Isogeny based cryptography
the new frontier of number theoretic cryptography

Luca De Feo

IBM Research Zürich

February 15, 2022
Seminario di Matematica, Università Roma Tor Vergata

Crypto <3 Number Theory

1976 Diffie–Hellman key exchange, discrete logarithm

1977 Rivest, Shamir and Adleman invent RSA, factorization

Crypto <3 Number Theory

1976	Diffie–Hellman key exchange,	discrete logarithm
1977	Rivest, Shamir and Adleman invent RSA,	factorization
1980	Miller and Koblitz introduce elliptic curve cryptography,	(hyper)elliptic curves

Crypto <3 Number Theory

1976	Diffie–Hellman key exchange,	discrete logarithm
1977	Rivest, Shamir and Adleman invent RSA,	factorization
1980	Miller and Koblitz introduce elliptic curve cryptography,	(hyper)elliptic curves
1996	Hoffstein, Pipher and Silverman invent NTRU,	ideal lattices
2001	Joux' tripartite key exchange, Boneh–Franklin IBE,	elliptic pairings
2006	Couveignes–Rostovtsev–Stolbunov key exchange,	complex multiplication
2006	Charles–Goren–Lauter hash function.	quaternionic multiplication

Cryptography

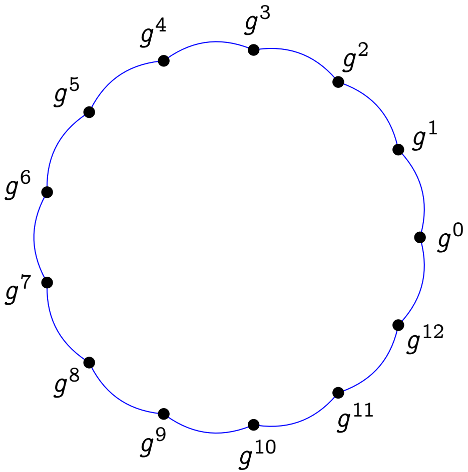
Basic goals

- Symmetric encryption,
- Key exchange,
- Public key encryption,
- Authentication,
- Digital signatures.

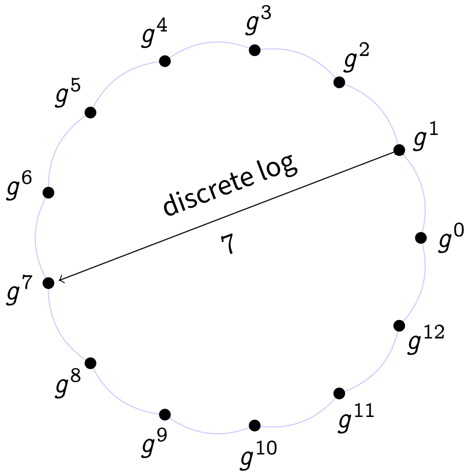
Advanced goals

- Identity/Attribute based encryption,
- Fully homomorphic encryption,
- Zero-knowledge proofs,
- Multi-party computation,
- ...

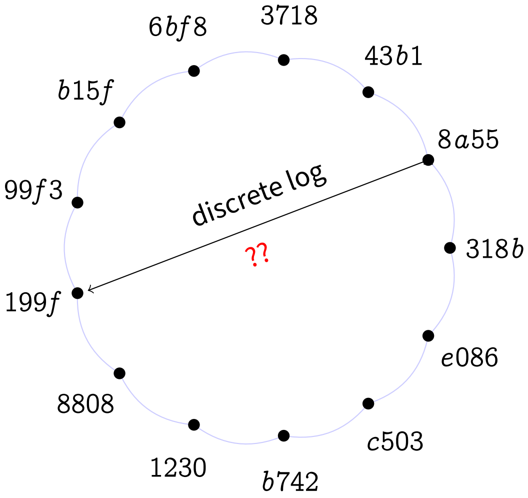
Discrete logarithm



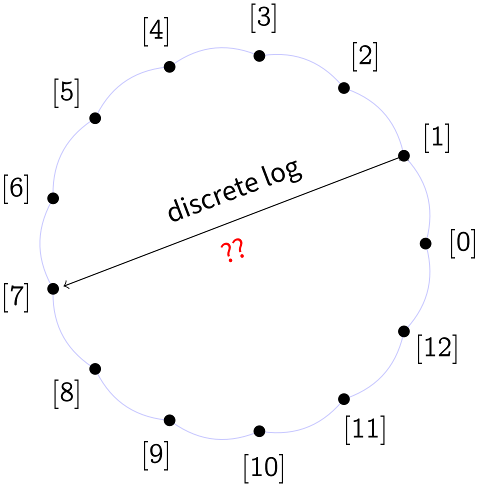
Discrete logarithm



Discrete logarithm



Discrete logarithm



The axioms of a dlog group:

prod: $[a][b] = [a+b]$,

exp: $n[a] = [na]$.

The hard problem:

dlog: $[a] \mapsto a$.

Diffie–Hellman key exchange

Alice **Bob**

pick random $a \in (\mathbb{Z}/N\mathbb{Z})^\times$

pick random $b \in (\mathbb{Z}/N\mathbb{Z})^\times$

$$\xrightarrow{\quad [a] \quad}$$

$$\xleftarrow[\quad [b] \quad]{}$$

Shared secret is $a[b] = [ab] = b[a]$

Why isogenies?

