UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

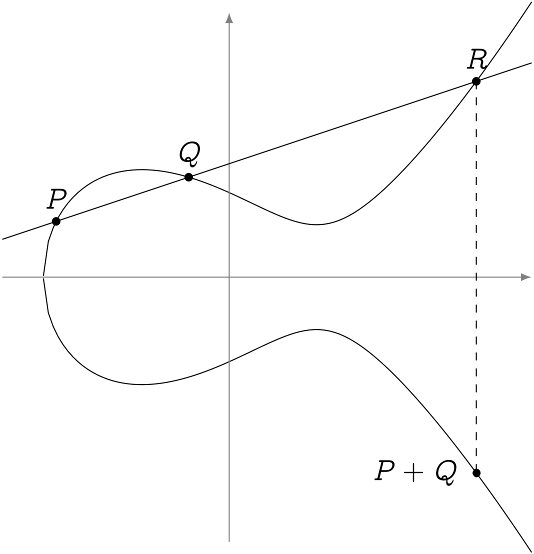
ISOGENY GRAPHS IN CRYPTOGRAPHY

Luca De Feo[1]
joint work with David Jao[2] and Jérôme Plût[1]

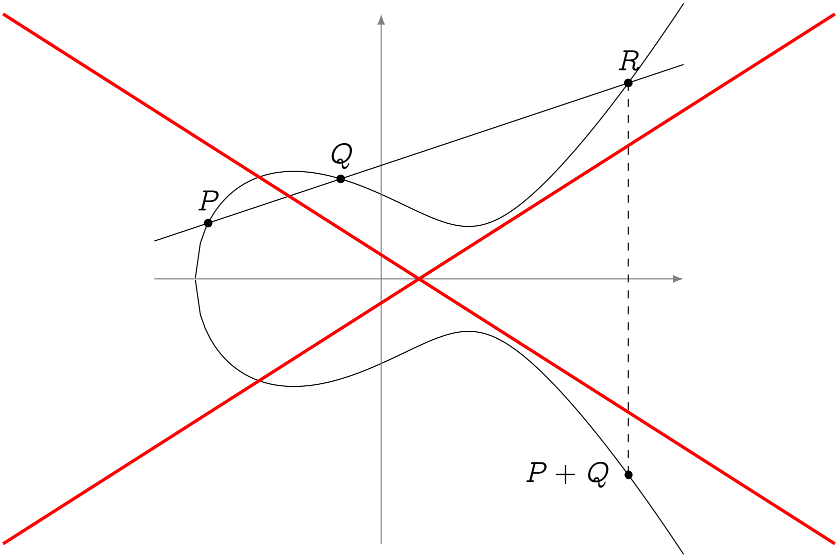
[1] Université de Versailles – Saint-Quentin-en-Yvelines, France
[2] University of Waterloo, Canada

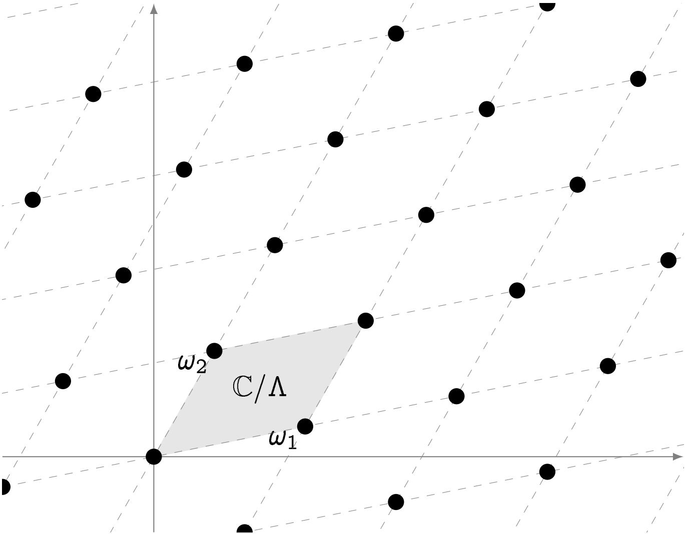
September 27, 2012, YACC '12, Porquerolles, France

Elliptic curves



Elliptic curves

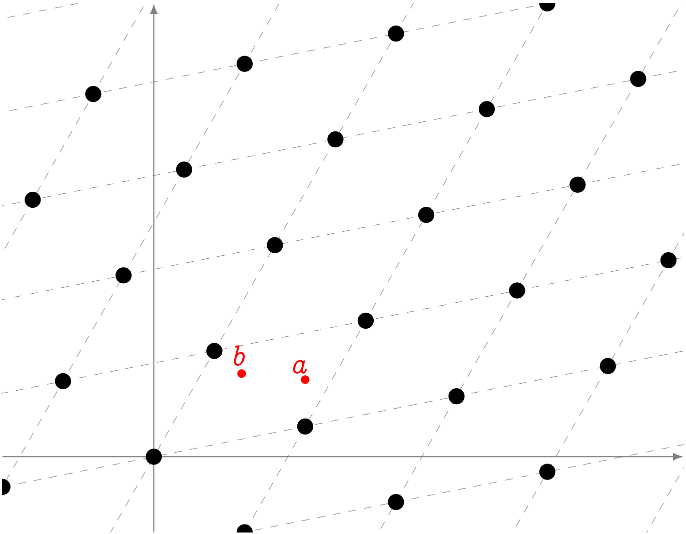




Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

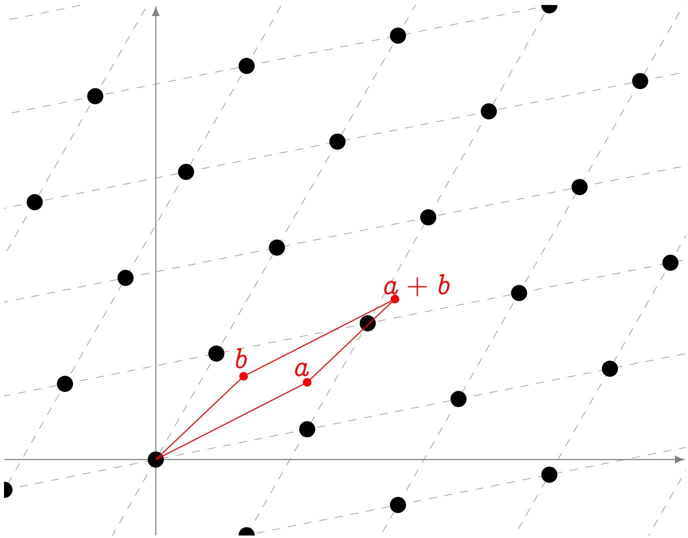
$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$$

$\mathbb{C}/\Lambda$ is an elliptic curve.



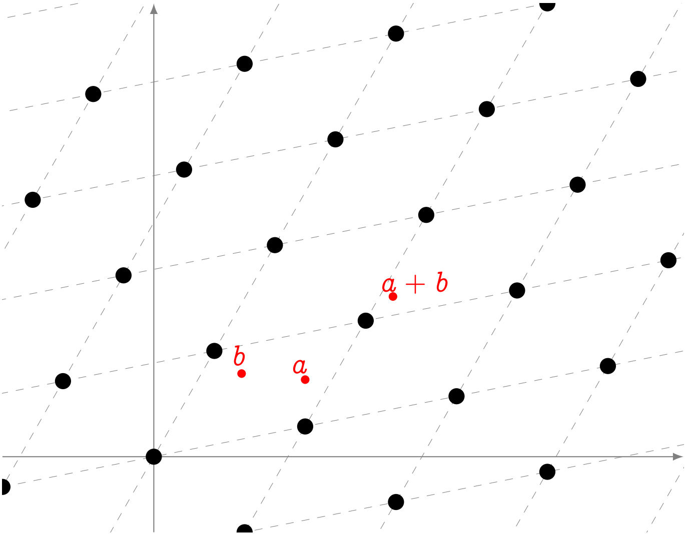
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves



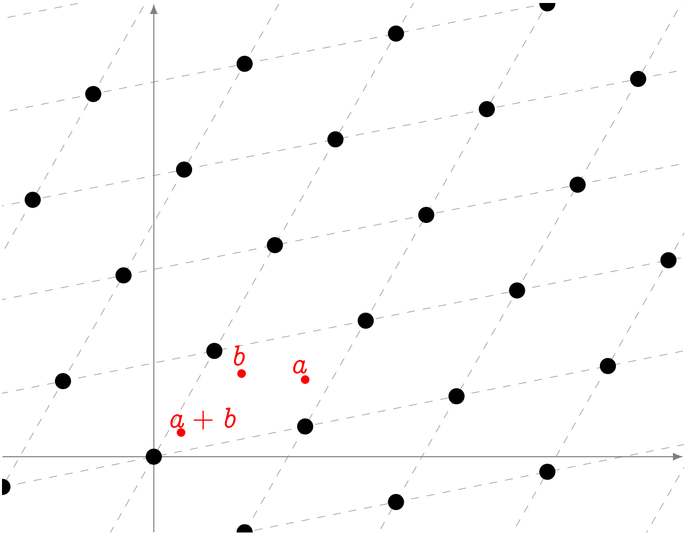
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves



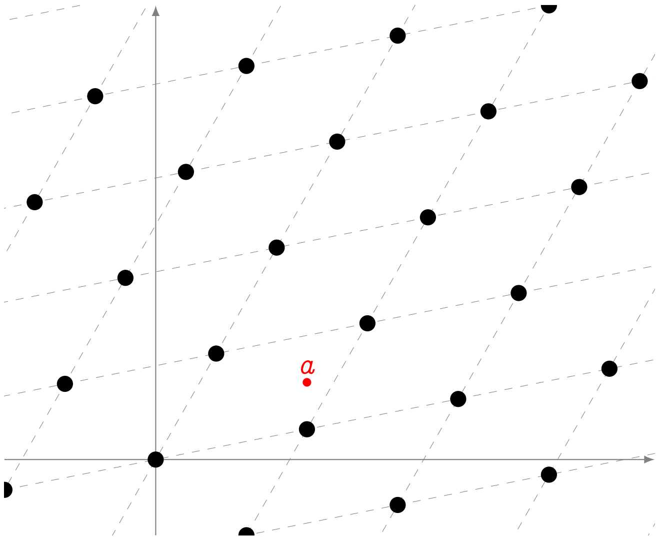
Addition law induced by addition on $\mathbb{C}$.

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES



Addition law induced by addition on $\mathbb{C}$.

