Division Polynomials for Twisted Edwards Curves

Richard Moloney
(Joint work with Gary McGuire)

Claude Shannon Institute,
School of Mathematics,
University College Dublin

July 16, 2009
9th International Conference on Finite Fields and their Applications

Outline

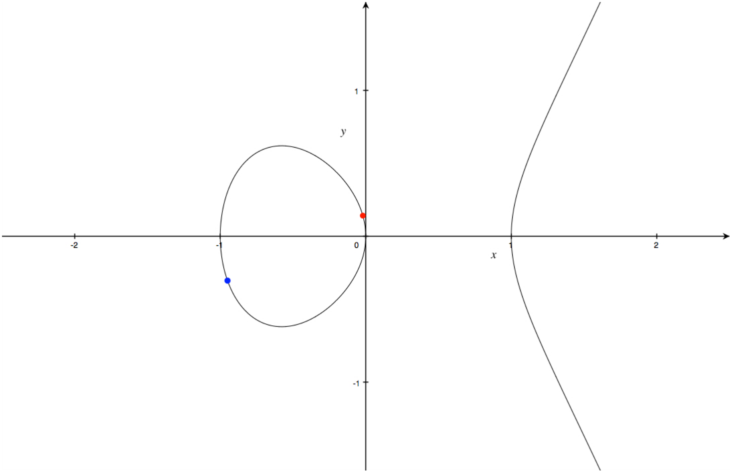
Elliptic Curves

- Let k be a field of characteristic $\neq 2$ or 3.
- An elliptic curve defined over k is a set

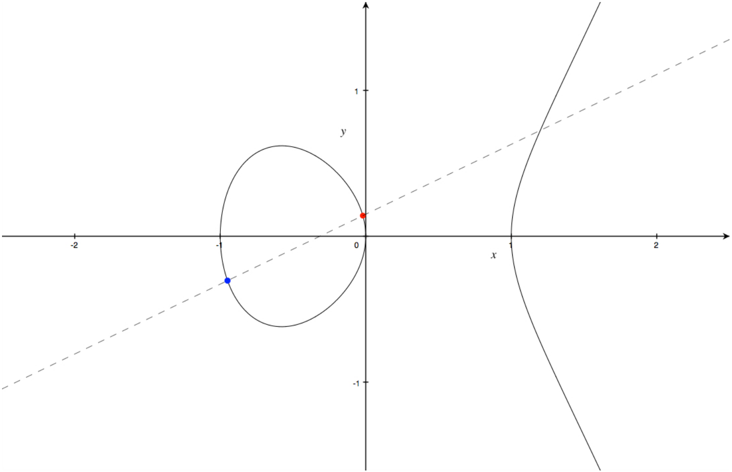
$$E(k) = \{(x, y) \in k^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

  for some $a, b \in k,\ 4a^3 + 27b^2 \neq 0.$
- The equation $y^2 = x^3 + ax + b$ is called the Weierstrass form of the elliptic curve.
- $\mathcal{O}$, not being an affine point, is often called "the **point at infinity**" of E.
- For $k = \mathbb{R}$, a geometric addition operation is defined on an elliptic curve.