Quantum-safe crypto

- Shortest ciphertexts and public keys for Encryption: SIDH/SIKE
  CSIDH*
- Shortest public key + Signature: SQISign
- Only efficient Non-Interactive Key Exchange: CSIDH*
- Acceptable Threshold Signatures: CSI-FiSh*

*Secure parameter sizes still debated, big impact on performance.

Time-delay crypto (not quantum safe)

- Only efficient alternative to group-based Verifiable Delay Functions Asiacrypt '19
- Only known instantiation of Delay Encryption Eurocrypt '21

Brief history of isogeny-based cryptography

1997 Couveignes introduces the Hard Homogeneous Spaces framework. His work stays unpublished for 10 years.

2006 Rostovtsev & Stolbunov independently rediscover Couveignes ideas, suggest isogeny-based Diffie–Hellman as a quantum-resistant primitive.

2006-2010 Other isogeny-based protocols by Teske and Charles, Goren & Lauter.

2011-2012 D., Jao & Plût introduce SIDH, an efficient post-quantum key exchange inspired by Couveignes, Rostovtsev, Stolbunov, Charles, Goren, Lauter.

2017 SIDH is submitted to the NIST competition (with the name SIKE, only isogeny-based candidate).

2018 Castryck, Lange, Martindale, Panny & Renes create an efficient variant of the Couveignes–Rostovtsev–Stolbunov protocol, named CSIDH.

2019 Isogeny signature craze: SeaSign (D. & Galbraith; Decru, Panny & Vercauteren), CSI-FiSh (Beullens, Kleinjung & Vercauteren), VDF (D., Masson, Petit & Sanso).

2020 Isogeny signatures get interesting: SQISign (D., Kohel, Leroux, Petit, Wesolowski). SIKE is an Alternate candidate finalist in NIST's 3rd round.

Diffie–Hellman key exchange

Alice | **Bob**

pick random $a \in (\mathbb{Z}/N\mathbb{Z})^\times$

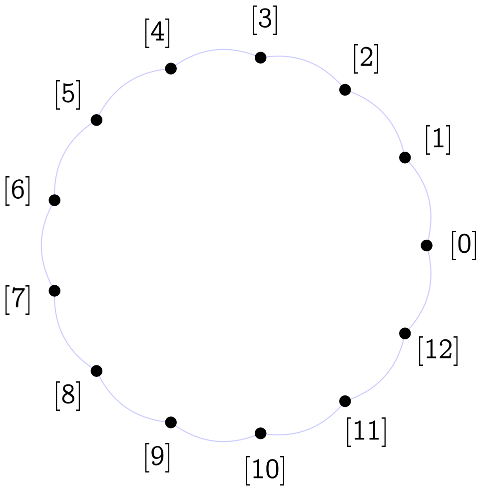
pick random $b \in (\mathbb{Z}/N\mathbb{Z})^\times$

$$\xrightarrow{\quad [a] \quad}$$

$$\xleftarrow[\quad [b] \quad]{}$$

Shared secret is $a[b] = [ab] = b[a]$

What's needed for key exchange?



The axioms of a dlog group:

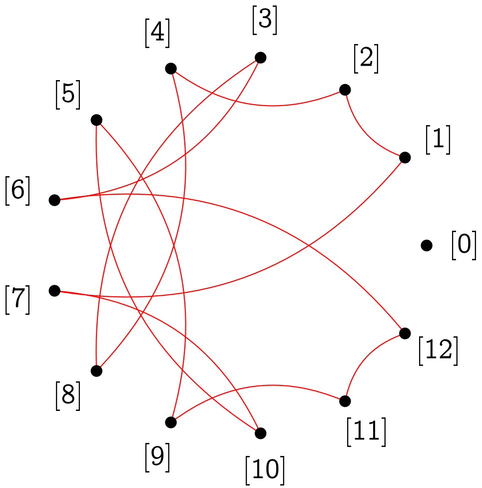
~~prod:~~ $\cancel{[a][b] = [a+b]}$,

exp: $n[a] = [na]$.

The hard problem:

dlog: $[a] \mapsto a$.

What's needed for key exchange?



The axioms of a dlog group:

~~prod:~~ $\cancel{[a][b] = [a+b]}$,

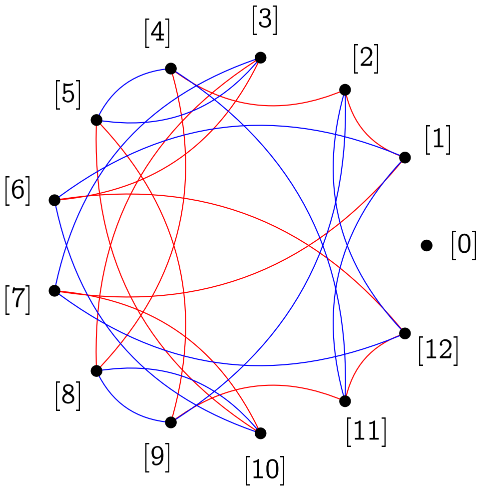
exp: $n[a] = [na]$.

The hard problem:

dlog: $[a] \mapsto a$.

$[a]$ —— $2[a]$

What’s needed for key exchange?



The axioms of a dlog group:

~~prod:~~ $\cancel{[a][b] = [a+b]}$,

exp: $n[a] = [na]$.