Isomorphism classes

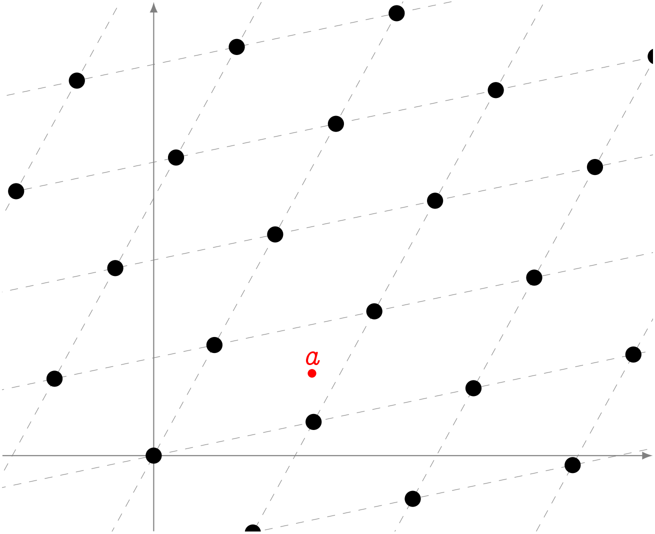


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

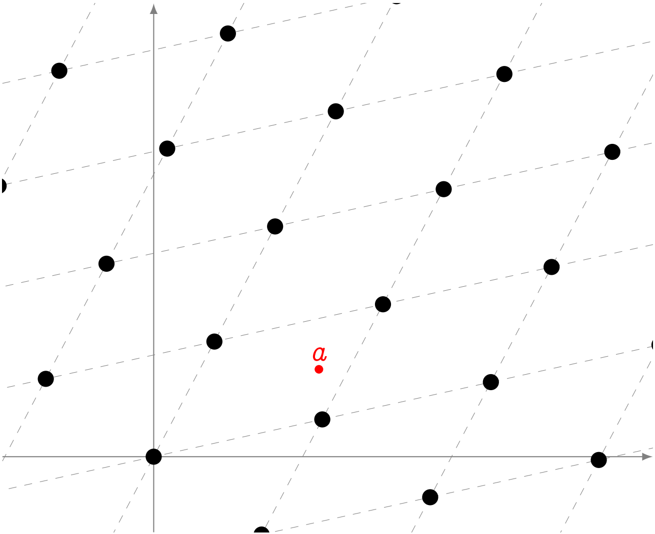


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

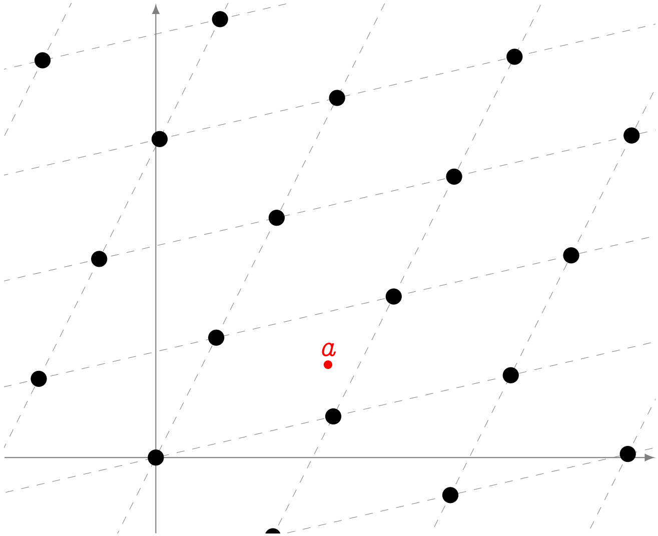


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

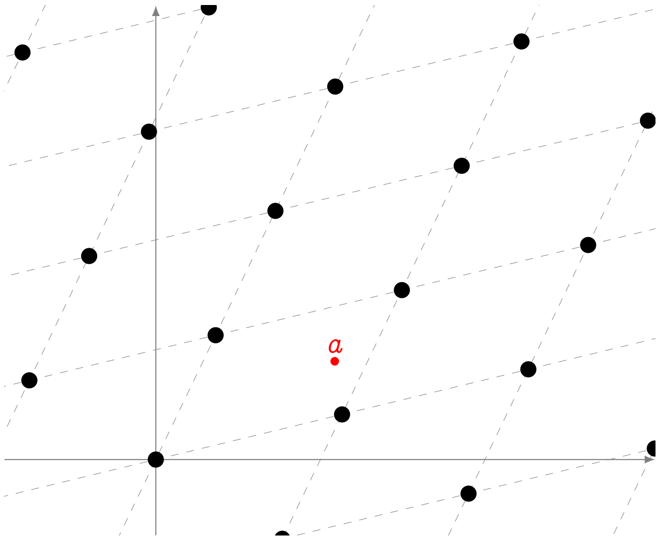


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

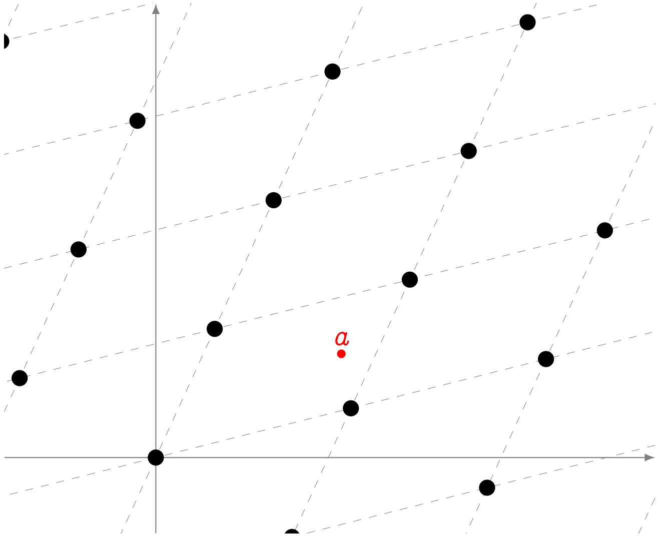


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

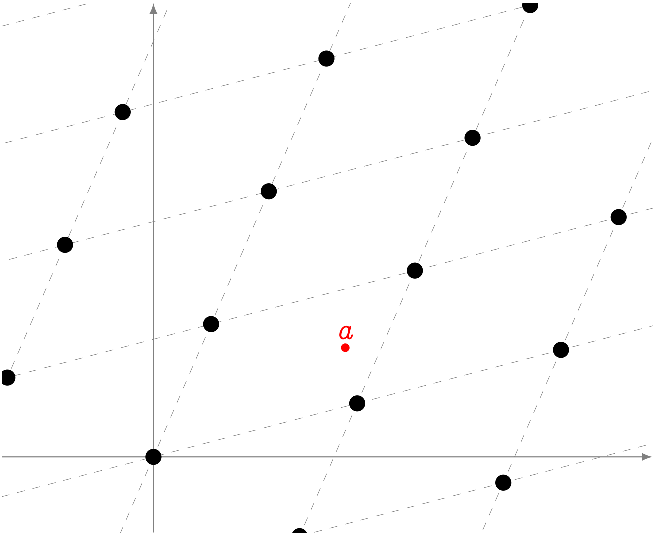
Isomorphism classes



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

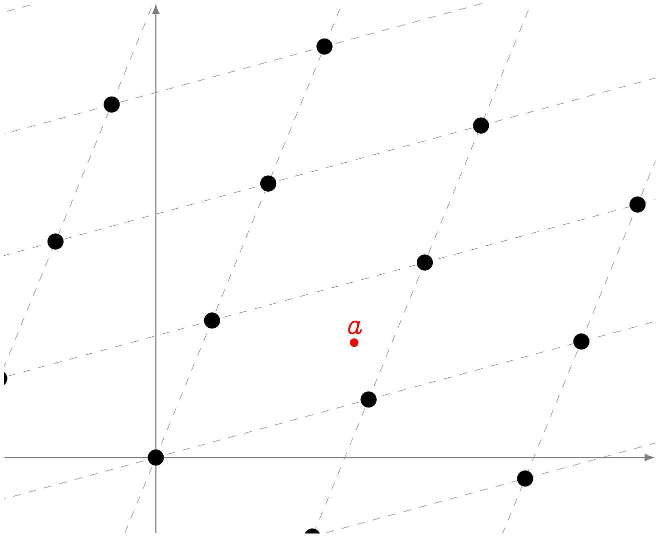


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

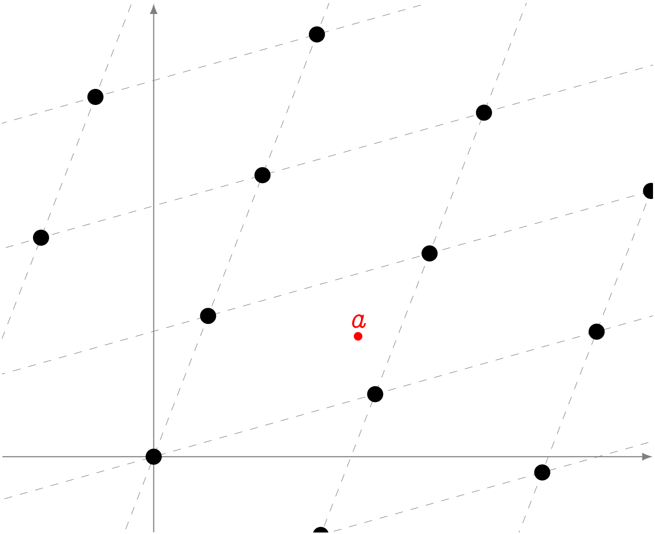
UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

