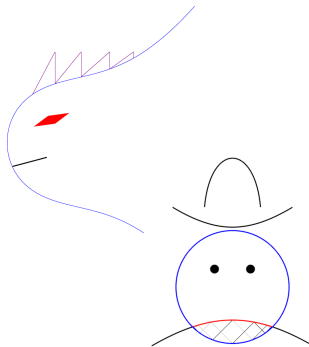


Compact algebraic representations of isogeny walks

Aleksei Udovenko

SnT, University of Luxembourg

Leuven Isogeny Days 7 | September 18, 2026



Work funded by the Luxembourg National Research Fund's (FNR)
project PQSeal (CORE/24/IS/18978392)

Do you remember ... isogeny graphs?



Do you remember ... isogeny graphs?



$$\begin{aligned}\Phi_2(X, Y) = & X^3 + Y^3 - X^2Y^2 + 1488XY(X + Y) - 162000(X^2 + Y^2) \\ & + 40773375XY + 8748000000(X + Y) - 157464000000000\end{aligned}$$

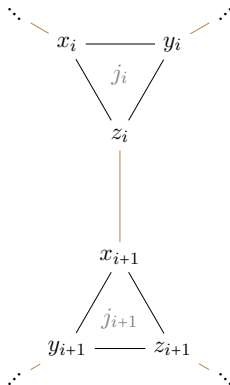
Some alternatives

Requirements:

- **algebraic**: finite fields
- **iterative**: $\Phi(X_i, X_{i+1}) = 0$ describes a walk
- **[non-backtracking]**: cyclic isogenies

$$\Phi(X, Y) = Y^2 - 2X^2Y + 1$$

$$\begin{cases} x_i + y_i + z_i = 0 \\ x_i y_i z_i = 16 \\ z_i x_{i+1} = 16 \end{cases}$$



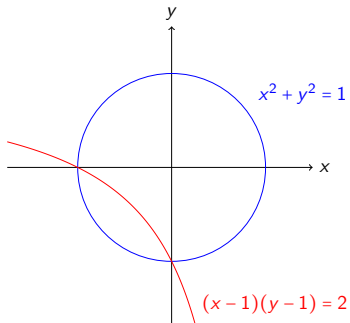
$$(\cos \alpha_i - 1)(\sin \alpha_{i+1} - 1) = 2$$

$$(\cos \alpha_i - 1)(\sin \alpha_{i+1} - 1) = 2$$

$$\Leftrightarrow \begin{cases} x_i^2 + y_i^2 = 1 \\ (y_i - 1)(x_{i+1} - 1) = 2 \end{cases}$$

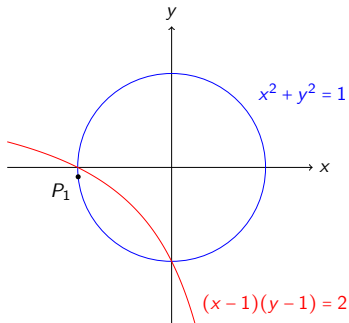
$$(\cos \alpha_i - 1)(\sin \alpha_{i+1} - 1) = 2$$

$$\Leftrightarrow \begin{cases} x_i^2 + y_i^2 = 1 \\ (y_i - 1)(x_{i+1} - 1) = 2 \end{cases}$$



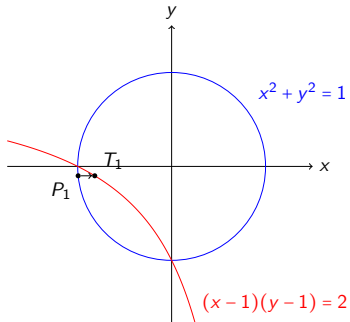
$$(\cos \alpha_i - 1)(\sin \alpha_{i+1} - 1) = 2$$

$$\Leftrightarrow \begin{cases} x_i^2 + y_i^2 = 1 \\ (y_i - 1)(x_{i+1} - 1) = 2 \end{cases}$$



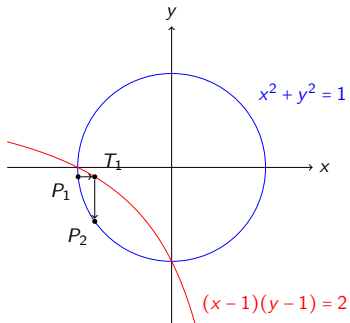
$$(\cos \alpha_i - 1)(\sin \alpha_{i+1} - 1) = 2$$

$$\Leftrightarrow \begin{cases} x_i^2 + y_i^2 = 1 \\ (y_i - 1)(x_{i+1} - 1) = 2 \end{cases}$$



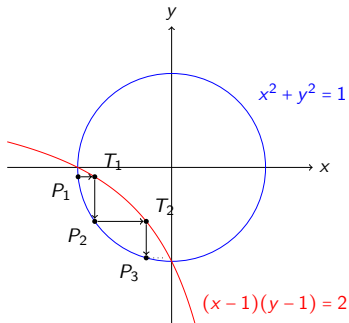
$$(\cos \alpha_i - 1)(\sin \alpha_{i+1} - 1) = 2$$

$$\Leftrightarrow \begin{cases} x_i^2 + y_i^2 = 1 \\ (y_i - 1)(x_{i+1} - 1) = 2 \end{cases}$$



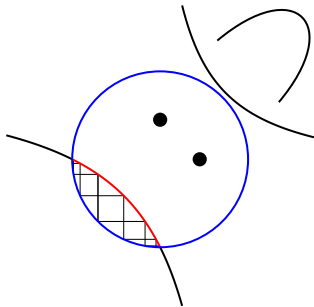
$$(\cos \alpha_i - 1)(\sin \alpha_{i+1} - 1) = 2$$

$$\Leftrightarrow \begin{cases} x_i^2 + y_i^2 = 1 \\ (y_i - 1)(x_{i+1} - 1) = 2 \end{cases}$$