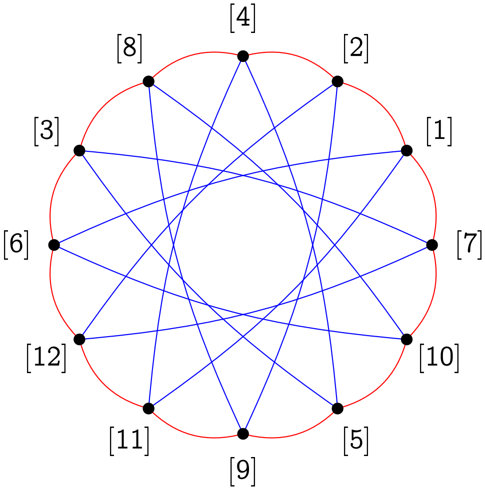
The hard problem:

dlog: $[a] \mapsto a$.

$[a]$ —— $2[a]$

$[a]$ —— $6[a]$

What's needed for key exchange?



The axioms of a dlog group:

~~prod:~~ $\cancel{[a][b] = [a+b]}$,

exp: $n[a] = [na]$.

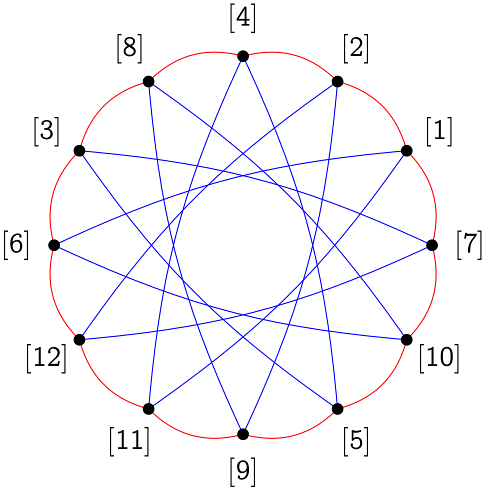
The hard problem:

dlog: $[a] \mapsto a$.

$[a]$ —— $2[a]$

$[a]$ —— $6[a]$

What’s needed for key exchange?



The axioms of a dlog group:

~~prod:~~ $\cancel{[a][b] = [a+b]}$,

exp: $n[a] = [na]$.

The hard problem:

dlog: $[a] \mapsto a$.

$[a]$ ——— $2[a]$

$[a]$ ——— $6[a]$

Automorphism group: $(\mathbb{Z}/13\mathbb{Z})^\times$.

Group action

$\mathcal{G} \circlearrowleft \mathcal{E}$: A (finite) set $\mathcal{E}$ acted upon by a group $\mathcal{G}$ freely and transitively:

$$\begin{aligned} * : \mathcal{G} \times \mathcal{E} &\longrightarrow \mathcal{E} \\ \mathfrak{g} * E &\longmapsto E' \end{aligned}$$

Compatibility: $\mathfrak{g}' * (\mathfrak{g} * E) = (\mathfrak{g}'\mathfrak{g}) * E$ for all $\mathfrak{g}, \mathfrak{g}' \in \mathcal{G}$ and $E \in \mathcal{E}$;

Identity: $\mathfrak{e} * E = E$ if and only if $\mathfrak{e} \in \mathcal{G}$ is the identity element;

Regularity: for all $E, E' \in \mathcal{E}$ there exist a unique $\mathfrak{g} \in \mathcal{G}$ such that $\mathfrak{g} * E' = E$.

Cryptographic Group Actions (Alamati, D., Montgomery, Patranabis 2021)

Hard Homogeneous Space (HHS) — Couveignes 1997 (eprint:2006/291)

$\mathcal{G} \circlearrowleft \mathcal{E}$ such that $\mathcal{G}$ is commutative and:

- Evaluating $E' = \mathfrak{g} * E$ is easy;
- Inverting the action is hard.

Example

Let G be a group of order 13, then $(\mathbb{Z}/13\mathbb{Z})^\times \circlearrowleft G$ defined by

$$a * g := g^a$$

is an HHS. . .

Cryptographic Group Actions (Alamati, D., Montgomery, Patranabis 2021)

Hard Homogeneous Space (HHS) — Couveignes 1997 (eprint:2006/291)

$\mathcal{G} \circlearrowleft \mathcal{E}$ such that $\mathcal{G}$ is commutative and:

- Evaluating $E' = \mathfrak{g} * E$ is easy;
- Inverting the action is hard.

Example

Let G be a group of order 13, then $(\mathbb{Z}/13\mathbb{Z})^\times \circlearrowleft G$ defined by

$$a * g := g^a$$

is an HHS…But

$$g^a \cdot g^b = g^{a+b}$$

has no interpretation as a group action!

Key exchange from group actions

Public parameters:

- A HHS $\mathcal{G} \circlearrowright \mathcal{E}$ of order N (large, but not necessarily prime);
- A starting set element $E_0 \in \mathcal{E}$.

Notation: $[\mathfrak{a}] := \mathfrak{a} * E_0$.