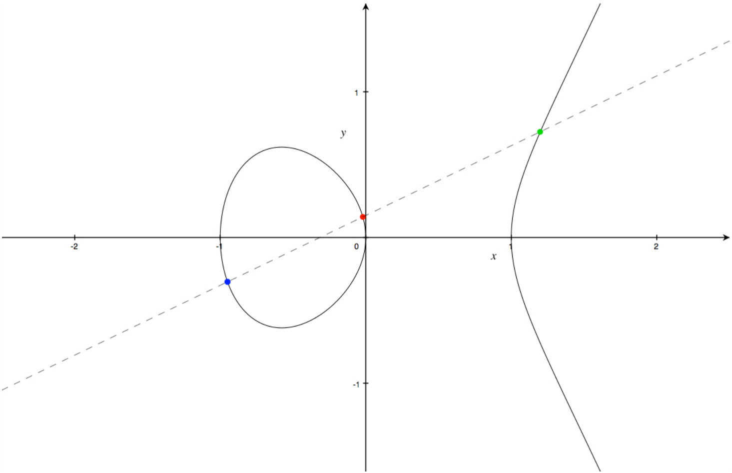
Addition operation



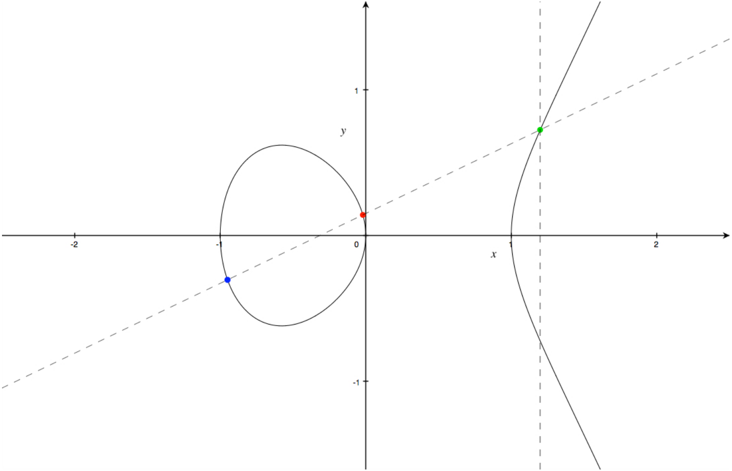
Addition operation



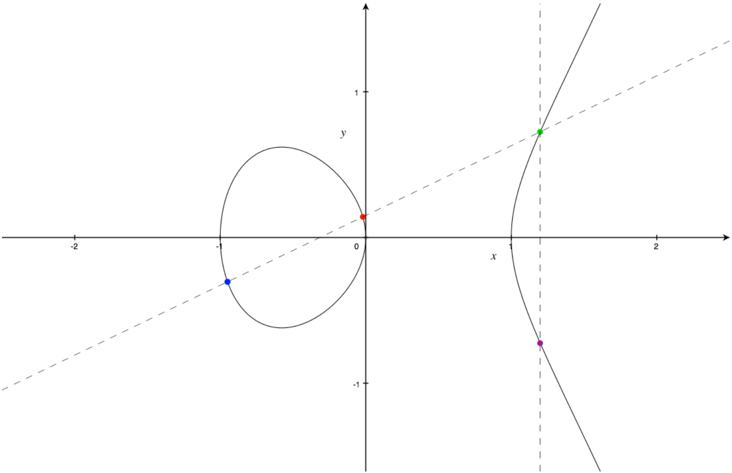
Addition operation



Addition operation



Addition operation



Point addition in $E(k)$

- We can formalize and adapt this addition operation to a general field k. Let E be the elliptic curve over k with Weierstrass form $y^2 = x^3 + ax + b$.
- $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E(k)$.
- Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E(k) \backslash \{\mathcal{O}\}$. Then
- If $x_1 = x_2$ & $y_1 = -y_2$, then $P_2 = -P_1$ and $P_1 + P_2 = \mathcal{O}$.

Point addition in $E(k)$ (cont'd)

If $P_2 \neq -P_1$:

- If $P_1 = P_2$ set $\lambda = \frac{3x_1^2 + a}{2y_1}$.
- Otherwise set $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.
- $x_3 := \lambda^2 - x_1 - x_2$,
- $y_3 := \lambda(x_1 - x_3) - y_1$,
- Then $P_1 + P_2 = (x_3, y_3)$.

- $(E(k), +)$ is an abelian group.