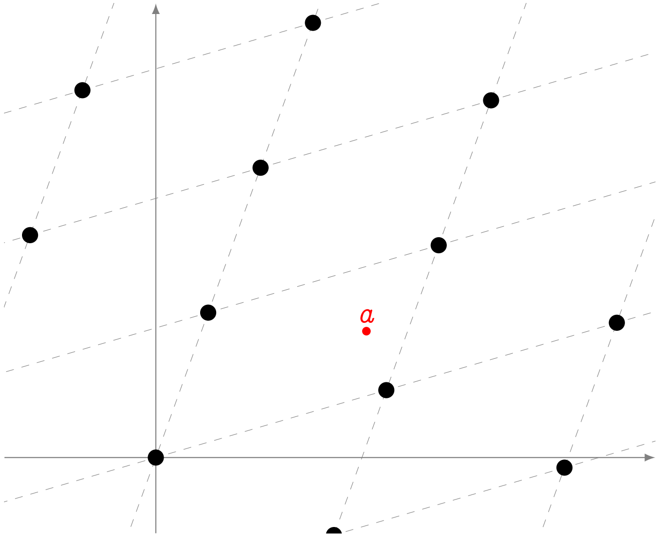


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

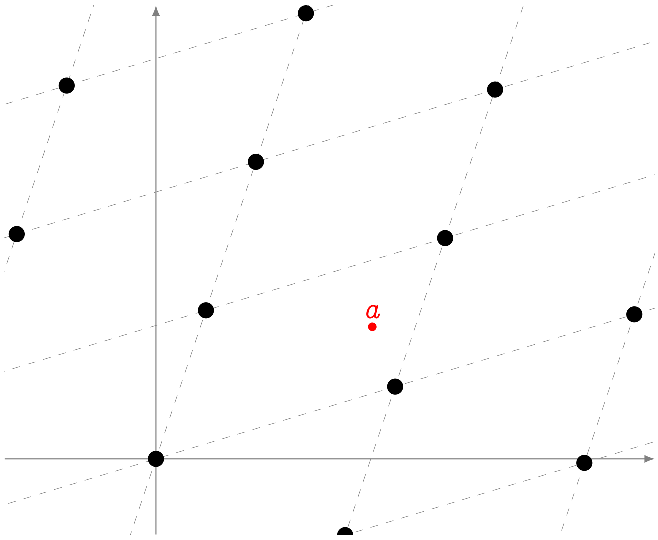


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

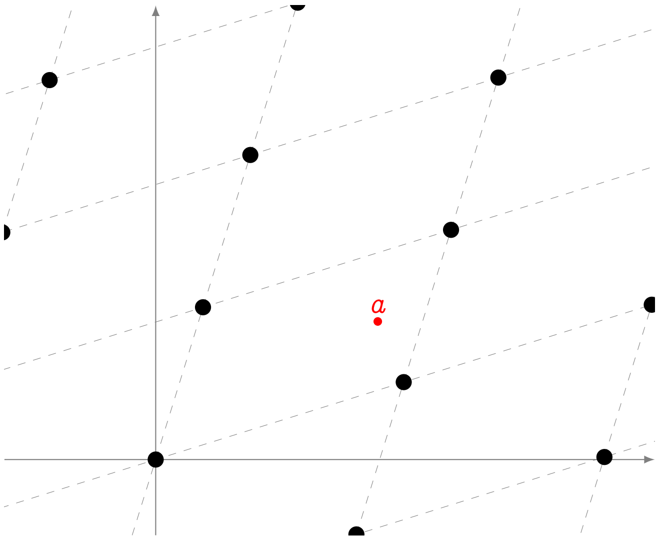
Isomorphism classes



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

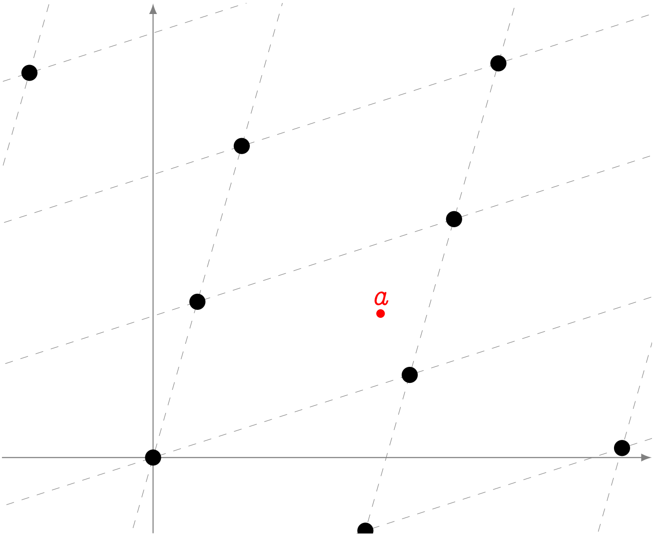
The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

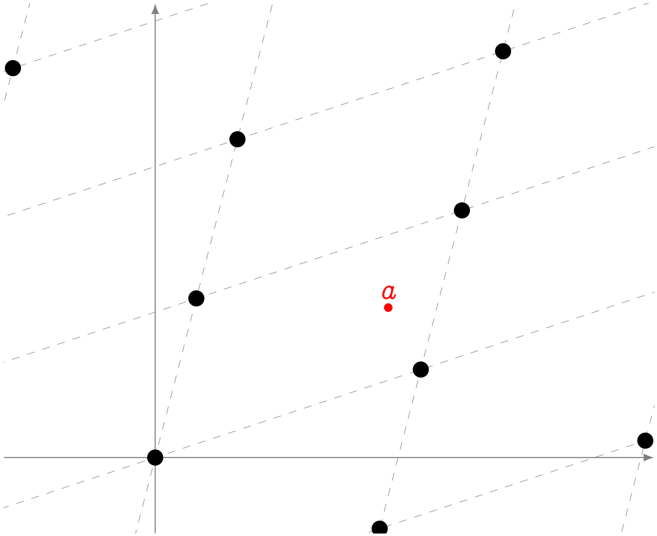


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

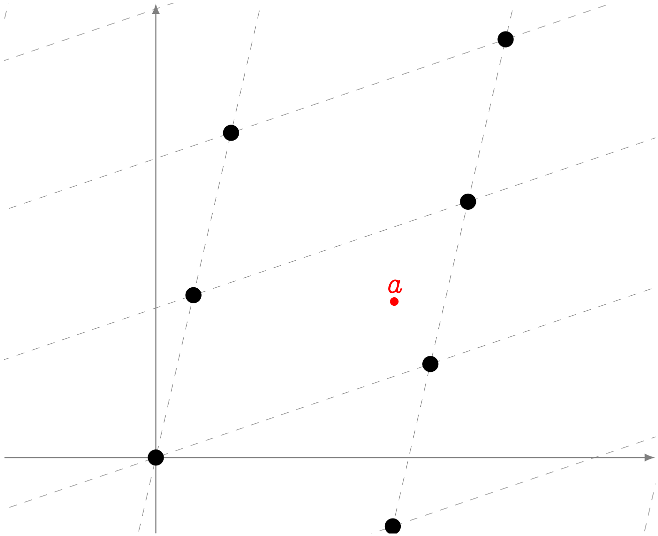


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

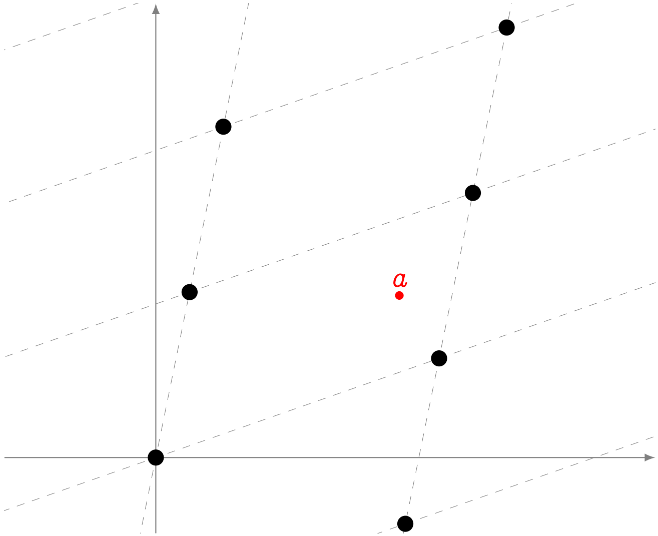


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

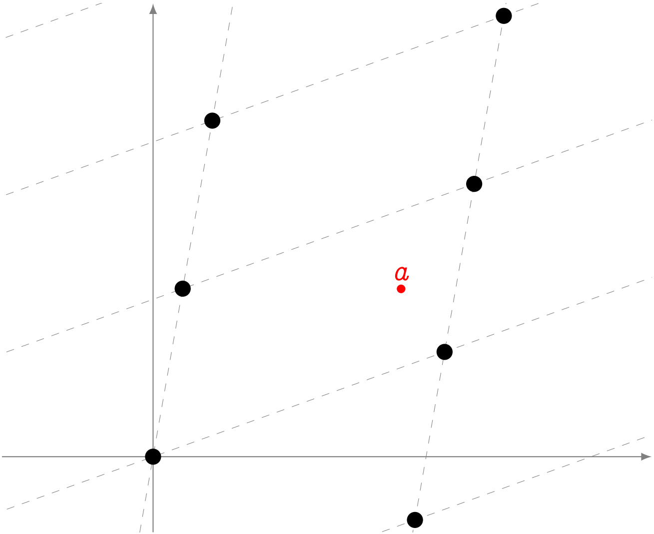


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

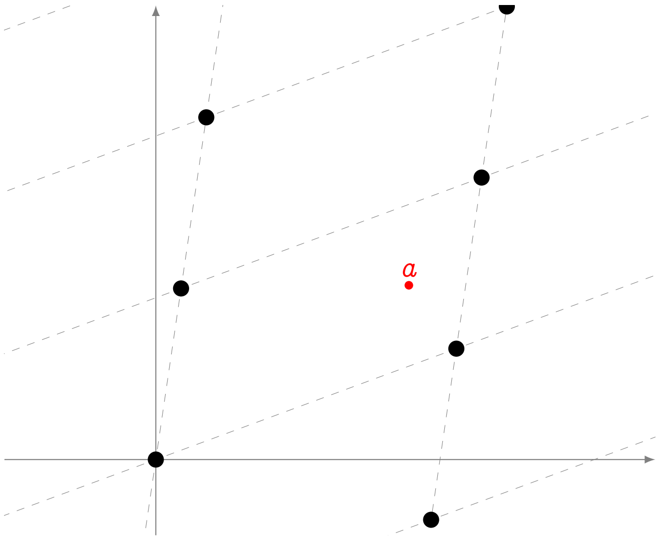
Isomorphism classes



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

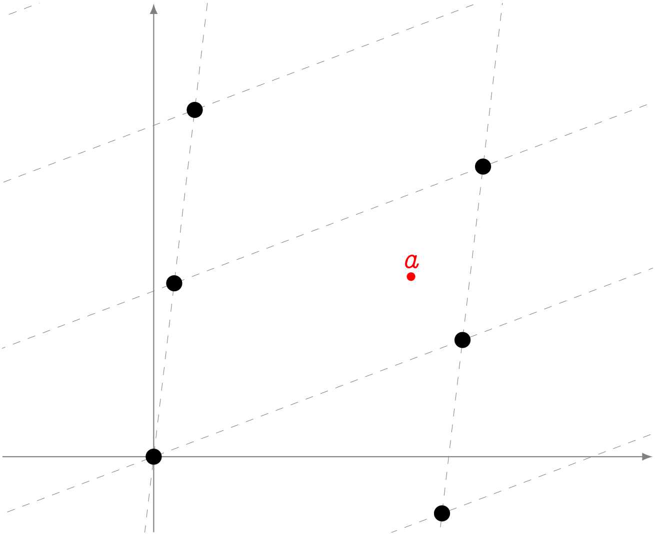
The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