Alice | **Bob**

pick random $\mathfrak{a} \in \mathcal{G}$ | pick random $\mathfrak{b} \in \mathcal{G}$

$$\xrightarrow{\quad[\mathfrak{a}]\quad}$$

$$\xleftarrow[\quad[\mathfrak{b}]\quad]{}$$

Shared secret is $\mathfrak{a}[\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}] = \mathfrak{b}[\mathfrak{a}]$

Quantum security

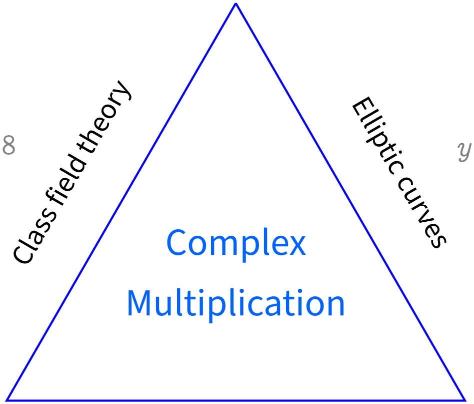
Fact: Shor's algorithm does not apply to Diffie-Hellman protocols from group actions.

Subexponential attack $\exp(\sqrt{\log p \log\log p})$

- Reduction to the hidden shift problem by evaluating the class group action in quantum superposition (subexpoential cost);
- Well known reduction from the hidden shift to the dihedral (non-abelian) hidden subgroup problem;
- Kuperberg's algorithm solves the dHSP with a subexponential number of class group evaluations.
- Recent work suggests that 2^{64}-qbit security is achieved somewhere in $512 < \log p < 2048$.

$$H(j) = j - 1728$$

$$y^2 = x^3 - ax - b$$



Modular functions

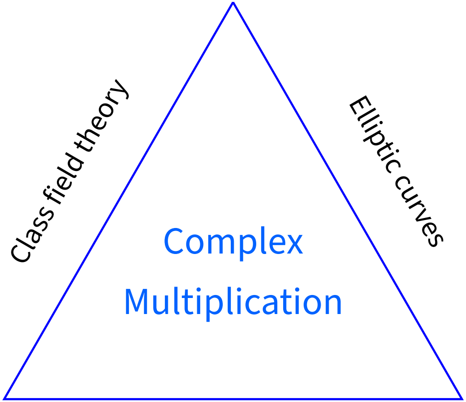
$$j(z) = \frac{1}{q} + 744 + 196884q + \cdots$$

Abelian extensions

of $\mathbb{Q}(\sqrt{-D})$

Elliptic curves with

$\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{-D})$

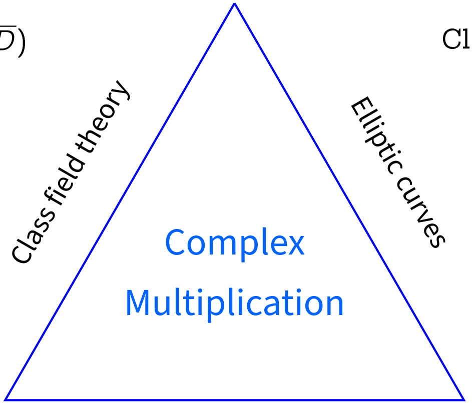


Modular functions

Galois group of $K/\mathbb{Q}(\sqrt{-D})$

$\simeq$

Class group $\mathrm{Cl}(-D)$

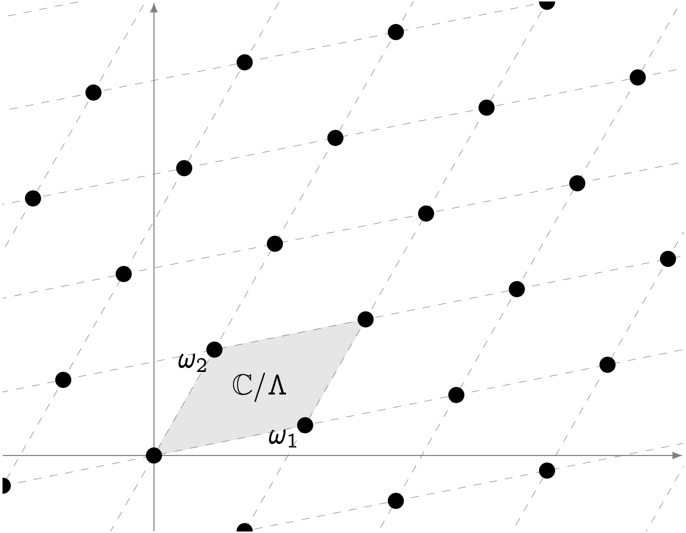


$\mathrm{Cl}(-D)$ acts on set of E s.t.