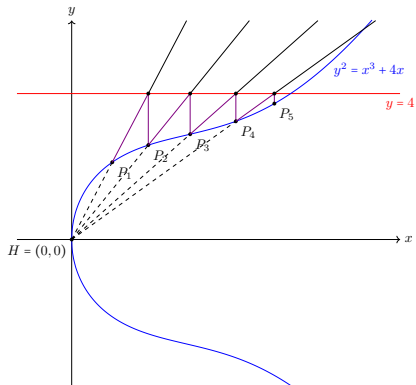
$$(\cos \alpha_i - 1)(\sin \alpha_{i+1} - 1) = 2$$

$$\Leftrightarrow \begin{cases} x_i^2 + y_i^2 = 1 \\ (y_i - 1)(x_{i+1} - 1) = 2 \end{cases}$$



$$\begin{cases} y_i^2 = x_i^3 + 4x_i \\ x_{i+1} = 4\frac{x_i}{y_i} \end{cases}$$

$$\begin{cases} y_i^2 = x_i^3 + 4x_i \\ x_{i+1} = 4\frac{x_i}{y_i} \end{cases}$$



$$\begin{cases} y_i^2 = x_i^3 + 4x_i \\ x_{i+1} = 4\frac{x_i}{y_i} \end{cases}$$



$$\ell = 2$$

$$\begin{cases} (x_i^2 - 1)(y_i^2 - 1) = 1 \\ (y_i - 1)(x_{i+1} - 1) = 4 \end{cases}$$

Noam D. Elkies. **Explicit modular towers** (2001)

$$\ell = 2$$

$$\begin{cases} (x_i^2 - 1)(y_i^2 - 1) = 1 \\ (y_i - 1)(x_{i+1} - 1) = 4 \end{cases}$$

$$\ell = 3$$

$$\begin{cases} (x_i^3 - 1)(y_i^3 - 1) = 1 \\ (y_i - 1)(x_{i+1} - 1) = 3 \end{cases}$$

$$\ell = 2$$

$$\begin{cases} (x_i^2 - 1)(y_i^2 - 1) = 1 \\ (y_i - 1)(x_{i+1} - 1) = 4 \end{cases}$$

$$\ell = 3$$

$$\begin{cases} (x_i^3 - 1)(y_i^3 - 1) = 1 \\ (y_i - 1)(x_{i+1} - 1) = 3 \end{cases}$$

$$\ell = 4$$

$$\begin{cases} (x_i^4 - 1)(y_i^4 - 1) = 1 \\ (y_i - 1)(x_{i+1} - 1) = 2 \end{cases}$$

$$\ell = 2$$

$$\begin{cases} (x_i^2 - 1)(y_i^2 - 1) = 1 \\ (y_i - 1)(x_{i+1} - 1) = 4 \end{cases}$$

$$\ell = 3$$

$$\begin{cases} (x_i^3 - 1)(y_i^3 - 1) = 1 \\ (y_i - 1)(x_{i+1} - 1) = 3 \end{cases}$$

$$\ell = 4$$

$$\begin{cases} (x_i^4 - 1)(y_i^4 - 1) = 1 \\ (y_i - 1)(x_{i+1} - 1) = 2 \end{cases}$$

$$\ell = 2$$

$$\begin{cases} (x_i^2 - 1)(y_i^2 - 1) = -8 \\ (y_i - 1)(x_{i+1} - 1) = 4 \end{cases}$$

01

Parametrizing isogenies

Modular curves

- $Y_0(N)$ is an abstract algebraic curve parametrizing cyclic N -isogenies ($p \nmid N$), up to pre-/post-isomorphisms:

$$Y_0(N) \cong \{(E, C) \mid C \subseteq E[N] \text{ cyclic}, |C| = N\} / \cong$$

Modular curves

- $Y_0(N)$ is an abstract algebraic curve parametrizing cyclic N -isogenies ($p \nmid N$), up to pre-/post-isomorphisms:

$$Y_0(N) \cong \{(E, C) \mid C \subseteq E[N] \text{ cyclic}, |C| = N\} / \cong$$

- $X_0(N) = Y_0(N) \cup \mathcal{C}$ is a compactification of $Y_0(N)$
- $\mathcal{C}$ is a finite set of *cusps* (roughly: cusp = “isogeny” at $j = \infty$)

Modular curves

- $Y_0(N)$ is an abstract algebraic curve parametrizing cyclic N -isogenies ($p \nmid N$), up to pre-/post-isomorphisms:

$$Y_0(N) \cong \{(E, C) \mid C \subseteq E[N] \text{ cyclic}, |C| = N\} / \cong$$

- $X_0(N) = Y_0(N) \cup \mathcal{C}$ is a compactification of $Y_0(N)$
- $\mathcal{C}$ is a finite set of *cusps* (roughly: cusp = “isogeny” at $j = \infty$)
- $\Phi_N(X, Y) = 0$ is a **singular** model of $X_0(N)$

Parametrizing isogenies

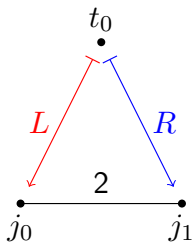
$$\begin{array}{ccc} & \Phi_2 = 0 & \\ \bullet & \text{---} & \bullet \\ j_0 & & j_1 \end{array}$$

Parametrizing isogenies

- $\Phi_2(X, Y)$: genus-zero
 $\Rightarrow X_0(2) \simeq \mathbb{P}^1$

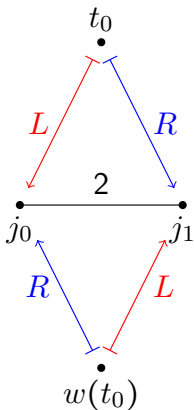
$$\begin{array}{ccc} & \Phi_2 = 0 & \\ \bullet & \text{---} & \bullet \\ j_0 & & j_1 \end{array}$$

Parametrizing isogenies



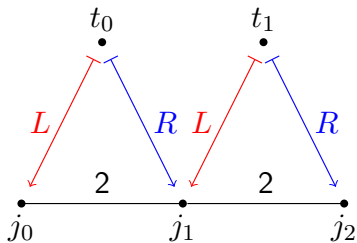
- $\Phi_2(X, Y)$: genus-zero
 $\Rightarrow X_0(2) \simeq \mathbb{P}^1$
- $L(t) = \frac{(t+256)^3}{t^2}$
- $R(t) = \frac{(t+16)^3}{t}$