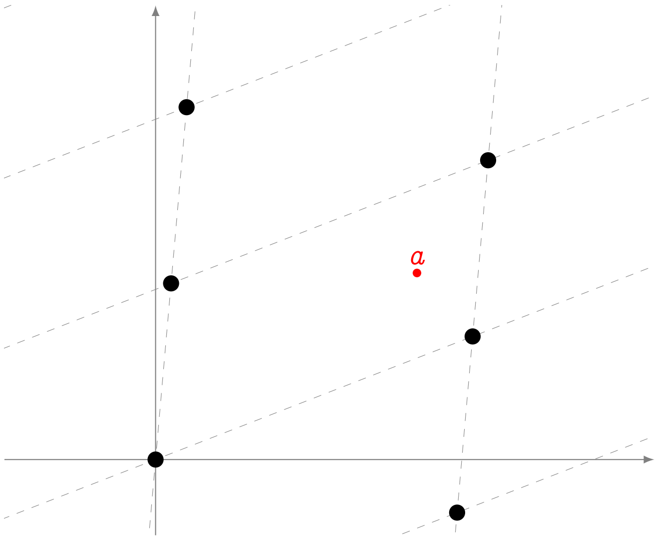


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

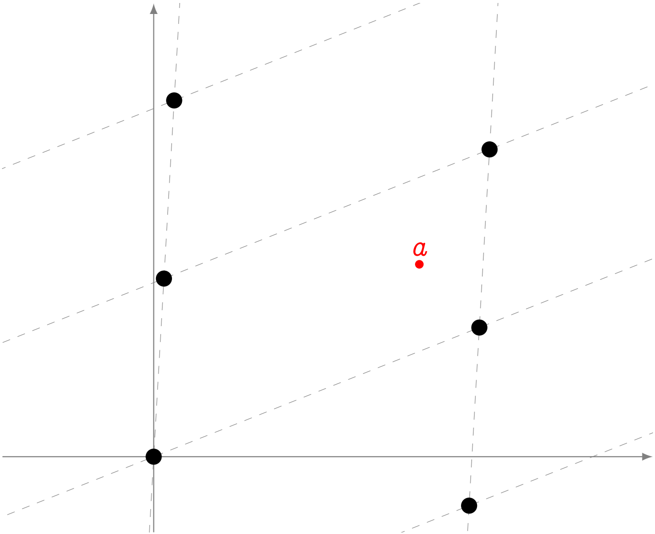


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

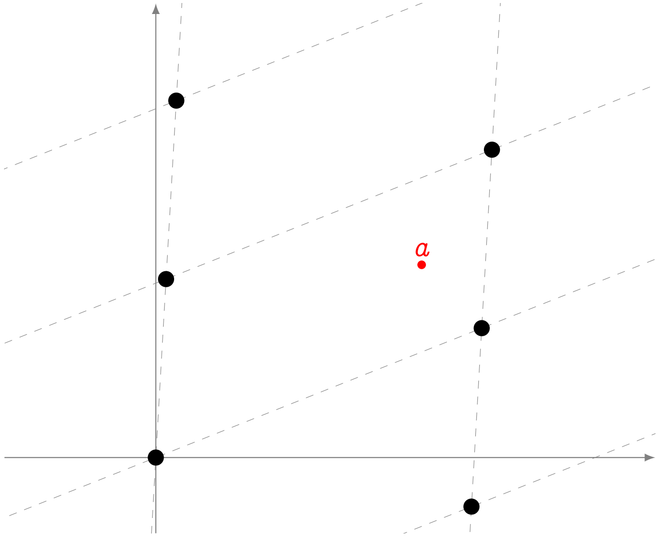


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

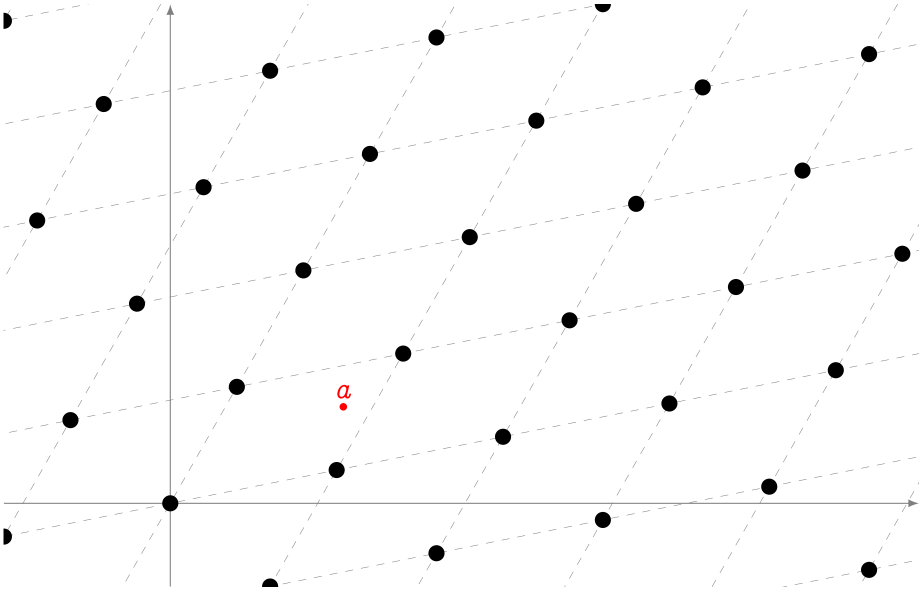


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

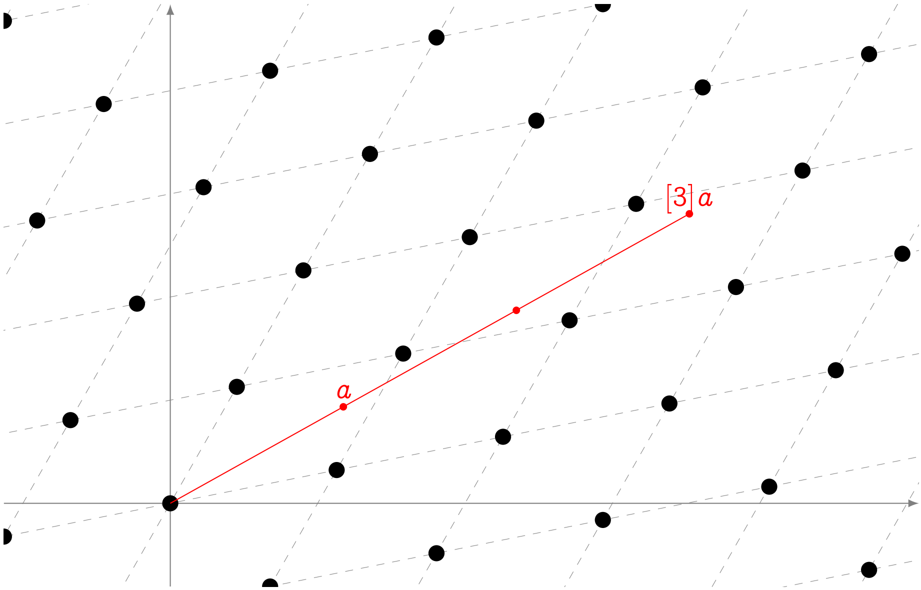
$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