$\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{-D})$

Modular functions

Complex tori

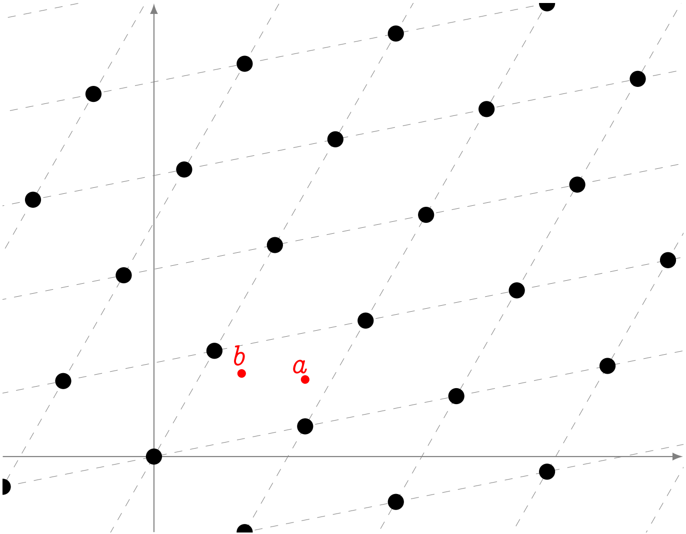


Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

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

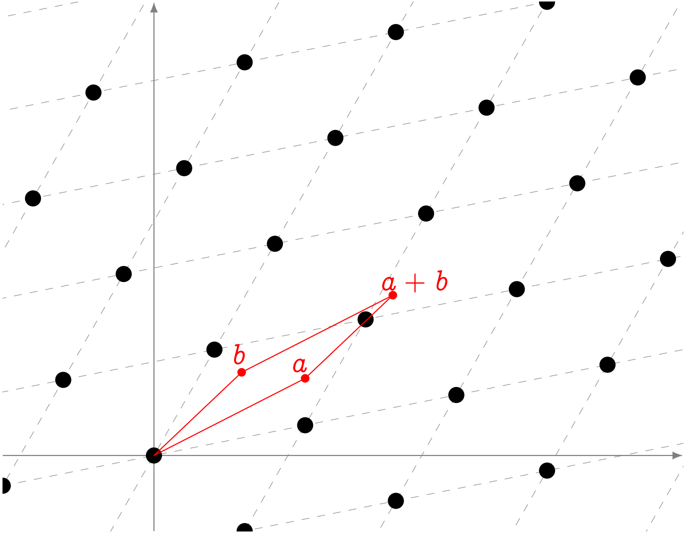
$\mathbb{C}/\Lambda$ is a complex torus.

Complex tori



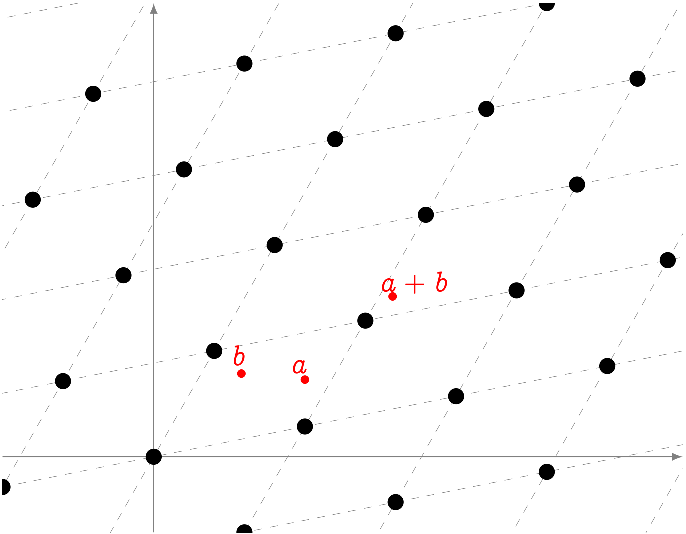
Addition law induced by addition on $\mathbb{C}$.

Complex tori



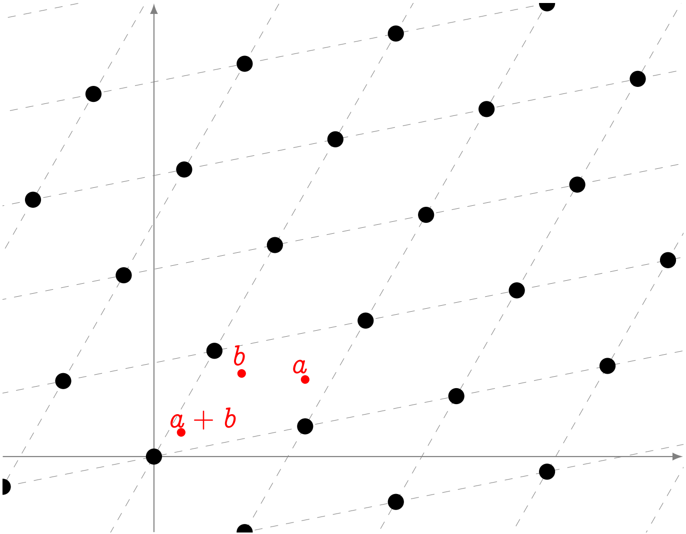
Addition law induced by addition on $\mathbb{C}$.

Complex tori



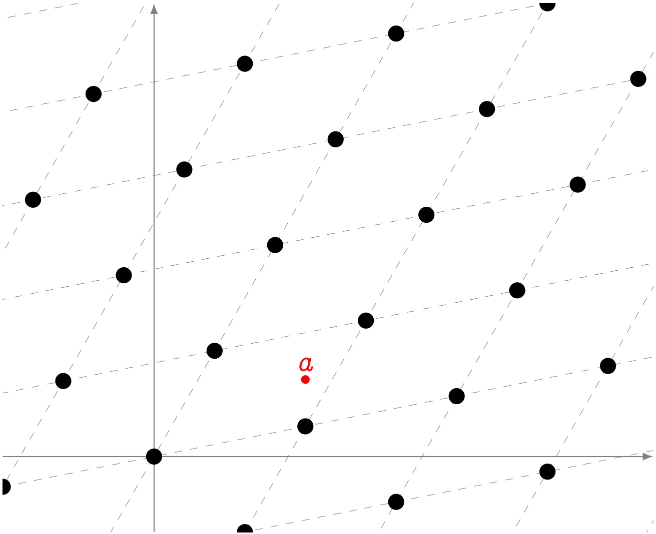
Addition law induced by addition on $\mathbb{C}$.

