ for $i = 1, 2$
- Write $e = dx_1 x_2 y_1 y_2$
- We will use proof by contradiction
- Assume $e = -1, 1 \in \mathcal{F}$
- This implies $x_1, x_2, y_1, y_2 \neq 0$ and $e^2 = 1$

Edwards Curve Arithmetic Properties

- Now calculate $dx_1^2y_1^2(x_2^2+y_2^2)$

$$
\begin{aligned}
dx_1^2y_1^2(x_2^2+y_2^2) &= dx_1^2y_1^2(1+dx_2^2y_2^2) \\
&= dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\
&= dx_1^2y_1^2 + e^2 \\
&= 1 + dx_1^2y_1^2
\end{aligned}
$$

- We have obtained $dx_1^2y_1^2(x_2^2+y_2^2) = 1 + dx_1^2y_1^2 = x_1^2 + y_1^2$

Edwards Curve Arithmetic Properties

- We now calculate $(x_1 + ey_1)^2$

$$
\begin{aligned}
(x_1 + ey_1)^2 &= x_1^2 + y_1^2 + 2e\, x_1 y_1 \\
&= d\, x_1^2 y_1^2 (x_2^2 + y_2^2) + 2 x_1 x_2 y_1 y_2 x_1 y_1 \\
&= d\, x_1^2 y_1^2 (x_2^2 + 2 x_2 y_2 + y_2^2) \\
&= d\, x_1^2 y_1^2 (x_2 + y_2)^2
\end{aligned}
$$

- This gives an expression for d as

$$
d = \frac{(x_1 + ey_1)^2}{x_1^2 y_1^2 (x_2 + y_2)^2} = \left(\frac{x_1 + ey_1}{x_1 y_1 (x_2 + y_2)} \right)^2
$$

- This implies that d is a square, if $x_2 + y_2 \neq 0$

Edwards Curve Arithmetic Properties

- Similarly, we calculate $(x_1 - ey_1)^2$

$$\begin{aligned}(x_1 - ey_1)^2 &= x_1^2 + y_1^2 - 2e\,x_1 y_1 \\ &= d\,x_1^2 y_1^2 (x_2^2 + y_2^2) - 2x_1 x_2 y_1 y_2 x_1 y_1 \\ &= d\,x_1^2 y_1^2 (x_2^2 - 2x_2 y_2 + y_2^2) \\ &= d\,x_1^2 y_1^2 (x_2 - y_2)^2\end{aligned}$$

- This gives an expression for d as

$$d = \frac{(x_1 - ey_1)^2}{x_1^2 y_1^2 (x_2 - y_2)^2} = \left(\frac{x_1 - ey_1}{x_1 y_1 (x_2 - y_2)}\right)^2$$

- This implies that d is a square, if $x_2 - y_2 \neq 0$

Edwards Curve Arithmetic Properties

- Considering these two expressions together:

$$x_2 + y_2 \neq 0 \implies \left(\frac{x_1 + ey_1}{x_1 y_1 (x_2 + y_2)}\right)^2 \implies d \text{ is square}$$

$$x_2 - y_2 \neq 0 \implies \left(\frac{x_1 - ey_1}{x_1 y_1 (x_2 - y_2)}\right)^2 \implies d \text{ is square}$$

- However, $x_2 + y_2 = 0$ and $x_2 - y_2 = 0$ imply $x_2 = y_2 = 0$
- Therefore, we reach a contradiction: x_2 and y_2 were nonzero
- This implies that e cannot be -1 or 1
- Therefore the denominators cannot be zero

An Example Edwards Curve

- Let us denote the $x^2 + y^2 = 1 + dx^2y^2$ over GF(p) using $\mathcal{E}(d, p)$
- Consider the curve $\mathcal{E}(5, 23)$
- We can check if 5 is not a square in GF(23)
- Euler's test: a is not square if $a^{(p-1)/2} = -1 \pmod{p}$
- $5^{(23-1)/2} = 5^{11} = 22 = -1 \pmod{23}$, thus, 5 is not square
- We now generate all elements of $\mathcal{E}(5, 23)$ and find its order

Edwards Curve: $x^2 + y^2 = 1 + 5x^2y^2$ in GF(23)

- We know that $(0,1) \in \mathcal{E}(5,23)$
- It is the neutral element of the group and its order is 1
- These elements also belong to $\mathcal{E}(5,23)$: $(0,-1)$, $(1,0)$, and $(-1,0)$ since they satisfy the curve equation
- Since $(0,-1) \oplus (0,-1) = (0,1)$, its order is 2
- Since $(1,0) \oplus (1,0) = (0,-1)$, its order is 4
- Since $(-1,0) \oplus (-1,0) = (0,-1)$, its order is 4

Edwards Curve: $x^2 + y^2 = 1 + 5x^2y^2$ in GF(23)

- To find other elements of the group $\mathcal{E}(5, 23)$, we give values to $x \in \text{GF}(23)$, and solve for y in

$$x^2 + y^2 = 1 + 5x^2y^2$$

  in GF(23)

- For $x = 0$, we already know solutions $(0, 1)$ and $(0, 1)$ since $y^2 = 1 \pmod{23}$ implies $y = \pm 1$
- For $x = \pm 1$, we obtain $1 + y^2 = 1 + 5y^2$ which implies $y^2 = 0$, and thus $y = 0$, giving two solutions $(\pm 1, 0)$