Parametrizing isogenies

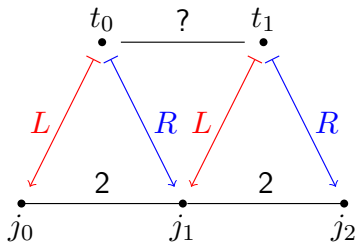


- $\Phi_2(X, Y)$: genus-zero
 $\Rightarrow X_0(2) \simeq \mathbb{P}^1$
- $L(t) = \frac{(t+256)^3}{t^2}$
- $R(t) = \frac{(t+16)^3}{t}$
- $w(t) = \frac{4096}{t}$

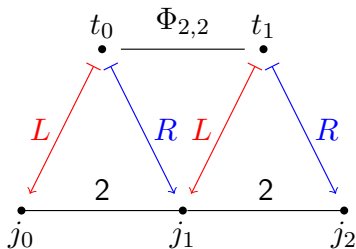
Parametrizing isogenies



Parametrizing isogenies

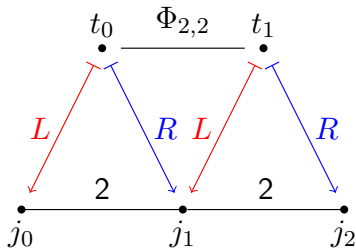


Parametrizing isogenies



- $R(t_0) = L(t_1) \quad (= j_1)$

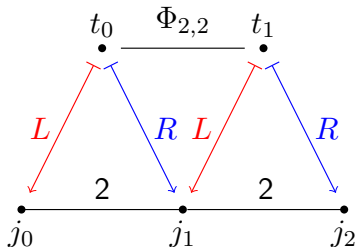
Parametrizing isogenies



- $R(t_0) = L(t_1) \quad (= j_1)$
- Splits as:

$$(t_1 - w(t_0)) \cdot \Phi_{2,2}(t_0, t_1) = 0$$

Parametrizing isogenies

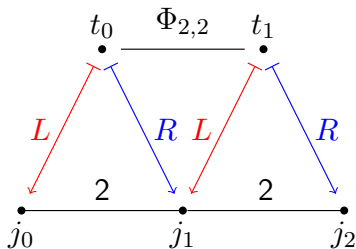


- $R(t_0) = L(t_1) \quad (= j_1)$
- Splits as:

$$(t_1 - w(t_0)) \cdot \Phi_{2,2}(t_0, t_1) = 0$$
- $\Phi_{2,2}(X, Y) =$

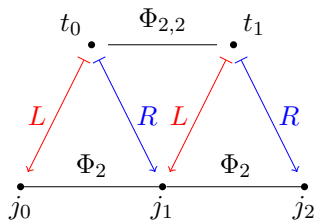
$$X^2Y + 48XY + 4096X - Y^2$$

Parametrizing isogenies



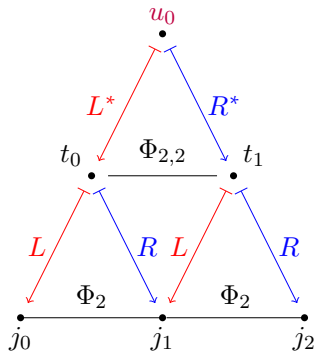
- $R(t_0) = L(t_1) \quad (= j_1)$
- Splits as:
 $(t_1 - w(t_0)) \cdot \Phi_{2,2}(t_0, t_1) = 0$
- $\Phi_{2,2}(X, Y) =$
 $X^2Y + 48XY + 4096X - Y^2$
- Still genus-zero!

Going deeper & overlaps



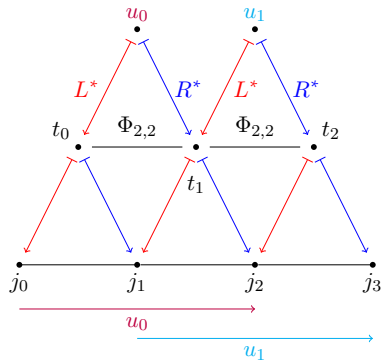
- $\Phi_{2,2}(X, Y)$: genus-zero

Going deeper & overlaps

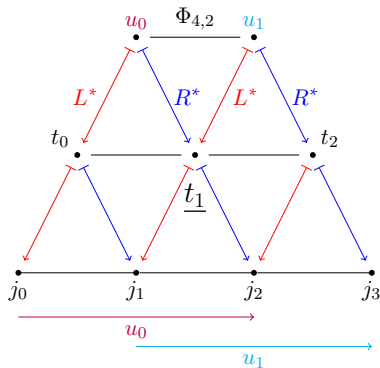


- $\Phi_{2,2}(X, Y)$: genus-zero
- $L^*(u) = \frac{-4(u+2)^2}{u-2}$
- $R^*(u) = 16u^2 - 64$

Going deeper & overlaps



Going deeper & overlaps



- $R^*(u_0) = L^*(u_1)$

- Yields directly

$$\Phi_{4,2}(X, Y) =$$

$$4(X^2 - 4)(Y - 2) + (Y + 2)^2$$

2-isogenies of 2^e -isogenies

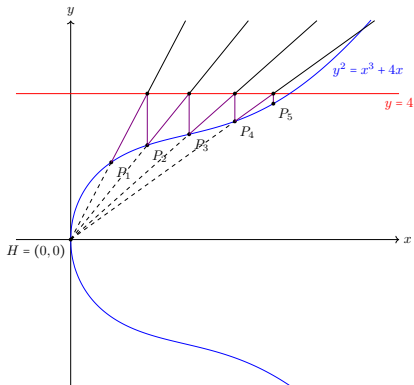
N	$L(t)$	$R(t)$	$\Phi_{N,2}(X, Y)$
1	—	—	$\Phi_2(X, Y)$
2	$\frac{(t+256)^3}{t^2}$	$\frac{(t+16)^3}{t}$	$X^2Y + 48XY + 4096X - Y^2$
4	$\frac{-4(t+2)^2}{t-2}$	$16t^2 - 64$	$4(X^2 - 4)(Y - 2) + (Y + 2)^2$
8	$-t - \frac{1}{t}$	$-4t^2 + 2$	$4X^2Y - (Y + 1)^2$
16	$\frac{1}{2} \left(t + \frac{1}{t} \right)$	t^2	$2X^2Y - Y^2 - 1$