Complex tori



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

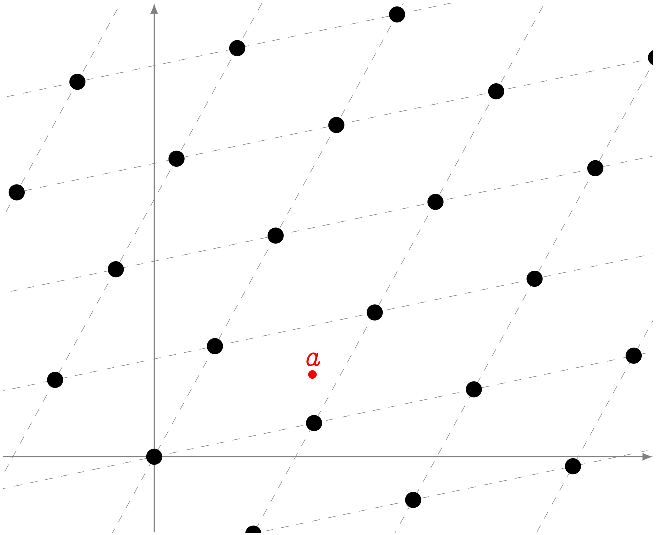
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

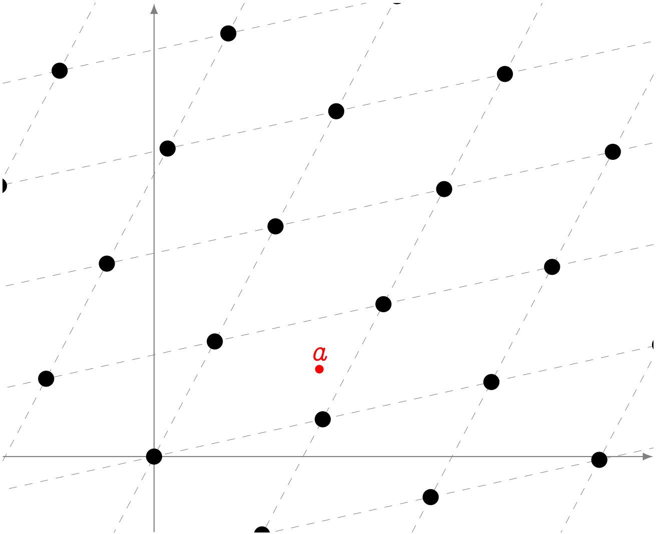
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

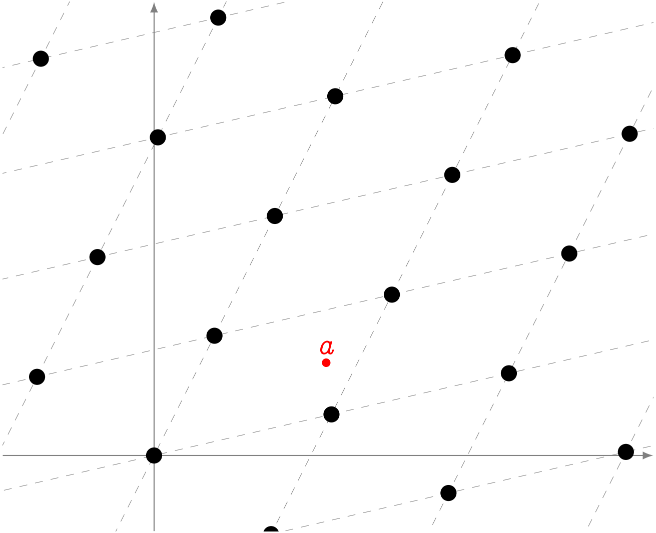
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

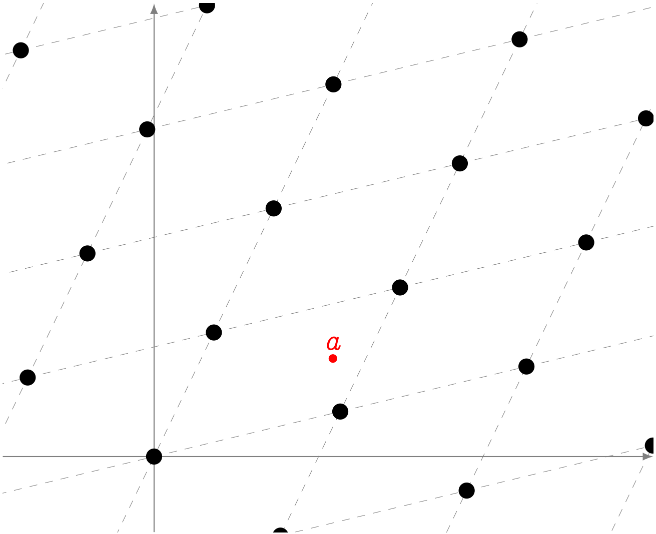
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