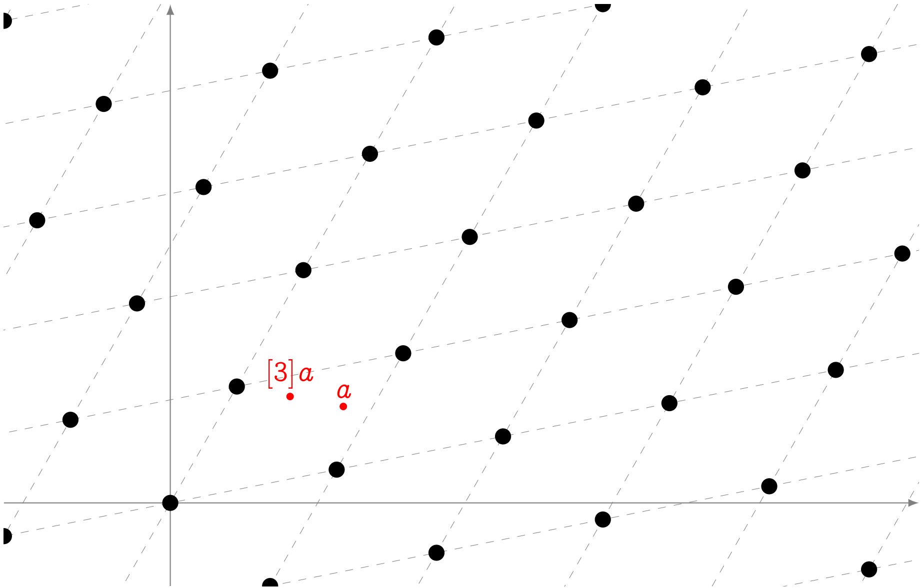
Multiplication



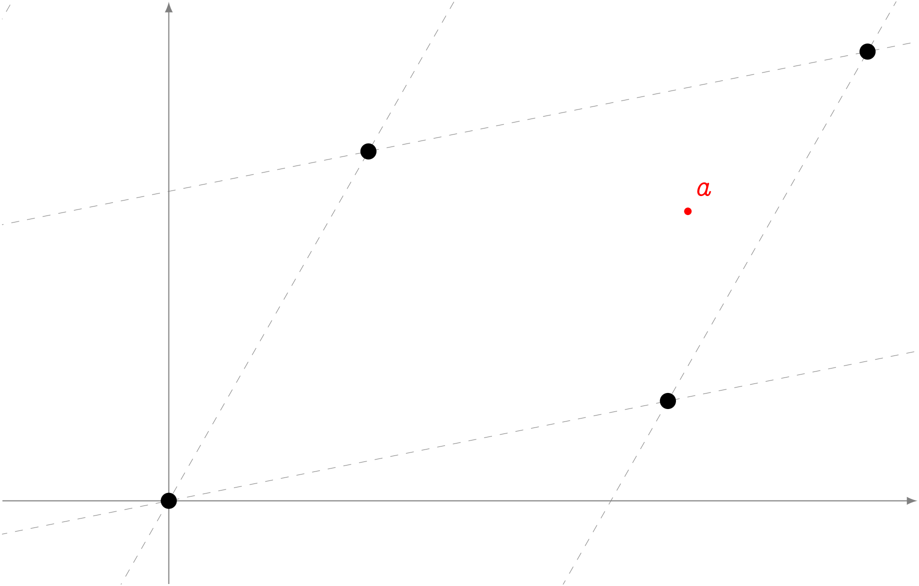
MULTIPLICATION



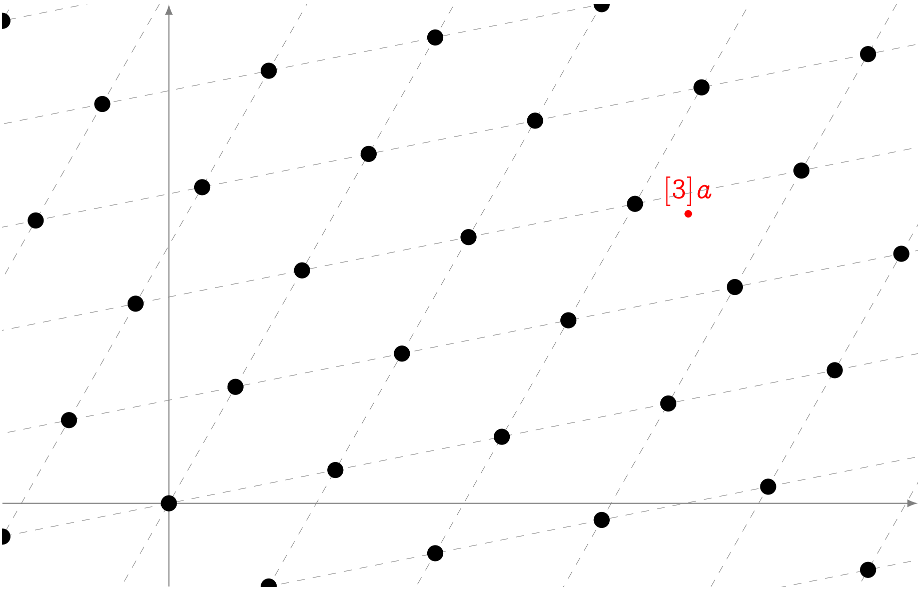
Multiplication



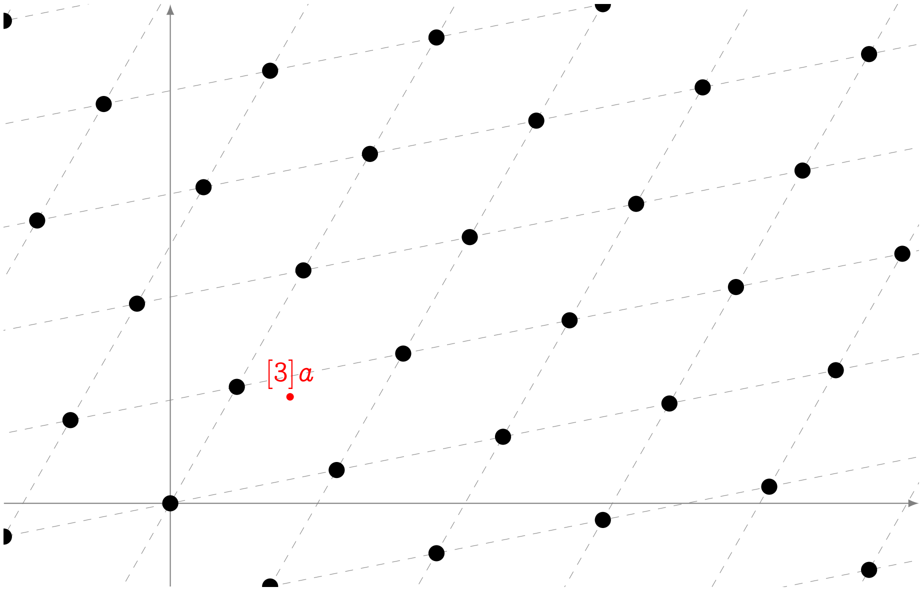
Multiplication + homothety



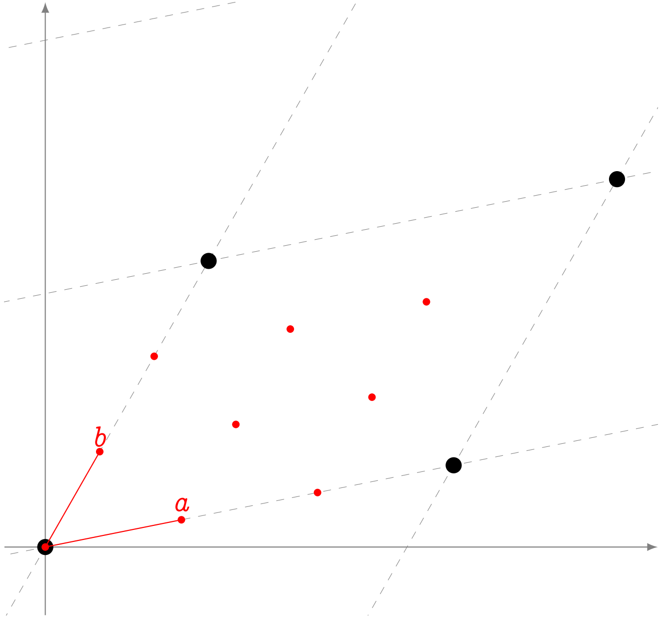
Multiplication + homothety



Multiplication + homothety



Torsion subgroups

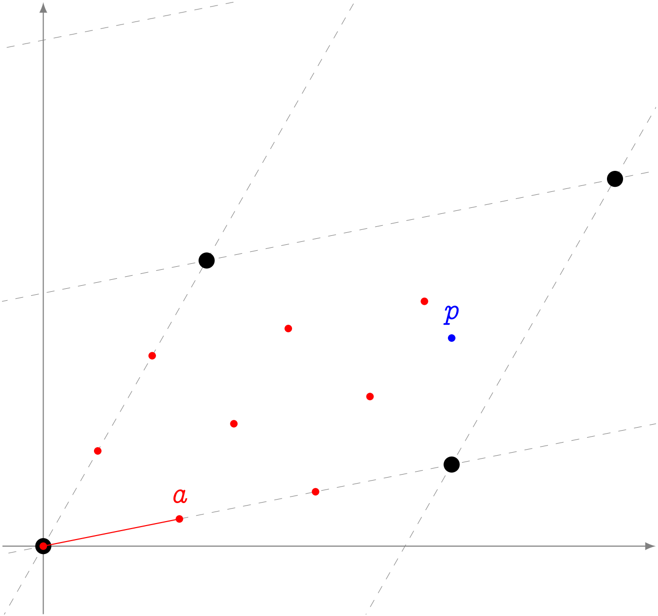


The ℓ-torsion subgroup is made up by the points

$$\left(\frac{i\omega_1}{\ell}, \frac{j\omega_2}{\ell}\right)$$

It is a group of rank two

$$E[\ell] = \langle a, b \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$



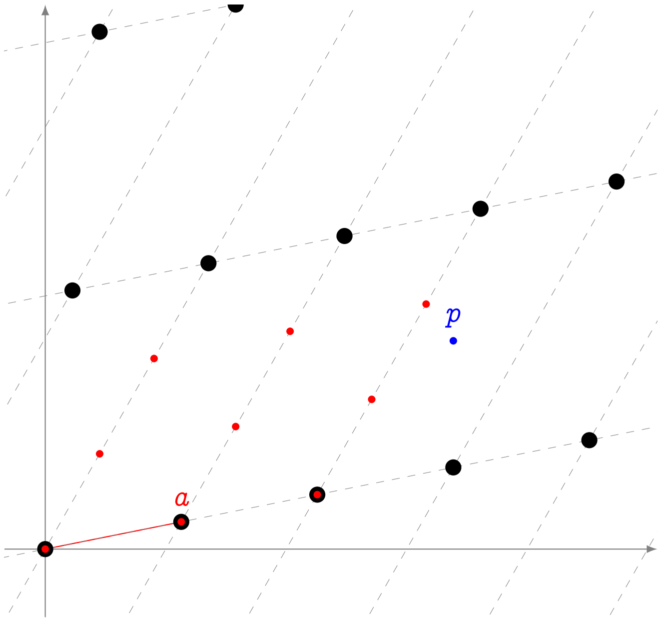
Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

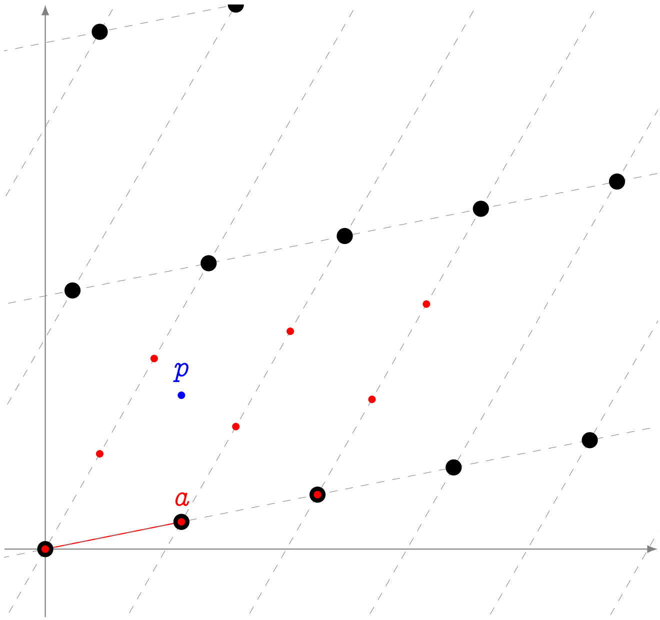
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES



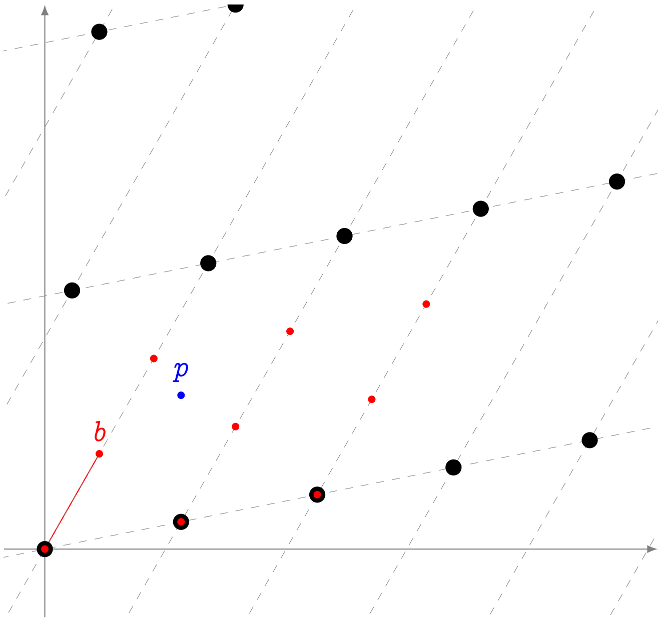
Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

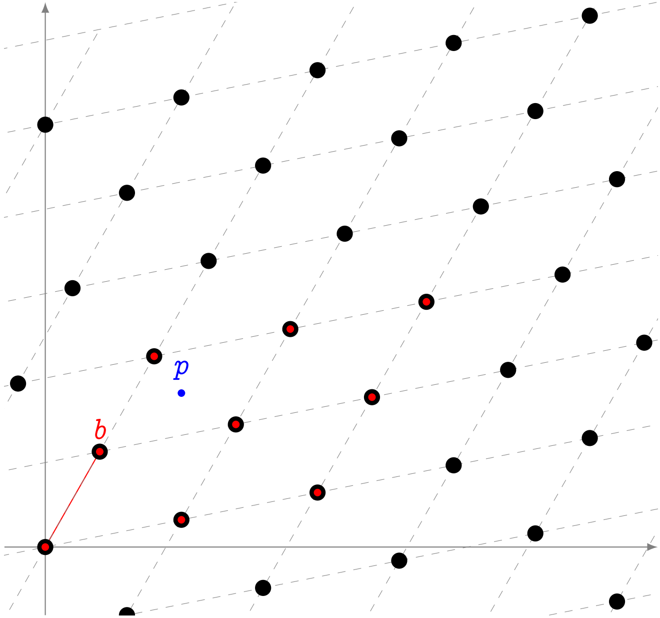


Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.
$\hat{\phi}$ is called the dual isogeny of ϕ.

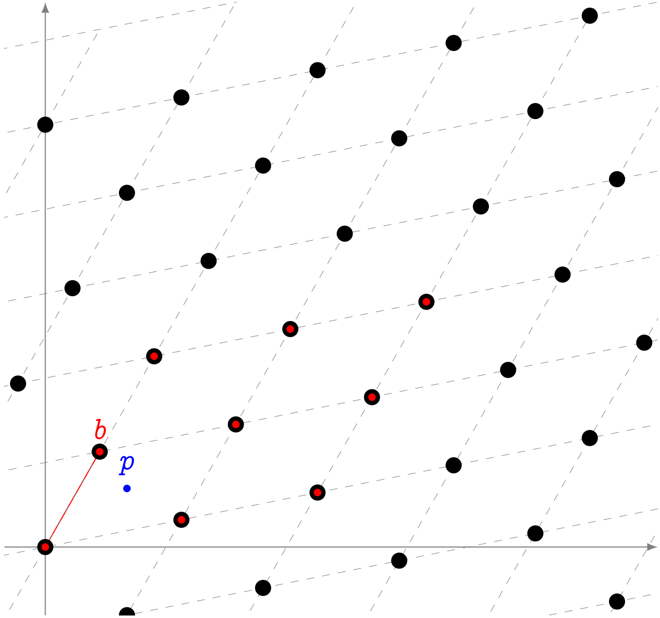
Isogenies



Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map. $\hat{\phi}$ is called the dual isogeny of ϕ.



Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.

$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies over arbitrary fields

Isogenies are just the right notion of morphism for elliptic curves

- Surjective group morphisms.
- Algebraic maps (i.e., defined by polynomials).

$$0 \to H \to E \xrightarrow{\phi} E' \to 0$$

The kernel H determines the image curve E' up to isomorphism

$$E/H \stackrel{\text{def}}{=} E'.$$

Isogeny degree

Neither of these definitions is quite correct, but they *nearly* are:

- The degree of ϕ is the cardinality of $\ker \phi$.
- (Bisson) the degree of ϕ is the time needed to compute it.

Natural questions one may ask about isogenies are

- How do isogenies act on the j-invariants?
- Does a dual isogeny always exist?

Furthermore, in non-algebraically closed fields, one is concerned with rationality

- When is the kernel of the isogeny rational?
- When is the algebraic map rational?
- When are two curves isomorphic? When are they isogenous?

The computational point of view

In practice: an isogeny ϕ is just a rational fraction (or maybe two)

$$\frac{N(x)}{D(x)} = \frac{x^n + \cdots + n_1 x + n_0}{x^{n-1} + \cdots + d_1 x + d_0} \in k(x), \qquad \text{with } n = \deg \phi,$$

and $D(x)$ vanishes on $\ker \phi$.

The explicit isogeny problem

INPUT: A *description* of the isogeny (e.g, its kernel).

OUTPUT: The curve E/H and the rational fraction N/D.

LOWER BOUND: $\Omega(n)$.

The isogeny evaluation problem

INPUT: A *description* of the isogeny ϕ, a point $P \in E(k)$.

OUTPUT: The curve E/H and $\phi(P)$.

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

$$\phi : E \to E'$$

If ϕ is efficiently computable, the discrete log has the same difficulty on E and E'.

EXAMPLE: EXTENDING THE GHS ATTACK

- The GHS attack[a] reduces the discrete log of $E/\mathbb{F}_{2^{n\ell}}$ to the discrete log of a hyperelliptic Jacobian $J/\mathbb{F}_{2^n}$.
- If J has low dimension, this reduction may yield a practical attack.
- Not all curves in the same isogeny class reduce to Jacobians of the same dimension.
- Using isogeny walks more curves can be attacked[b].

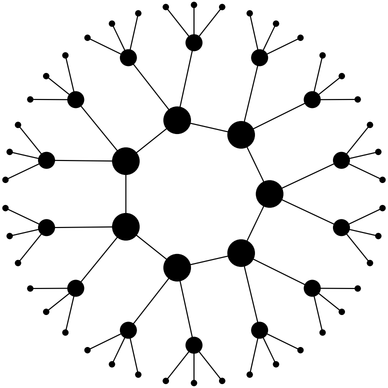
[a] Gaudry, Hess, and Smart 2002.
[b] Galbraith, Hess, and Smart 2002.

Isogeny graphs

We want to study the graph of elliptic curves with isogenies up to isomorphism. We say two isogenies ϕ, ϕ' are isomorphic if:

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[dr, "\phi'"'] & E' \arrow[d, leftrightarrow, "\wr"] \\ & E' \end{tikzcd}$$

Example: Finite field, ordinary case, graph of isogenies of degree 3.



Structure of the graph[1]

Theorem (Serre-Tate)

Two curves are isogenous over a finite field k if and only if they have the same number of points on k.

The graph of isogenies of prime degree $\ell \neq p$

Ordinary case

- Nodes can have degree $0, 1, 2$ or $\ell + 1$.
- Connected components form so called volcanoes.

Supersingular case

- The graph is $\ell + 1$-regular.
- There is an unique connected component made of all supersingular curves with the same number of points.

[1] Kohel 1996; Fouquet and Morain 2002.

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

$$\begin{tikzcd} E \arrow[r, bend left, "\phi'"] \arrow[r, bend right, "\phi"'] & E' \end{tikzcd}$$

In some cases we want to identify edges between the same vertices. We say two isogenies ϕ, ϕ' are in the same class if there exist endomorphisms a and b of E and E' such that:

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "a"'] & E' \arrow[d, "b"] \\ E \arrow[r, "\phi'"'] & E' \end{tikzcd}$$

Facts

- This is an equivalence relation.
- Two isogenies are in the same class if and only if they have the same domain and codomain.

The dual isogeny theorem

Theorem: for any isogeny $\phi : E \to E'$ there exists $\hat{\phi}$

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "{[m]}"'] & E' \arrow[dl, "\hat{\phi}"] \\ E & \end{tikzcd}$$

- $\hat{\phi}$ is called the dual isogeny, $\deg \phi = \deg \hat{\phi} = m$.
- $\hat{\hat{\phi}} = \phi$.

Obvious corollaries:

- $\phi(E[m]) = \ker \hat{\phi}$ (dual isogenies are "easy" to compute).
- Graphs of isogenies are undirected (more or less).

Expander graphs

Let G be a finite undirected k-regular graph.

- k is the trivial eigenvalue of the adjacency matrix of G.
- G is called an expander if all non-trivial eigenvalues satisfy $|\lambda| \le (1-\delta)k$.
- It is called a Ramanunjan graph if $|\lambda| \le 2\sqrt{k-1}$. This is optimal.

In practice, in an expander graph random walks of length $O(\frac{1}{\delta}\log|G|)$ land anywhere in the graph with probability distribution close to uniform.

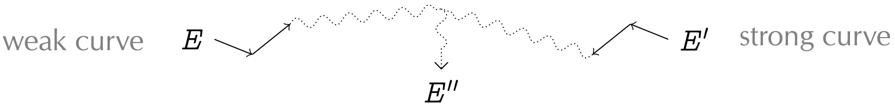
Isogeny graphs and expansion

- The graph of ordinary isogenies of degree less than $(\log 4q)^B$ is an expander if $B > 2$.[a]
- The graph of supersingular isogenies of prime degree $\ell \neq p$ is Ramanujan.[b]

[a] Jao, Miller, and Venkatesan 2009.
[b] Pizer 1990, 1998.

Isogeny walks and cryptanalysis[2]

Recall: Vulnerability to GHS attack is not isogeny invariant.



Fourth root attacks

- Start two random walks from the two curves and wait for a collision.
- Over $\mathbb{F}_q$, the average size of an isogeny class is $h_\Delta \sim \sqrt{q}$.
- A collision is expected after $O(\sqrt{h_\Delta}) = O(q^{\frac{1}{4}})$ steps.

[2] Galbraith, Hess, and Smart 2002; Galbraith 1999; Bisson and Sutherland 2011; Charles, Lauter, and Goren 2009.

Random walks and key escrow[3]

weak curve $E_s \xrightarrow{3} \cdot \xrightarrow{5} \cdot \dashrightarrow E_{pb}$ strong curve

Over $\mathbb{F}_{2^{161}}$ there are $\sim 2^{94}$ isomorphism classes of ordinary curves vulnerable to GHS. Assumption: these are uniformly distributed among isogeny classes.

1. Create E_s vulnerable to GHS, give it to the escrow authority.
2. Take a random walk, land on a curve E_{pb} immune to GHS. Use it for ordinary crypto.

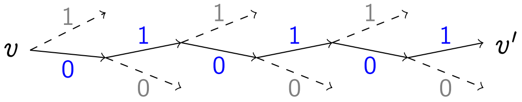
If the isogeny class of E_s has size h:

- Escrow authority looks for an isogeny $E_{pb} \to E_s$. $O(\sqrt{h})$
- Attacker looks for an isogeny to any weak curve. $O(\min(h, 2^{161}/h))$

[3] Teske 2006.

Random walks and hash functions

Any expander graph gives rise to a hash function.



$$H(010101) = v'$$

- Fix a starting vertex v;
- The value to be hashed determines a random path to v';
- v' is the hash.

Provably secure hash functions

- Use the Ramanujan graph of supersingular 2-isogenies;[a]
- Collision resistance = hardness of finding cycles in the graph;
- Preimage resistance = hardness of finding a path from v to v'.

[a] Charles, Lauter, and Goren 2009.

The endomorphism ring

- An endomorphism is an isogeny $\phi : E \to E$.
- The endomorphisms form a ring denoted $\mathrm{End}_k(E)$.

Theorem

$\mathbb{Q} \otimes \mathrm{End}_{\bar{k}}(E)$ is isomorphic to one of the following

ORDINARY CASE: $\mathbb{Q}$ *(only possible if* $\mathrm{char}\, k = 0$*),*

ORDINARY CASE (COMPLEX MULTIPLICATION): *an imaginary quadratic field,*

SUPERSINGULAR CASE: *a quaternion algebra (only possible if* $\mathrm{char}\, k \neq 0$*).*

Corollary

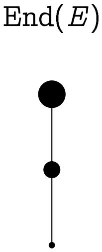
$\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O} \subset \mathbb{Q} \otimes \mathrm{End}(E)$.

THEOREM (SERRE-TATE)

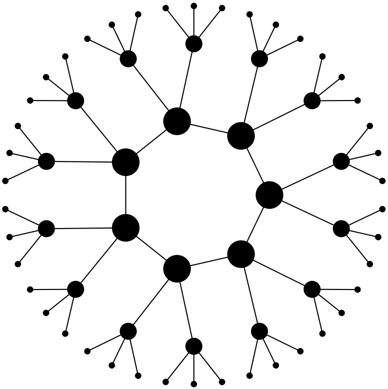
Two elliptic curves E, E' are isogenous if and only if

$$\mathbb{Q} \otimes \mathrm{End}(E) \simeq \mathbb{Q} \otimes \mathrm{End}(E').$$

Example: Finite field, ordinary case, 3-isogeny graph.



bigger node $=$ bigger $\mathrm{End}(E)$



Let $\mathrm{End}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{d})$ be the endomorphism ring of E. Define

- $\mathcal{I}(\mathcal{O})$, the group of invertible fractional ideals,
- $\mathcal{P}(\mathcal{O})$, the group of principal ideals,

Definition (The class group)

The class group of $\mathcal{O}$ is

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

- It is a finite abelian group.
- It arises as the Galois group of an abelian extension of $\mathbb{Q}(\sqrt{d})$.

Isogeny (classes) = ideal (classes)

Definition

Let

- $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$;
- $E[\mathfrak{a}]$ be the the subgroup of $E(\bar{k})$ annihilated by $\mathfrak{a}$;
- $\phi : E \to E/E[\mathfrak{a}]$.

Then $\deg \phi = \mathcal{N}(\mathfrak{a})$. We denote by $*$ the action on the set of elliptic curves.

$$\mathfrak{a} * j(E) = j(E/E[\mathfrak{a}]).$$

Theorem

The action $*$ factors through $\mathrm{Cl}(\mathcal{O})$. It is faithful and transitive.