Cryptography

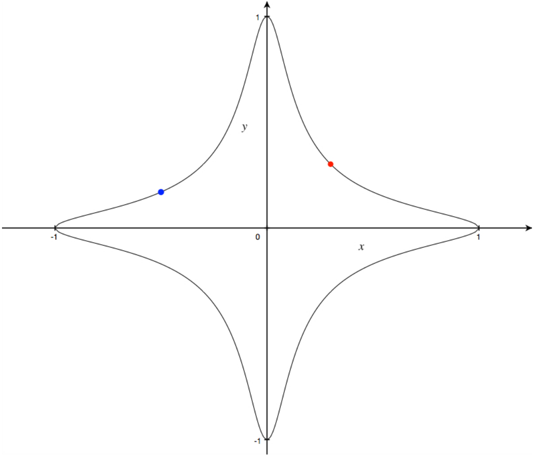
- Cryptography on elliptic curves relies on the discrete logarithm problem. A private key is some integer n, and the corresponding public key is nP for some given point $P \in E(k)$.
- k, E and P are known parameters of the system; security depends on the difficulty of discovering n given nP.
- k here is generally a field of order p, a prime of size at least 2^{128}.
- The efficiency of encryption depends on the speed with which one can compute multiples of points.
- One approach has been to turn to different models for elliptic curves, such as Montgomery curves, Jacobi quartics, and most recently, Edwards curves.

Edwards Curves

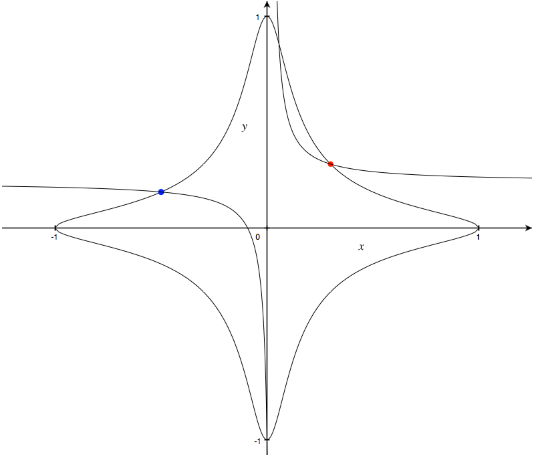
- An **Edwards curve** over k is an affine plane curve defined by the equation $x^2 + y^2 = 1 + dx^2y^2$, where $d \in k \setminus \{0, 1\}$.
- Every Edwards curve is birationally equivalent to an elliptic curve (Edwards, 2007).
- Thus an addition law is defined on Edwards curves:
- $(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right)$

Actually, this isn't quite the form of curve used by Edwards in his paper, rather the adapted form used by Bernstein et al. We use this form as it covers a larger class of curves over finite fields.

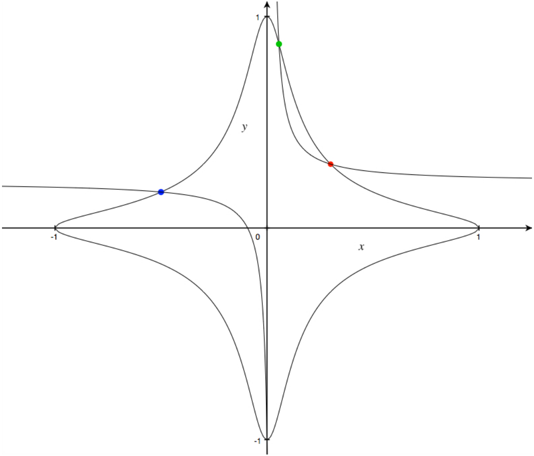
Addition on Edwards curves (graphically)



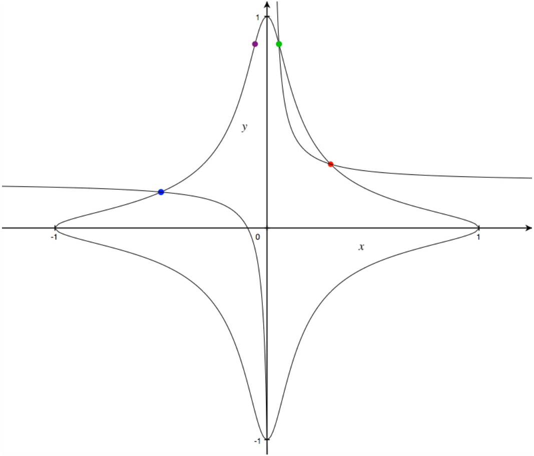
Addition on Edwards curves (graphically)