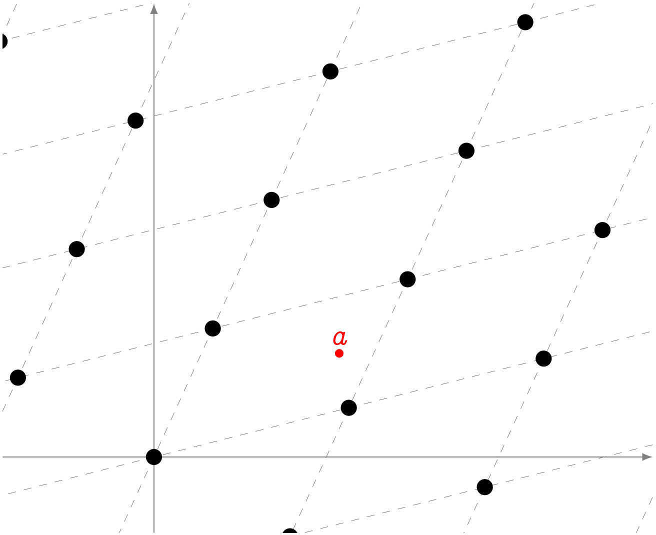
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

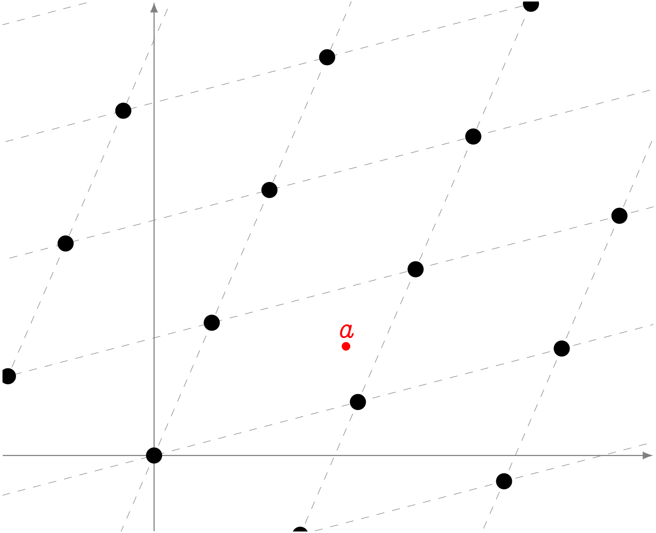
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

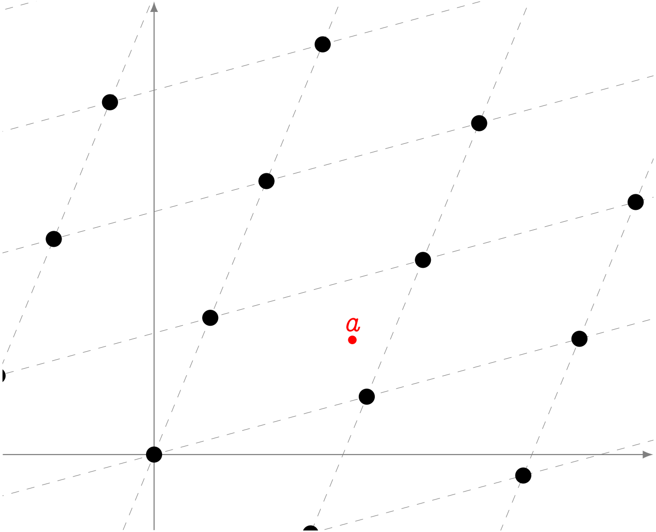
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

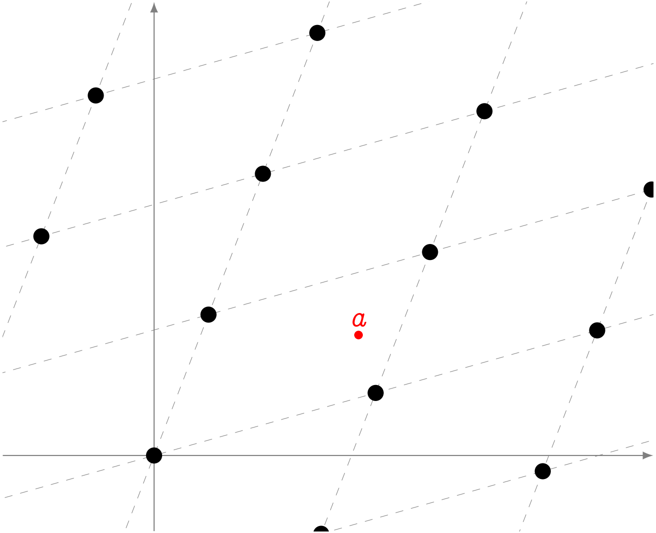
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

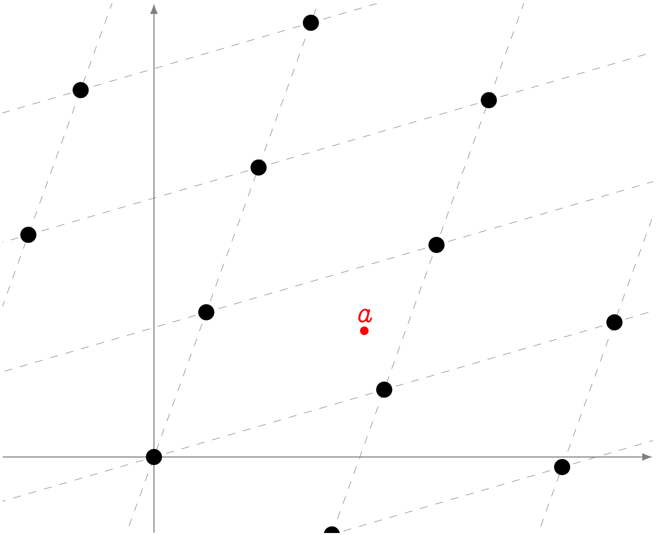
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