2-isogenies of 2^e -isogenies

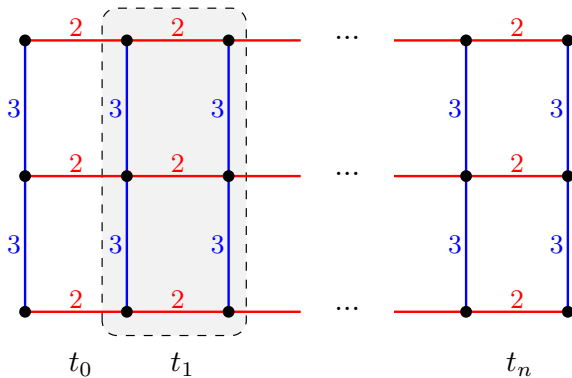
N	$L(t)$	$R(t)$	$\Phi_{N,2}(X, Y)$
1	—	—	$\Phi_2(X, Y)$
2	$\frac{(t+256)^3}{t^2}$	$\frac{(t+16)^3}{t}$	$X^2Y + 48XY + 4096X - Y^2$
4	$\frac{-4(t+2)^2}{t-2}$	$16t^2 - 64$	$4(X^2 - 4)(Y - 2) + (Y + 2)^2$
8	$-t - \frac{1}{t}$	$-4t^2 + 2$	$4X^2Y - (Y + 1)^2$
16	$\frac{1}{2} \left(t + \frac{1}{t} \right)$	t^2	$2X^2Y - Y^2 - 1$
32	$\frac{t_1}{2t_0}$	$\frac{2}{t_0}$	$X_0Y_1 - 4Y_0$
$(t_0, t_1) \in E : y^2 = x^3 + 4x$			

Godzilla walk

$$\begin{cases} y_i^2 = x_i^3 + 4x_i \\ x_{i+1} = 4\frac{x_i}{y_i} \end{cases}$$



Describing ladders $(X_0(18 \cdot 2^n))$



$$t_{i+1}^2 - t_i^2 t_{i+1} + 2t_i = 0$$

Advantages

1. **Non-backtracking** (cyclic isogenies):

$\Phi_{N,\ell}(X, Y) = 0$ is a model for $X_0(N\ell)$

Advantages

1. **Non-backtracking** (cyclic isogenies):

$\Phi_{N,\ell}(X, Y) = 0$ is a model for $X_0(N\ell)$

2. Reduced singularities (more **smooth** models):

Advantages

1. **Non-backtracking** (cyclic isogenies):

$\Phi_{N,\ell}(X, Y) = 0$ is a model for $X_0(N\ell)$

2. Reduced singularities (more **smooth** models):

- let $(t_0, \dots, t_n)$ be an isogeny walk, $\Phi_{N,\ell}(t_i, t_{i+1}) = 0$ ($X_0(N\ell^n)$)

Advantages

1. **Non-backtracking** (cyclic isogenies):

$\Phi_{N,\ell}(X, Y) = 0$ is a model for $X_0(N\ell)$

2. Reduced singularities (more **smooth** models):

- let $(t_0, \dots, t_n)$ be an isogeny walk, $\Phi_{N,\ell}(t_i, t_{i+1}) = 0$ ($X_0(N\ell^n)$)
- smooth away from $j = 0, 1728$ and cusps

Advantages

1. Non-backtracking (cyclic isogenies):

$\Phi_{N,\ell}(X, Y) = 0$ is a model for $X_0(N\ell)$

2. Reduced singularities (more smooth models):

- let $(t_0, \dots, t_n)$ be an isogeny walk, $\Phi_{N,\ell}(t_i, t_{i+1}) = 0$ ($X_0(N\ell^n)$)
- smooth away from $j = 0, 1728$ and cusps
- smooth away from cusps for (N, ℓ) pairs:

$(8, 2)$

$(16, 2)$

$(12, 2)$ $(12, 3)$

$(18, 2)$ $(18, 3)$

Radical 5-isogeny decomposition

$$x^5 = \frac{y^5 - 3y^4 + 4y^3 - 2y^2 + y}{y^4 + 2y^3 + 4y^2 + 3y + 1}$$

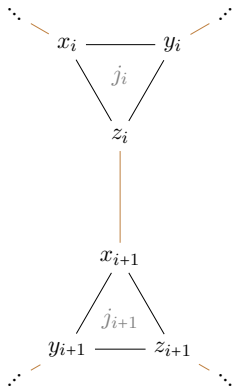
Radical 5-isogeny decomposition

$$\begin{aligned}x^5 &= \frac{y^5 - 3y^4 + 4y^3 - 2y^2 + y}{y^4 + 2y^3 + 4y^2 + 3y + 1} \\&= \left(\frac{1 - c_1 z}{z + c_1} \right) \circ (\cdot)^5 \circ \left(\frac{1 - c_2 z}{z + c_2} \right) (y) \\c_1 &= \frac{11 + 5\sqrt{5}}{2}, \quad c_2 = \frac{1 + \sqrt{5}}{2}\end{aligned}$$

03 Mysterious walks

Triangle walk

$$\begin{cases} x_i + y_i + z_i = 0 \\ x_i y_i z_i = 16 \\ z_i x_{i+1} = 16 \end{cases}$$