Addition on Edwards curves (graphically)



Addition on Edwards curves (graphically)



Twisted Edwards Curves

- Bernstein et al. (2007) introduced a generalisation of Edwards curves, the **twisted Edwards curves**.
- A twisted Edwards curve over k is an affine plane curve defined by the equation $ax^2 + y^2 = 1 + dx^2y^2$, where $a, d \in k \setminus \{0\}$, $a \neq d$. ($a = 1$ gives an Edwards curve.)
- The addition operation is similar to that for Edwards curves:
- $(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$

Division Polynomials: Elliptic Curves

Given the addition operation on an elliptic curve $E(k)$, two important, related questions are, for any integer n, and any point $P = (x, y)$ on the curve:

- Is $nP = \mathcal{O}$?
- What are the coordinates of nP in terms of x and y?

Both of these are addressed by **division polynomials**.

Definition

Division polynomials for elliptic curves

The division polynomials are elements of the function field of $E(k)$, which is the quotient field of the ring $k[x,y]/(y^2 - x^3 - ax - b)$.

- $\Psi_1(x,y) = 1$
- $\Psi_2(x,y) = 2y$
- $\Psi_3(x,y) = 3x^4 + 6ax^2 + 12bx - a^2$
- $\Psi_4(x,y) = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2)$
- $\Psi_{2m+1}(x,y) = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3$
- $\Psi_{2m}(x,y) = \frac{\Psi_m}{2y}\left(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2\right)$

Point Multiplication using Division Polynomials

The above defined polynomials give an explicit computation of a multiple of a point:

$$nP = \left(\frac{x\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{2n}}{2\Psi_n^4} \right)$$

Consequently, $nP = \mathcal{O}$ if & only if $\Psi_n(x, y) = 0$.

Division Polynomials: Twisted Edwards Curves

Can we do the same for Edwards, or more generally, twisted Edwards curves?

- By applying the explicit mapping between a given twisted Edwards curve and an elliptic curve to the division polynomials, we should be able to derive twisted Edwards division polynomials.

Transformation applied to division polynomials

- $\psi_1(x,y) = 1$
- $\psi_2(x,y) = \frac{(a-d)(1+y)}{x(2(1-y))}$
- $\psi_3(x,y) = \frac{(a-d)^3(a+2ay-2dy^3-dy^4)}{(2(1-y))^4}$
- $\psi_4(x,y) = \frac{2(a-d)^6 y(1+y)(a-dy^4)}{x((2(1-y))^7}$

- $\psi_{2m+1}(x,y) = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$
- $\psi_{2m}(x,y) = \frac{\psi_m}{\psi_2}\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right)$

Point multiplication formula

If we further define

$$\phi_n(x,y) := \frac{(1+y)\psi_n^2}{(1-y)} - \frac{4\psi_{n-1}\psi_{n+1}}{(a-d)}$$

and

$$\omega_n(x,y) := \frac{2\psi_{2n}}{(a-d)\psi_n},$$

then

$$n(x,y) = \left(\frac{\phi_n\psi_n}{\omega_n}, \frac{\phi_n - \psi_n^2}{\phi_n + \psi_n^2}\right).$$

- Given that the identity of the Edwards addition law is $(0,1)$, it is easy to see that $n(x,y) = (0,1)$ if & only if $\psi_n = 0$.

Division polynomials for Edwards curves

- It looks like the denominator is behaving in a uniform way, and that we can pull a sequence of "division polynomials" (in y alone) out of the numerators.
- If we do that, we get the following recursion:

Division polynomials for Edwards curves

$$
\begin{aligned}
\tilde{\psi}_0(y) &= 0 \\
\tilde{\psi}_1(y) &= 1 \\
\tilde{\psi}_2(y) &= y + 1 \\
\tilde{\psi}_3(y) &= -dy^4 - 2dy^3 + 2ay + a \\
\tilde{\psi}_4(y) &= -2y(y+1)(dy^4 - a)
\end{aligned}
$$

and

$$
\tilde{\psi}_{2r+1}(y) = \begin{cases}
\frac{4(a-d)(a-dy^2)^2\tilde{\psi}_{r+2}\tilde{\psi}_r^3}{(y+1)^2} - \tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3 & r \equiv 0 \ (4) \\
\tilde{\psi}_{r+2}\tilde{\psi}_r^3 - \frac{4(a-dy^2)^2\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3}{(y+1)^2} & r \equiv 1 \ (4) \\
\frac{4(a-dy^2)^2\tilde{\psi}_{r+2}\tilde{\psi}_r^{\ 3}}{(y+1)^2} - \tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3 & r \equiv 2 \ (4) \\
\tilde{\psi}_{r+2}\tilde{\psi}_r^3 - \frac{4(a-d)(a-dy^2)^2\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3}{(y+1)^2} & r \equiv 3 \ (4)
\end{cases}
$$

Division polynomials for Edwards curves

$$\tilde{\psi}_{2r}(y) = \begin{cases} \frac{\tilde{\psi}_r}{y+1}\left(\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2 - \tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2\right) & r \equiv 0\ (4) \\ \frac{\tilde{\psi}_r}{y+1}\left((a-d)\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2 - \tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2\right) & r \equiv 1\ (4) \\ \frac{\tilde{\psi}_r}{y+1}\left(\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2 - \tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2\right) & r \equiv 2\ (4) \\ \frac{\tilde{\psi}_r}{y+1}\left(\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2 - (a-d)\tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2\right) & r \equiv 3\ (4) \end{cases}$$

Properties of Edwards division polynomials

Fortunately, the $\tilde{\psi}_n$ have some nice properties.

- Each $\tilde{\psi}_n$ is a polynomial in y, with coefficients in $\mathbb{Z}[a, d]$.
- $\deg \tilde{\psi}_n(y) < \frac{n^2}{2}$.
- By substituting $-d$ for a, and $-a$ for d, $\tilde{\psi}_n(y)$ is mapped to its own reciprocal polynomial.

$$\begin{aligned}
\tilde{\psi}_3(y) &= -dy^4 - 2dy^3 + 2ay + a \\
\tilde{\psi}_3^*(y) &= -(-a)y^4 - 2(-a)y^3 + 2(-d)y + (-d) \\
&= ay^4 + 2ay^3 - 2dy - d
\end{aligned}$$

History of the lemniscate: The Bernoullis

- Edwards curves start with the **lemniscate of Bernoulli**, a curve with polar coordinate equation $r^2 = \cos 2\theta$.

- The lemniscate was first described by Jacob (and independently by Johann) Bernoulli in 1694 as the rectification of the elastic curve.
- The arc length of the lemniscate (in the first quadrant) is given by

$$s = \int_0^r \frac{dt}{\sqrt{1-t^4}} \; ,$$

an elliptic integral.

Fagnano, Euler

- The count G.C. di Fagnano was the next to study the curve, giving a formula for doubling the arc of the lemniscate.
- In 1751, Euler generalised Fagnano's work, giving a full addition formula for lemniscatic integrals:

$$\int_0^u \frac{dt}{\sqrt{1-t^4}} + \int_0^v \frac{dt}{\sqrt{1-t^4}} = \int_0^r \frac{dt}{\sqrt{1-t^4}}$$

where

$$r = \frac{u\sqrt{1-v^4} + v\sqrt{1-u^4}}{1+u^2v^2}$$

- Jacobi called this "the birth of elliptic functions"; the key insight was shifting the focus from the integral *per se* to the inverse function.

Gauss

- Though Gauss never published anything on the subject, there is copious work in his notebooks on the lemniscatic integral.
- Gauss called the inverse function of the lemniscatic integral the **lemniscatic sine** function.
- He also defined a lemniscatic cosine in a natural way, and derived the identity between them

$$s^2 + c^2 = 1 - s^2c^2 \ .$$

- Gauss then reformulated Euler's addition law as

$$s' = \frac{s_1c_2 + s_2c_1}{1 - s_1s_2c_1c_2}\,, \ c' = \frac{c_1c_2 - s_1s_2}{1 + s_1s_2c_1c_2} \ .$$

Comparison

These were the properties which Edwards was generalising in defining the curves.