Edwards Curve: $x^2 + y^2 = 1 + 5x^2y^2$ in GF(23)

- For $x = 2$, we obtain $4 + y^2 = 1 + 5 \cdot 4 \cdot y^2 \pmod{23}$, which gives $19y^2 = 3 \pmod{23}$
- We compute $19^{-1} \pmod{23}$ as 17, and write

$$y^2 = 3 \cdot 17 = 51 = 5 \pmod{23}$$

- For a solution for y to exist, the righthand side needs to be a quadratic residue
- Applying Euler's test $5^{(23-1)/2} = -1 \pmod{23}$, we discover that the the righthand side is not a square and there is no y for $x = 2$

Edwards Curve: $x^2 + y^2 = 1 + 5x^2y^2$ in GF(23)

- For a given x, we can write

$$
\begin{aligned}
x^2 + y^2 &= 1 + 5x^2y^2 \pmod{23} \\
x^2 - 1 &= (5x^2 - 1)y^2 \pmod{23} \\
y^2 &= (x^2 - 1)(5x^2 - 1)^{-1} \pmod{23}
\end{aligned}
$$

- For a solution for y to exist, the righthand side

$$R(x) = (x^2 - 1)(5x^2 - 1)^{-1} \pmod{23}$$

  needs to be a quadratic residue
- Euler's test: if $R(x)^{(23-1)/2} = 1 \pmod{23}$, then $R(x)$ is square
- If y exists, $y = R(x)^{(23+1)/4} \pmod{23}$, since $23 = 3 \pmod{4}$

Edwards Curve: $x^2 + y^2 = 1 + 5x^2y^2$ in GF(23)

- Every $\pm x$ maps to the same y
- For every x there are two $\pm y$ values
- If $(x, y) \in \mathcal{E}(d, p)$, so is $(y, x) \in \mathcal{E}(d, p)$
- Therefore, if $(x, y) \in \mathcal{E}(d, p)$, then all of these points are too:
  $(x, y), (x, -y), (-x, y), (-x, -y)$
  $(y, x), (y, -x), (-y, x), (-y, -x)$

Edwards Curve: $x^2 + y^2 = 1 + 5x^2y^2$ in GF(23)

- We only need to test positive x values, $x \in [2, 11]$
- For mod p this implies testing for $x \in [2, (p-1)/2]$

x	$R(x)$	$R(x)^{11}$	$y = R(x)^6$ if $R(x)^{11} = 1$
2	5	-1	
3	19	-1	
4	13	1	± 6
5	18	1	± 8
6	16	1	± 4
7	10	-1	
8	2	1	± 5
9	15	-1	
10	22	-1	
11	20	-1	

Edwards Curve: $x^2 + y^2 = 1 + 5x^2y^2$ in GF(23)

- Therefore, we find all elements $\mathcal{E}(5, 23)$

$$
\begin{array}{llll}
(0,1) & (0,-1) & & \\
(1,0) & (-1,0) & & \\
(4,6) & (4,-6) & (-4,6) & (-4,-6) \\
(6,4) & (6,-4) & (-6,4) & (-6,-4) \\
(5,8) & (5,-8) & (-5,8) & (-5,-8) \\
(8,5) & (8,-5) & (-8,5) & (-8,-5)
\end{array}
$$

- Since there are 20 elements, $\text{order}(\mathcal{E}(5, 23)) = 20$
- Hasse theorem applies

$$23 - 2\sqrt{23} \leq \text{order}(\mathcal{E}(5, 23)) \leq 23 + 2\sqrt{23}$$

- Furthermore, the factors 20 are 1, 2, 4, 5, 10, 20
- Therefore, element orders can only be one of these integers

Edwards Curve: $x^2 + y^2 = 1 + 5x^2y^2$ in GF(23)

- Group order: 20
- Order 1 element: $(0, 1)$
- Order 2 element: $(0, -1)$
- Order 4 elements: $(1, 0)$, $(-1, 0)$
- Order 5 elements: $(4, 6)$, $(-4, 6)$ and $(8, -5)$, $(-8, -5)$
- Order 10 elements: $(4, -6)$, $(-4, -6)$ and $(8, 5)$, $(-8, 5)$
- Order 20 elements:
  $(6, 4)$, $(6, -4)$, $(-6, 4)$, $(-6, -4)$
  $(5, 8)$, $(5, -8)$, $(-5, 8)$, $(-5, -8)$
- The set of order 20 elements are all primitive

A Complexity Result

- We know that $\mathcal{E}(d, p)$ has identity $(0, 1)$
- The element $(0, -1)$ is of order 2
- What are the orders of the other elements?

- Suppose p, q are prime numbers with $p = 4q - 1$.
- A few such (p, q) pairs are $(11, 3)$, $(19, 5)$, $(331, 83)$, $(1314883, 328721)$, $(2760727332067, 690181833017)$
- Consider the Edwards group $\mathcal{E}(d, p)$ with $d = -1$, which is a non square in $\mathrm{GF}(p)$

Theorem

Given primes p and q with $p = 4q - 1$, the elements $(x, y) \in \mathcal{E}(-1, p)$ are of order q, $2q$ or $4q$, except $(0, 1)$ and $(0, -1)$ whose orders are 1 and 2.