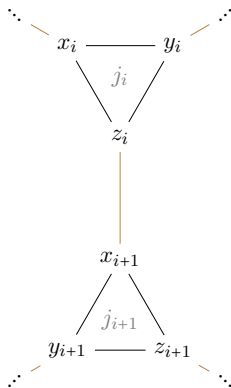


Triangle walk

1. Recall $R(D) = \frac{(D+16)^3}{D}$ for

$$D \in X_0(2)$$

$$\Rightarrow D^3 + 48D^2 + (768 - j)D + 4096 = 0$$

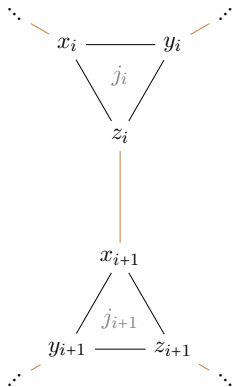


Triangle walk

1. Recall $R(D) = \frac{(D+16)^3}{D}$ for
 $D \in X_0(2)$
 $\Rightarrow D^3 + 48D^2 + (768 - j)D + 4096 = 0$

2. Roots $D_1, D_2, D_3 \in X_0(2)$ with
 $R(D_i) = j$ satisfy

$$\begin{cases} D_1 + D_2 + D_3 = -48, \\ D_1 D_2 D_3 = -4096 \end{cases}$$



Triangle walk

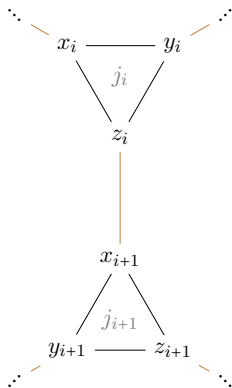
1. Recall $R(D) = \frac{(D+16)^3}{D}$ for
 $D \in X_0(2)$
 $\Rightarrow D^3 + 48D^2 + (768 - j)D + 4096 = 0$

2. Roots $D_1, D_2, D_3 \in X_0(2)$ with
 $R(D_i) = j$ satisfy

$$\begin{cases} D_1 + D_2 + D_3 = -48, \\ D_1 D_2 D_3 = -4096 \end{cases}$$

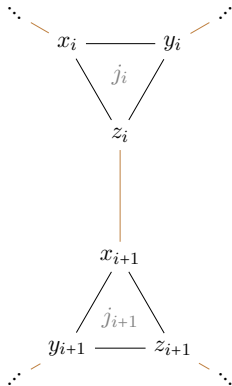
and switch triangles by

$$D' = w(D_i) = 4096/D_i$$



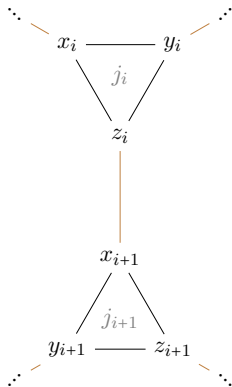
Triangle walk

$$\begin{cases} x_i + y_i + z_i = -48 \\ x_i y_i z_i = -4096 \\ z_i x_{i+1} = 4096 \end{cases}$$



Triangle walk

1. Extract cube roots! $d = \sqrt[3]{D}$



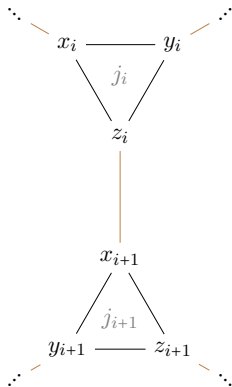
Triangle walk

1. Extract cube roots! $d = \sqrt[3]{D}$

2. $R_Y(d) = \frac{d^3+16}{d}$ for

$$d \in Y = X_0(2) \otimes X_{\text{ns}}^+(3)$$

$$\Rightarrow d^3 - jd + 16 = 0$$



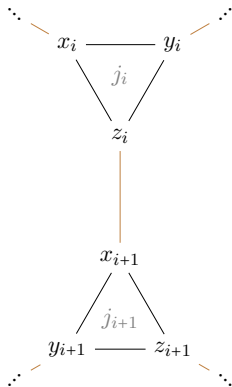
Triangle walk

1. Extract cube roots! $d = \sqrt[3]{D}$

2. $R_Y(d) = \frac{d^3+16}{d}$ for
 $d \in Y = X_0(2) \otimes X_{\text{ns}}^+(3)$
 $\Rightarrow d^3 - jd + 16 = 0$

3. Roots $d_1, d_2, d_3 \in Y$ with
 $R(d_i) = j$ satisfy

$$\begin{cases} d_1 + d_2 + d_3 = 0, \\ d_1 d_2 d_3 = -16 \end{cases}$$



Triangle walk

1. Extract cube roots! $d = \sqrt[3]{D}$

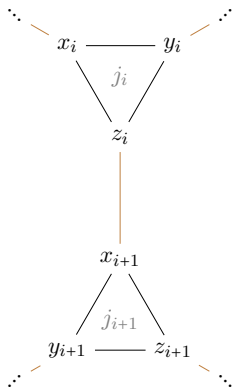
2. $R_Y(d) = \frac{d^3+16}{d}$ for
 $d \in Y = X_0(2) \otimes X_{\text{ns}}^+(3)$
 $\Rightarrow d^3 - jd + 16 = 0$

3. Roots $d_1, d_2, d_3 \in Y$ with
 $R(d_i) = j$ satisfy

$$\begin{cases} d_1 + d_2 + d_3 = 0, \\ d_1 d_2 d_3 = -16 \end{cases}$$

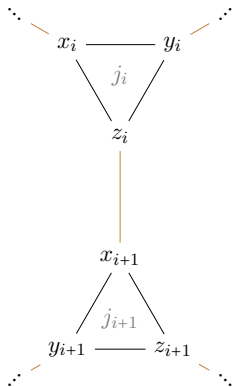
and switch triangles by

$$d' = w_Y(d_i) = 16/d_i$$



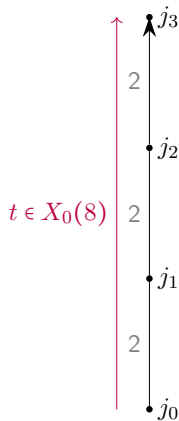
Triangle walk

$$\begin{cases} x_i + y_i + z_i = 0 \\ x_i y_i z_i = 16 \\ z_i x_{i+1} = 16 \end{cases}$$