Example: principal ideals

Let $\mathfrak{a} = m\mathcal{O}$, the ideal corresponding to multiplication by m. Then

- $\deg \phi = \mathcal{N}(m\mathcal{O}) = m^2$,
- $E[\mathfrak{a}] = E[m]$,
- $m\mathcal{O} \in \mathcal{P}(\mathcal{O})$,
- $m\mathcal{O} \equiv 1 \in \mathrm{Cl}(\mathcal{O})$.
- $\mathfrak{a} * j(E) = j(E)$.

Example: the dual isogeny

Let ϕ be an isogeny and $\hat{\phi}$ its dual. Let $\mathfrak{a}$ and $\hat{\mathfrak{a}}$ their associated ideals. Then

- $\hat{\mathfrak{a}}\mathfrak{a} = \mathfrak{a}\hat{\mathfrak{a}} = m\mathcal{O} \in \mathcal{P}(\mathcal{O})$,
- $\deg \phi = \mathcal{N}(\mathfrak{a}) = \mathcal{N}(\hat{\mathfrak{a}}) = \deg \hat{\phi}$,
- $\hat{\mathfrak{a}} \equiv \mathfrak{a}^{-1} \in \mathrm{Cl}(\mathcal{O})$.

DH-like key exchange based on (semi)-group actions

Let G be an abelian group acting (faithfully and transitively) on a set X.

$$
\begin{tikzcd}
 & x_0 \arrow[dl, "g"'] \arrow[dr, "h"] & \\
g \cdot x_0 \arrow[dr, "h"'] & & h \cdot x_0 \arrow[dl, "g"] \\
 & gh \cdot x_0 = hg \cdot x_0 &
\end{tikzcd}
$$

Université de Versailles St-Quentin-en-Yvelines

Let G be a group, X a set and $f : G \to X$. We say that f hides a subgroup $H \subset G$ if

$$f(g_1) = f(g_2) \Leftrightarrow g_1 H = g_2 H.$$

Definition (Hidden Subgroup Problem (HSP))

INPUT: G, X as above, an oracle computing f.

OUTPUT: generators of H.

Theorem (Schorr, Josza)

If G is abelian, then

- $HSP \in poly_{BQP}(\log|G|)$,
- *using* $poly(\log|G|)$ *queries to the oracle.*

Post-Quantum cryptography

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Known reductions

- Discrete Log on G of size p $\rightarrow$ HSP on $(\mathbb{Z}/p\mathbb{Z})^2$,
- hence DH, ECDH, etc. are broken by quantum computers.
- Semigroup-DH on G $\rightarrow$ HSP on the dihedral group $G \ltimes \mathbb{Z}/2\mathbb{Z}$.

Quantum algorithms for dihedral HSP

Kuperberg[a]: $2^{O(\sqrt{\log|G|})}$ quantum time, space and query complexity.

Regev[b]: $L_{|G|}(\frac{1}{2}, \sqrt{2})$ quantum time and query complexity, poly$(\log(|G|)$) quantum space.

[a] Kuperberg 2005.

[b] Regev 2004.

Remark (Regev): certain lattice-based cryptosystems are also vulnerable to the HSP for dihedral groups.

Public data:

- $E/\mathbb{F}_p$ ordinary elliptic curve with complex multiplication field $\mathbb{K}$,
- primes ℓ_1,ℓ_2 not dividing $\mathrm{Disc}(E)$ and s.t. $\left(\frac{D_{\mathbb{K}}}{\ell_i}\right) = 1$.
- A *direction* on the isogeny graph (a Frobenius eigenvalue).

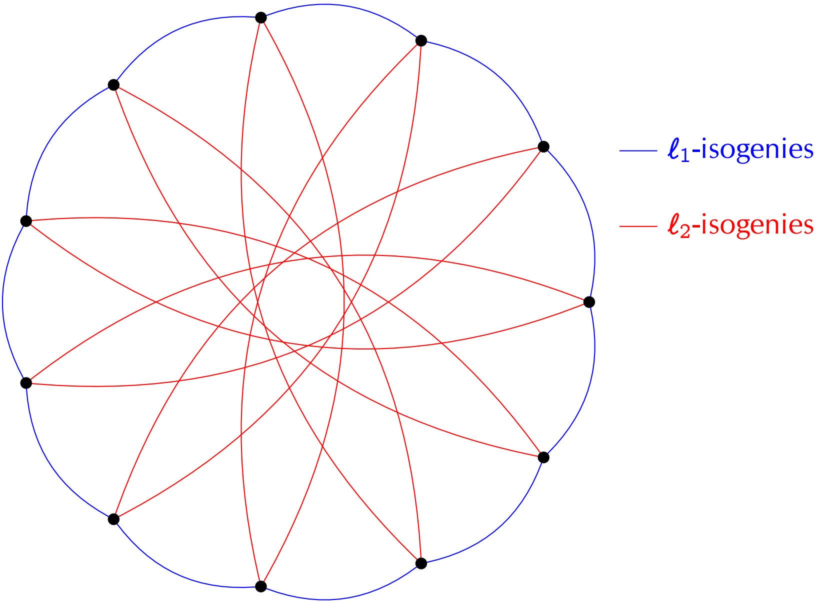
Secret data: Random walks $\mathfrak{a}$, $\mathfrak{b}$ in the ℓ_i-isogeny graphs.

$$
\begin{tikzcd}
 & E \arrow[dl, "\ell_1^{a_1}\ell_2^{a_2} = \mathcal{N}(\mathfrak{a})"'] \arrow[dr, "\mathcal{N}(\mathfrak{b}) = \ell_1^{b_1}\ell_2^{b_2}"] & \\
\mathfrak{a} * E \arrow[dr] & & \mathfrak{b} * E \arrow[dl] \\
 & \mathfrak{ab} * E = \mathfrak{ba} * E &
\end{tikzcd}
$$

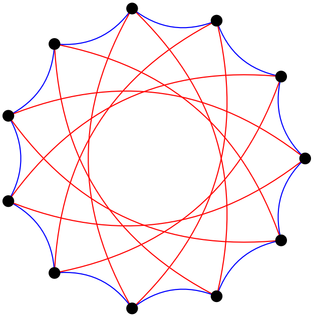
---

[4] Rostovtsev and Stolbunov 2006.

R&S KEY EXCHANGE



R&S KEY EXCHANGE



KEY GENERATION: compose small degree isogenies
polynomial in the lenght of the random walk.

ATTACK: find an isogeny between two curves
polynomial in the degree, exponential in the length.

QUANTUM[5]: HShP + isogeny evaluation
subexponential in the length of the walk.

[5] Childs, Jao, and Soukharev 2010.

$\mathbb{Q} \otimes \mathrm{End}(E)$ is a quaternion algebra (non-commutative)

Facts

- Every supersingular curve is defined over $\mathbb{F}_{p^2}$.
- $E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$ (up to twist, and overly simplifying!).
- There are $g(X_0(p)) + 1 \sim \frac{p+1}{12}$ supersingular curves up to isomorphism.
- For every maximal order type of the quaternion algebra $\mathbb{Q}_{p,\infty}$ there are 1 or 2 curves over $\mathbb{F}_{p^2}$ having endomorphism ring isomorphic to it.
- There is a unique isogeny class of supersingular curves over $\bar{\mathbb{F}}_p$ (there are two over any finite field).
- The graph of ℓ-isogenies is $\ell + 1$-regular.

R&S KEY EXCHANGE WITH SUPERSINGULAR CURVES

GOOD NEWS: there is no action of a commutative class group.
BAD NEWS: there is no action of a commutative class group.

However: left ideals of $\mathrm{End}(E)$ still act on the isogeny graph:

$$\begin{tikzcd} E \arrow[r, "\mathfrak{a}"] \arrow[d, "\mathfrak{b}"'] & E' \arrow[d, "\mathfrak{b}_{\mathfrak{a}}"] \\ E'' \arrow[r, "\mathfrak{a}_{\mathfrak{b}}"'] & E''' \end{tikzcd}$$

- The action factors through the right-isomorphism equivalence of ideals.
- Ideal classes form a groupoid (in other words, an undirected multigraph...).

From ideals back to isogenies

In practice, computations with ideals are hard. We fix, instead:

- Small primes ℓ_A, ℓ_B;
- A large prime p such that $p+1 = \ell_A^{e_A}\ell_B^{e_B}$;
- A supersingular curve E over $\mathbb{F}_{p^2}$, such that

$$E \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2 = (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^2,$$

- We use isogenies of degrees $\ell_A^{e_A}$ and $\ell_B^{e_B}$ with cyclic rational kernels;
- The diagram below can be constructed in time poly$(e_A + e_B)$.

$$\ker\phi = \langle P\rangle \subset E[\ell_A^{e_A}]$$

$$\ker\psi = \langle Q\rangle \subset E[\ell_B^{e_B}]$$

$$\ker\phi' = \langle \psi(P)\rangle$$

$$\ker\psi' = \langle \phi(Q)\rangle$$

$$\begin{tikzcd}
E \arrow[r, "\phi"] \arrow[d, "\psi"'] & E/\langle P\rangle \arrow[d, "\psi'"] \\
E/\langle Q\rangle \arrow[r, "\phi'"'] & E/\langle P, Q\rangle
\end{tikzcd}$$

A ZK proof of knowledge

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from E to $E/\langle S\rangle$.

$$E \overset{\phi}{\longrightarrow} E/\langle S\rangle$$

A ZK PROOF OF KNOWLEDGE

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from E to $E/\langle S\rangle$.

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "?"'] & E/\langle S\rangle \arrow[d, dash, "?"] \\
E/\langle P\rangle \arrow[r, dash, "?"'] & E/\langle P, S\rangle
\end{tikzcd}$$

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;

A ZK proof of knowledge

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from E to $E/\langle S\rangle$.

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle S\rangle \arrow[d, dash, "\psi'"] \\
E/\langle P\rangle \arrow[r, dash, "?"'] & E/\langle P, S\rangle
\end{tikzcd}$$

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier asks one of the two questions:
   - Reveal the degree $\ell_B^{e_B}$ isogenies;

A ZK PROOF OF KNOWLEDGE

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from E to $E/\langle S\rangle$.

$$
\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "?"'] & E/\langle S\rangle \arrow[d, dash, "?"] \\
E/\langle P\rangle \arrow[r, dash, "\phi'"'] & E/\langle P, S\rangle
\end{tikzcd}
$$

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier asks one of the two questions:
   - Reveal the degree $\ell_B^{e_B}$ isogenies;
   - Reveal the bottom isogeny.

SECURITY

$$
\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "?"'] & E/\langle S \rangle \arrow[d, dash, "?"] \\
E/\langle P \rangle \arrow[r, dash, "\phi'"'] & E/\langle P, S \rangle
\end{tikzcd}
$$

What information does ϕ' give on ϕ?

- We prove that the protocol is zero-knowledge if distinguishing a pair (ϕ, ϕ') from a random pair (ϕ, χ) is hard.
- We conjecture this problem is hard, even using ideal classes.
- Remark: this problem is trivial (at most subexponential) in the ordinary case.

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

$$\begin{tikzcd} E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle S\rangle \arrow[d, dash, "\psi'"] \\ E/\langle P\rangle \arrow[r, dash, "?"'] & E/\langle P, S\rangle \end{tikzcd}$$

What information do ψ and ψ' give on ϕ?