Edwards curve	Lemniscatic functions
$x^2 + y^2 = 1 + dx^2y^2$	$s^2 + c^2 = 1 - s^2c^2$
$\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}$	$\frac{s_1c_2+s_2c_1}{1-s_1s_2c_1c_2}$
$\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}$	$\frac{c_1c_2-s_1s_2}{1+s_1s_2c_1c_2}$

Gauss, Abel

Gauss computed the results of various iterations of this formula: (From Gauss's posthumously published notebooks)

$$
\begin{aligned}
\sin\operatorname{lemn}\varphi &= s \\
\sin\operatorname{lemn}2\varphi &= sc(1+ss)\frac{2}{1+s^4} = sc(1+cc)\frac{2}{1+c^4} \\
\sin\operatorname{lemn}3\varphi &= s\,\frac{3-6s^4-s^8}{1+6s^4-3s^8} \\
\sin\operatorname{lemn}4\varphi &= 4sc(1+ss)\frac{1-5s^4-5s^8+s^{12}}{1+20s^4-26s^8+20s^{12}+s^{16}} \\
\sin\operatorname{lemn}5\varphi &= s\,.\,\frac{5-2s^4+s^8}{1-2s^4+5s^8}\,.\,\frac{1-12s^4-26s^8+52s^{12}+s^{16}}{1+52s^4-26s^8+12s^{12}+s^{16}} \\
\sin\operatorname{lemn}n\varphi &= s\,.\,\frac{n-\frac{n\,.\,nn-1\,.\,nn+6}{60}s^4-\frac{n^6-13n^4+36nn+420\,.\,n\,.\,nn+1}{10080}s^8\ldots}{1+\frac{n\,.\,n\,.\,nn-1}{12}s^4-\frac{nn\,.\,nn-1\,.\,nn-4\,.\,nn+75}{10080}s^8\ldots}
\end{aligned}
$$

Abel studied these rational functions in more detail, using them to prove that the arc of the lemniscate can be divided into n equal parts using straightedge and compass if $n = 2^a p_1 p_2 \cdots p_t$, where the p_i are distinct Fermat primes.

Applying lemniscatic theory to Edwards curves

As we've implied, (twisted) Edwards curves are generalisations of lemniscatic functions. By analogy with the theory of lemniscatic functions, we derive new results for twisted Edwards curves.

- Let $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$. Then we can rephrase the addition law as:

$$x_3 = \frac{x_1 y_2 (1 - d x_2^2) + x_2 y_1 (1 - d x_1^2)}{1 - a d x_1^2 x_2^2}$$

$$y_3 = \frac{(a-d) y_1 y_2 - (a - d y_1^2)(a - d y_2^2) x_1 x_2}{a - d(y_1^2 + y_2^2) + d y_1^2 y_2^2}$$

An incremental point multiplication formula

- If we let $(x_n, y_n) = n(x, y)$ for all n, we use the above formula to show that

$$x_{n+1} + x_{n-1} = \frac{2x_n y(1 - dx^2)}{1 - adx_n^2 x^2}$$

The benefit of this is that it allows us to perform point multiplication with the x-coordinate only.

Point multiplication

- We apply this formula to get a recursion for the multiple of a point:

$$x_n = \begin{cases} \dfrac{xyP_n(x^2)}{Q_n(x^2)} & \text{if } n \text{ is even} \\ \\ \dfrac{xP_n(x^2)}{Q_n(x^2)} & \text{if } n \text{ is odd} \end{cases}$$

- The polynomials P_{n+1}, Q_{n+1} are generated by a recursion on $P_n,\ Q_n,\ P_{n-1},\ Q_{n-1}$.
- Unlike our original division polynomials, which required the previous $\frac{n}{2}$ to generate each new polynomial, this system only needs the previous 2 rounds.