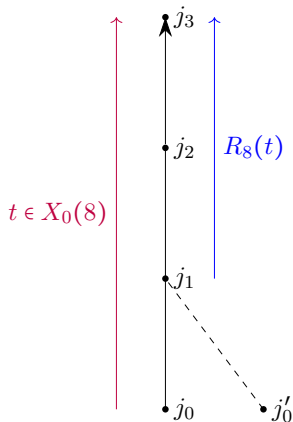
Circle-hyperbola walk

1. Let $t \in X_0(8)$



Circle-hyperbola walk

1. Let $t \in X_0(8)$
2. $R_8(t) = -4t^2 + 2 \in X_0(4)$



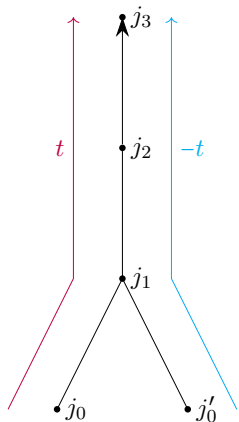
Circle-hyperbola walk

1. Let $t \in X_0(8)$
2. $R_8(t) = -4t^2 + 2 \in X_0(4)$
3. Short tail “wiggle”:

$$R_8(x) = R_8(y)$$

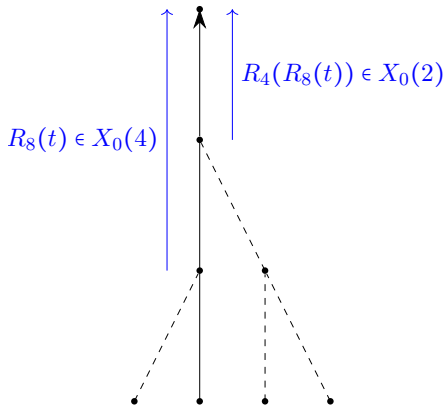
$$\iff x^2 = y^2$$

$$\iff x = \pm y$$



Circle-hyperbola walk

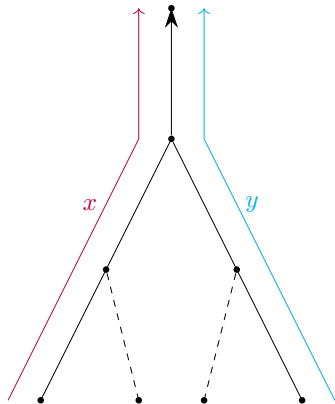
1. Let $t \in X_0(8)$
2. $R_8(t) = -4t^2 + 2 \in X_0(4)$
3. $R_4(t) = 16t^2 - 64 \in X_0(2)$



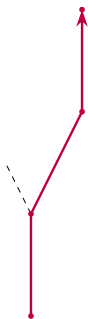
Circle-hyperbola walk

1. Let $t \in X_0(8)$
2. $R_8(t) = -4t^2 + 2 \in X_0(4)$
3. $R_4(t) = 16t^2 - 64 \in X_0(2)$
4. Long tail “wiggle”:

$$\begin{aligned} R_4(R_8(x)) &= R_4(R_8(y)) \\ \iff x^2(1-x^2) &= y^2(1-y^2) \\ \iff \underbrace{(x^2 - y^2)}_{\text{short}} \underbrace{(x^2 + y^2 - 1)}_{\text{long}} \end{aligned}$$