- On the first round, we learn $(P, \phi(P))$,

Security

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle S\rangle \arrow[d, dash, "\psi'"] \\
E/\langle Q\rangle \arrow[r, dash, "?"'] & E/\langle Q, S\rangle
\end{tikzcd}$$

What information do ψ and ψ' give on ϕ?

- On the first round, we learn $(P, \phi(P))$,
- On the second round, we learn $(Q, \phi(Q))$,
- …

SECURITY

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle S\rangle \arrow[d, dash, "\psi'"] \\
E/\langle Q\rangle \arrow[r, dash, "?"'] & E/\langle Q, S\rangle
\end{tikzcd}$$

What information do ψ and ψ' give on ϕ?

- On the first round, we learn $(P, \phi(P))$,
- On the second round, we learn $(Q, \phi(Q))$,
- $\ldots$
- With high probabilty, $\langle P, Q\rangle = E[\ell_B^{e_B}]$, and we learn $\phi(E[\ell_B^{e_B}])$.
- We make $\phi(E[\ell_B^{e_B}])$ part of the public data, and we conjecture that this is secure.

Going Diffie-Hellman

The idea: Alice chooses ϕ, Bob chooses ψ.

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle P\rangle \arrow[d, dash, "\psi'"] \\
E/\langle Q\rangle \arrow[r, dash, "\phi'"'] & E/\langle P, Q\rangle
\end{tikzcd}$$

Problem:

- How does Alice know the kernel of ϕ'?
- How does Bob know the kernel of ψ'?

Going Diffie-Hellman

The idea: Alice chooses ϕ, Bob chooses ψ.

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "\psi"'] & E/\langle P\rangle \arrow[d, dash, "\psi'"] \\
E/\langle Q\rangle \arrow[r, dash, "\phi'"'] & E/\langle P, Q\rangle
\end{tikzcd}$$

Problem:

- How does Alice know the kernel of ϕ'?
- How does Bob know the kernel of ψ'?

Our solution:

- It is not so dangerous to publish $\phi(E[\ell_B^{e_B}])$.
- It is not so dangerous to publish $\psi(E[\ell_A^{e_A}])$.

OUR PROPOSAL[6]

Public data:

- Prime p such that $p+1 = \ell_A^a \ell_B^b$;
- Supersingular curve $E \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$;
- $E[\ell_A^a] = \langle P_A, Q_A \rangle$;
- $E[\ell_B^b] = \langle P_B, Q_B \rangle$.

Secret data:

- $R_A = m_A P_A + n_A Q_A$,
- $R_B = m_B P_B + n_B Q_B$,

$$
\begin{tikzcd}
 & E \arrow[dl, "\phi"'] \arrow[dr, "\psi"] & \\
E/\langle R_A \rangle \arrow[dr, "\psi'"'] & & E/\langle R_B \rangle \arrow[dl, "\phi'"] \\
\frac{E/\langle R_A \rangle}{\phi(R_B)} \simeq & E/\langle R_A, R_B \rangle & \simeq \frac{E/\langle R_B \rangle}{\psi(R_A)}
\end{tikzcd}
$$

[6] Jao and De Feo 2011.

Our proposal[6]

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Public data:

- Prime p such that $p+1=\ell_A^a\ell_B^b$;
- Supersingular curve $E\simeq(\mathbb{Z}/(p+1)\mathbb{Z})^2$;
- $E[\ell_A^a]=\langle P_A,Q_A\rangle$;
- $E[\ell_B^b]=\langle P_B,Q_B\rangle$.

Secret data:

- $R_A=m_AP_A+n_AQ_A$,
- $R_B=m_BP_B+n_BQ_B$,

$$
\begin{tikzcd}
 & & E \arrow[dl, "\phi"'] \arrow[dr, "\psi"] & & \\
 & \begin{array}{c} E/\langle R_A\rangle \\ \phi(P_B) \\ \phi(Q_B) \end{array} \arrow[dr, "\psi'"'] & & \begin{array}{c} E/\langle R_B\rangle \\ \psi(P_A) \\ \psi(Q_A) \end{array} \arrow[dl, "\phi'"] & \\
\frac{E/\langle R_A\rangle}{\phi(R_B)} \simeq & & E/\langle R_A,R_B\rangle & & \simeq \frac{E/\langle R_B\rangle}{\psi(R_A)}
\end{tikzcd}
$$

[6] Jao and De Feo 2011.

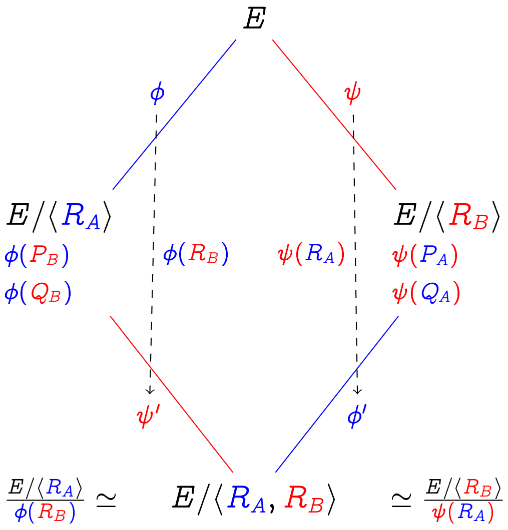
Our proposal[6]

Public data:

- Prime p such that $p + 1 = \ell_A^a \ell_B^b$;
- Supersingular curve $E \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$;
- $E[\ell_A^a] = \langle P_A, Q_A \rangle$;
- $E[\ell_B^b] = \langle P_B, Q_B \rangle$.

Secret data:

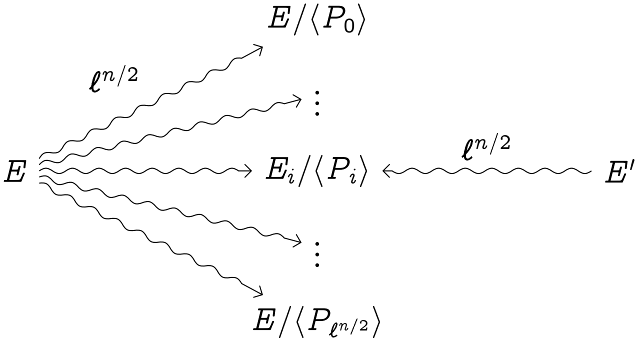
- $R_A = m_A P_A + n_A Q_A$,
- $R_B = m_B P_B + n_B Q_B$,



[6] Jao and De Feo 2011.

Generic attacks

Problem: Given E, E', isogenous of degree ℓ^n, find $\phi : E \to E'$.



- With high probability ϕ is the unique collision (or *claw*).
- A quantum claw finding[7] algorithm solves the problem in $O(\ell^{n/3})$.

[7] Tani 2008.

Our recommended parameters

- For efficiency chose p such that $p+1 = 2^a 3^b$.
- For classical n-bit security, choose $2^a \sim 3^b \sim 2^{2n}$, hence $p \sim 2^{4n}$.
- For quantum n-bit security, choose $2^a \sim 3^b \sim 2^{3n}$, hence $p \sim 2^{6n}$.

Practical optimizations:

- -1 is a quadratic non-residue: $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X]/(X^2+1)$.
- E (or its twist) has a 4-torsion point: it has an Edwards and a Montgomery form.
- A quasi-linear strategy to evaluate composite degree isogenies[a].
- Our implementation performs a 128 classical bits security key exchange in about 50ms on a standard processor.

[a] De Feo, Jao, and Plût 2011.

CONCLUSIONS

- Isogeny graphs are a lot of fun.
- They have many interesting applications inside and outside of cryptography.
- There are tons of shaky security assumptions that need to be checked.

Come and get some!

References I

Kohel, David (1996).
"Endomorphism rings of elliptic curves over finite fields".
PhD thesis. University of California at Berkley.

Gaudry, Pierrick, Florian Hess, and Niegel Smart (Mar. 2002).
"Constructive and destructive facets of Weil descent on elliptic curves".
In: Journal of Cryptology 15.1,
Pp. 19–46–46.

Galbraith, Steven D., Florian Hess, and Nigel P. Smart (2002).
"Extending the GHS Weil descent attack".
In: Advances in cryptology—EUROCRYPT 2002 (Amsterdam).
Vol. 2332.
Lecture Notes in Comput. Sci.
Berlin: Springer,
Pp. 29–44.

References II

Fouquet, Mireille and FranCcois Morain (2002).
"Isogeny Volcanoes and the SEA Algorithm".
In: Algorithmic Number Theory Symposium.
Ed. by Claus Fieker and David R. Kohel.
Vol. 2369.
Lecture Notes in Computer Science.
Berlin, Heidelberg: Springer Berlin / Heidelberg.
Chap. 23, pp. 47–62.

Jao, David, Stephen D. Miller, and Ramarathnam Venkatesan (June 2009).
"Expander graphs based on GRH with an application to elliptic curve cryptography".
In: Journal of Number Theory 129.6,
Pp. 1491–1504.

References III

Pizer, Arnold K. (1990).
"Ramanujan graphs and Hecke operators".
In: Bull. Amer. Math. Soc. (N.S.) 23.1.

— (1998).
"Ramanujan graphs".
In: Computational perspectives on number theory (Chicago, IL, 1995).
Vol. 7.
AMS/IP Stud. Adv. Math.
Providence, RI: Amer. Math. Soc.

Galbraith, Steven D. (1999).
"Constructing Isogenies between Elliptic Curves Over Finite Fields".
In: LMS Journal of Computation and Mathematics 2,
Pp. 118–138.

References IV

Bisson, Gaetan and Andrew V. Sutherland (June 2011).
"A low-memory algorithm for finding short product representations in finite groups".
In: Designs, Codes and Cryptography 63.1,
Pp. 1–13.

Teske, Edlyn (Jan. 2006).
"An Elliptic Curve Trapdoor System".
In: Journal of Cryptology 19.1,
Pp. 115–133.

Charles, Denis X., Kristin E. Lauter, and Eyal Z. Goren (Jan. 2009).
"Cryptographic Hash Functions from Expander Graphs".
In: Journal of Cryptology 22.1,
Pp. 93–113.

References V

Kuperberg, Greg (2005).
"A subexponential-time quantum algorithm for the dihedral hidden subgroup problem".
In: SIAM J. Comput. 35.1,
Pp. 170–188.
eprint: quant-ph/0302112.

Regev, Oded (June 2004).
A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space.
arXiv:quant-ph/0406151.

Rostovtsev, Alexander and Anton Stolbunov (2006).
Public-key cryptosystem based on isogenies.

References VI

Childs, Andrew M., David Jao, and Vladimir Soukharev (Dec. 2010).
"Constructing elliptic curve isogenies in quantum subexponential time".

Jao, David and Luca De Feo (2011).
"Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies".
In: Post-Quantum Cryptography.
Ed. by Bo-Yin Yang.
Vol. 7071.
Lecture Notes in Computer Science.
Taipei, Taiwan: Springer Berlin / Heidelberg.
Chap. 2, pp. 19–34.

Tani, Seiichiro (Mar. 2008).
"Claw Finding Algorithms Using Quantum Walk".

References VII

De Feo, Luca, David Jao, and Jérôme Plût (Sept. 2011). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.
URL: http://eprint.iacr.org/2011/506.