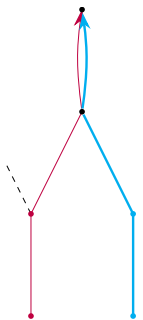


Snake dance



$$\mathbf{x}_1 \in X_0(8)$$

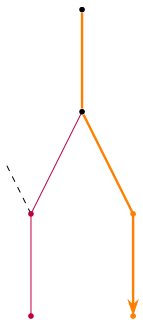
Snake dance



x_1 y_1

$$x_1^2 + y_1^2 = 1$$

Snake dance



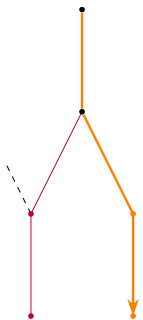
x_1

$\hat{y}_1$

$$x_1^2 + y_1^2 = 1$$

$$\hat{y}_1 = w_8(y_1)$$

Snake dance



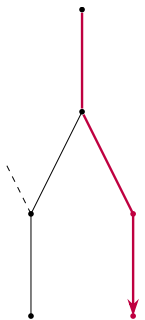
x_1

$\hat{y}_1$

$$x_1^2 + y_1^2 = 1$$

$$(\hat{y}_1 - 1)(y_1 - 1) = 2$$

Snake dance

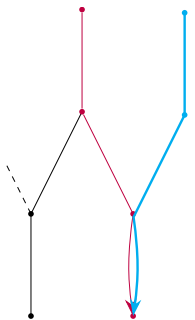


x_1

x_2

$$x_2 = \hat{y}_1$$

Snake dance



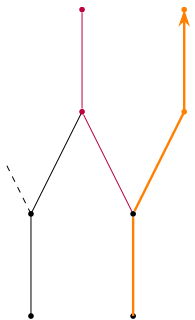
x_1

x_2

y_2

$$x_2^2 + y_2^2 = 1$$

Snake dance



x_1

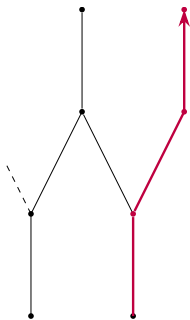
x_2

$\widehat{y}_2$

$$x_2^2 + y_2^2 = 1$$

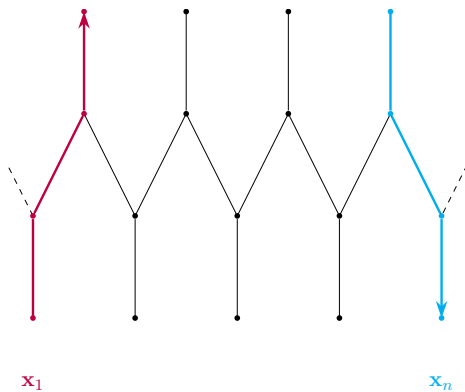
$$(\widehat{y}_2 - 1)(y_2 - 1) = 2$$

Snake dance

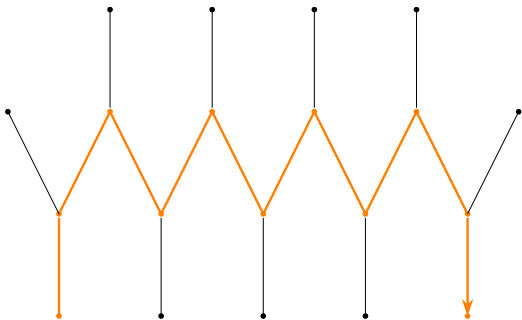


x_i

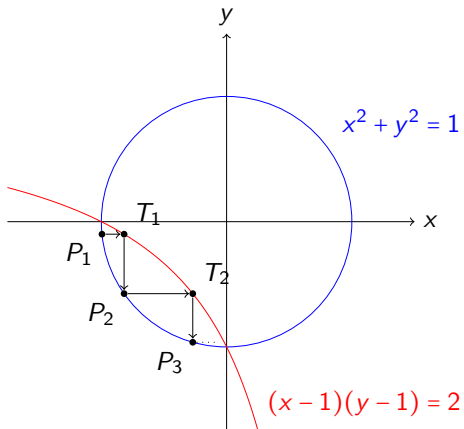
Snake dance



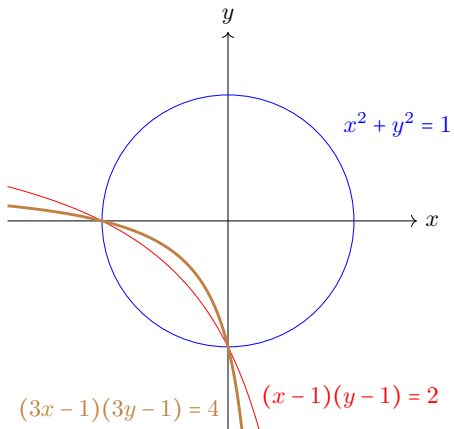
Snake dance



Snake dance



Snake dance



Conclusions

Elkies method modpolys:

- Non-backtracking
- Smooth(er)
- Many compact cases

Conclusions

Elkies method modpolys:

- Non-backtracking
- Smooth(er)
- Many compact cases

Applications:

- [Zero-knowledge] proofs
- Optimize algebraic attacks
- Funny walks
- ???

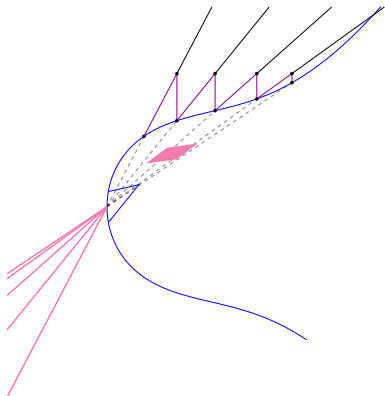
Conclusions

Elkies method modpolys:

- Non-backtracking
- Smooth(er)
- Many compact cases

Applications:

- [Zero-knowledge] **proofs**
- Optimize algebraic **attacks**
- Funny **walks**
- ???



04 Extras

2-isogenies of the Montgomery model

$$E_A : y^2 = x^3 + Ax + x$$

N	role	$\Phi_{N,2}$
1	j -invariant	$\Phi_2(j, j')$
2	discriminant $\simeq A^2 - 4$	$C^2D + 48CD + 4096C - D^2$
4	A -coefficient	$4(A^2 - 4)(B - 2) + (B + 2)^2$ *
8	x -coef. of nonconst. $E_A[2]$	$4x^2y - (y + 1)^2$ **
16	x -coef. of nonconst. $E_A[4] \setminus E_A[2]$	$2x^2y - y^2 - 1$ ***

2-isogenies of the Montgomery model

$$E_A : y^2 = x^3 + Ax + x$$

N	role	$\Phi_{N,2}$
1	j -invariant	$\Phi_2(j, j')$
2	discriminant $\simeq A^2 - 4$	$C^2D + 48CD + 4096C - D^2$
4	A -coefficient	$4(A^2 - 4)(B - 2) + (B + 2)^2$ *
8	x -coef. of nonconst. $E_A[2]$	$4x^2y - (y + 1)^2$ **
16	x -coef. of nonconst. $E_A[4] \setminus E_A[2]$	$2x^2y - y^2 - 1$ ***

* J. Meers, J. Nowakowski. Solving the Hidden Number Problem for CSIDH and CSURF via Automated Coppersmith (ASIACRYPT 2023)

2-isogenies of the Montgomery model

$$E_A : y^2 = x^3 + Ax + x$$

N	role	$\Phi_{N,2}$
1	j -invariant	$\Phi_2(j, j')$
2	discriminant $\simeq A^2 - 4$	$C^2D + 48CD + 4096C - D^2$
4	A -coefficient	$4(A^2 - 4)(B - 2) + (B + 2)^2$ *
8	x -coef. of nonconst. $E_A[2]$	$4x^2y - (y + 1)^2$ **
16	x -coef. of nonconst. $E_A[4] \setminus E_A[2]$	$2x^2y - y^2 - 1$ ***

** Wikipedia. [Modular lambda function](#)

J. M. Borwein, P. B. Borwein. [Pi and the AGM: a study in the analytic number theory and computational complexity](#) (1987)

2-isogenies of the Montgomery model

$$E_A : y^2 = x^3 + Ax + x$$

N	role	$\Phi_{N,2}$
1	j -invariant	$\Phi_2(j, j')$
2	discriminant $\simeq A^2 - 4$	$C^2D + 48CD + 4096C - D^2$
4	A -coefficient	$4(A^2 - 4)(B - 2) + (B + 2)^2$ *
8	x -coef. of nonconst. $E_A[2]$	$4x^2y - (y + 1)^2$ **
16	x -coef. of nonconst. $E_A[4] \setminus E_A[2]$	$2x^2y - y^2 - 1$ ***

*** J.J. León, V. Muñoz. On some non-linear recurrences over finite fields linked to isogeny graphs (ePrint 2025/608)

ℓ -isogenies of N -isogenies

N	ℓ	$\Phi_{N,\ell}(x, y)$
2	2	$x^2y + 48xy - y^2 + 4096x$
4	2	$4(x^2 - 4)(y - 2) + (y + 2)^2$
8	2	$4x^2y - (y + 1)^2$
16	2	$2x^2y - y^2 - 1$
Y	2	$x^2y - y^2 + 16x$

ℓ -isogenies of N -isogenies

N	ℓ	$\Phi_{N,\ell}(x, y)$
2	2	$x^2y + 48xy - y^2 + 4096x$
4	2	$4(x^2 - 4)(y - 2) + (y + 2)^2$
8	2	$4x^2y - (y + 1)^2$
16	2	$2x^2y - y^2 - 1$
Y	2	$x^2y - y^2 + 16x$
Z	3	$x^3y^2 - 27x^2y + 18xy^2 - y^3 + 729x$
9	3	$x^3(y^2 + 3y + 9) - (y + 6)^3$
18	3	$x^3(y^2 - y + 1) + (y^3 + 2y^2 + 4y)$

ℓ -isogenies of N -isogenies

N	ℓ	$\Phi_{N,\ell}(x, y)$
2	2	$x^2y + 48xy - y^2 + 4096x$
4	2	$4(x^2 - 4)(y - 2) + (y + 2)^2$
8	2	$4x^2y - (y + 1)^2$
16	2	$2x^2y - y^2 - 1$
Y	2	$x^2y - y^2 + 16x$
Z	3	$x^3y^2 - 27x^2y + 18xy^2 - y^3 + 729x$
9	3	$x^3(y^2 + 3y + 9) - (y + 6)^3$
18	3	$x^3(y^2 - y + 1) + (y^3 + 2y^2 + 4y)$
6	2	$x^2y - x^2 - 8xy - y^2 + 9y$
10	2	$x^2y - 2xy - y^2 - 4x$
12	2	$x^2(y - 1) - y(y + 3)$
18	2	$x^2y - y^2 - 2x$

ℓ -isogenies of N -isogenies

N	ℓ	$\Phi_{N,\ell}(x, y)$
2	2	$x^2y + 48xy - y^2 + 4096x$
4	2	$4(x^2 - 4)(y - 2) + (y + 2)^2$
8	2	$4x^2y - (y + 1)^2$
16	2	$2x^2y - y^2 - 1$
Y	2	$x^2y - y^2 + 16x$
Z	3	$x^3y^2 - 27x^2y + 18xy^2 - y^3 + 729x$
9	3	$x^3(y^2 + 3y + 9) - (y + 6)^3$
18	3	$x^3(y^2 - y + 1) + (y^3 + 2y^2 + 4y)$
6	2	$x^2y - x^2 - 8xy - y^2 + 9y$
10	2	$x^2y - 2xy - y^2 - 4x$
12	2	$x^2(y - 1) - y(y + 3)$
18	2	$x^2y - y^2 - 2x$

Radical form

- Let $R(t) = t^\ell$

Radical form

- Let $R(t) = t^\ell$
- Then $R(x) = L(y)$ becomes

$$x^\ell = w^* \circ R \circ w(y) = w^*(w(y)^\ell)$$

Radical form

- Let $R(t) = t^\ell$
- Then $R(x) = L(y)$ becomes

$$x^\ell = w^* \circ R \circ w(y) = w^*(w(y)^\ell)$$
$$\Leftrightarrow x = \sqrt[\ell]{w^*(w(y)^\ell)}$$

Radical form

- Let $R(t) = t^\ell$
- Then $R(x) = L(y)$ becomes

$$x^\ell = w^* \circ R \circ w(y) = w^*(w(y)^\ell)$$

$$\Leftrightarrow x = \sqrt[\ell]{w^*(w(y)^\ell)}$$

$$\Leftrightarrow y = w \left(\sqrt[\ell]{w^*(x^\ell)} \right)$$

Radical form

- Let $R(t) = t^\ell$
- Then $R(x) = L(y)$ becomes

$$x^\ell = w^* \circ R \circ w(y) = w^*(w(y)^\ell)$$

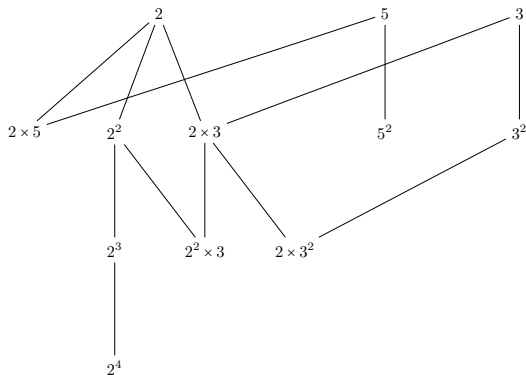
$$\Leftrightarrow x = \sqrt[\ell]{w^*(w(y)^\ell)}$$

$$\Leftrightarrow y = w \left(\sqrt[\ell]{w^*(x^\ell)} \right)$$

Radical expressions

$X_0(N)$	ℓ	t^ℓ	$w(u)^\ell$
$X_0(4)$	2	$\frac{-u^2+20u-28}{4u-8}$	$\frac{-4(t^2-8)}{t^2-4}$
$X_0(8)$	2	$\frac{(u-1)^2}{4u}$	$\frac{1}{t^2-1}$
$X_0(12)$	2	$\frac{u(u+3)}{u-1}$	$\frac{t^2-9}{t^2-1}$
$X_0(16)$	2	$\frac{u^2+1}{2u}$	$\frac{t^2+1}{t^2-1}$
$X_0(16)$	4	$\frac{(u-1)^4}{8(u(u^2+1))}$	$\frac{1}{t^4-1}$
$X_0(9)$	3	$\frac{u^3-36u^2-54u-270}{u^2+3u+9}$	$\frac{-27(t^3-54)}{t^3-27}$
$X_0(18)$	3	$\frac{u^3+4u^2+2u+2}{u^2-u+1}$	$\frac{t^3+10}{t^3+1}$
$X(5)$	5	$\frac{u(u^4-3u^3+4u^2-2u+1)}{u^4+2u^3+4u^2+3u+1}$	$\frac{-ct^5+1}{t^5+c}$

Genus-zero cases of $X_0(N)$



7

13