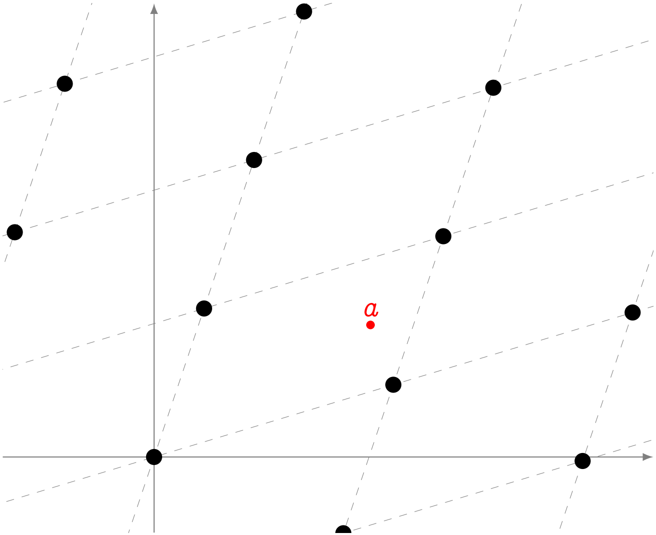
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

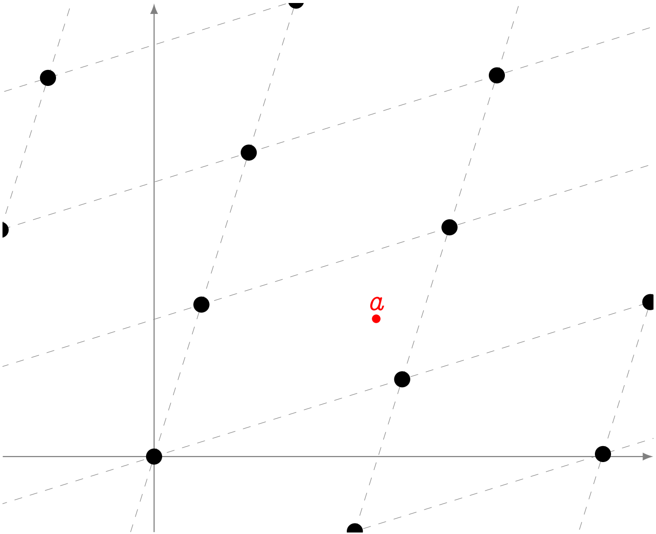
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

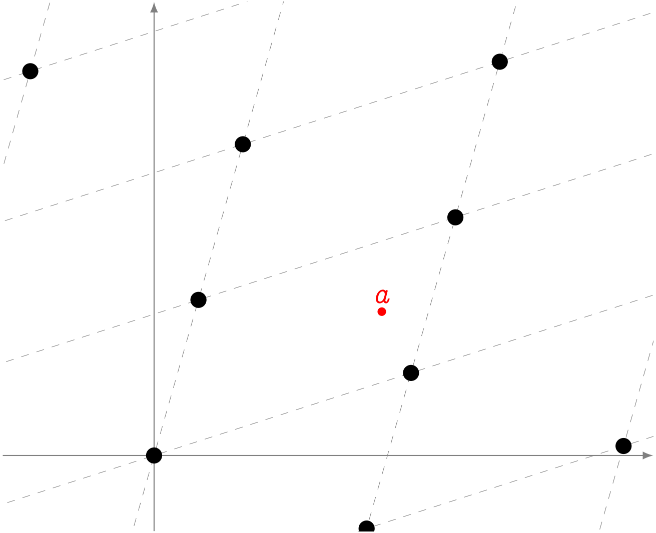
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

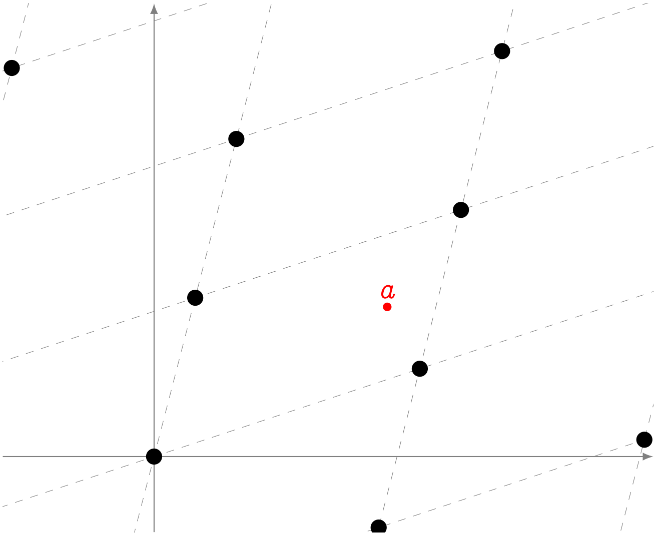
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

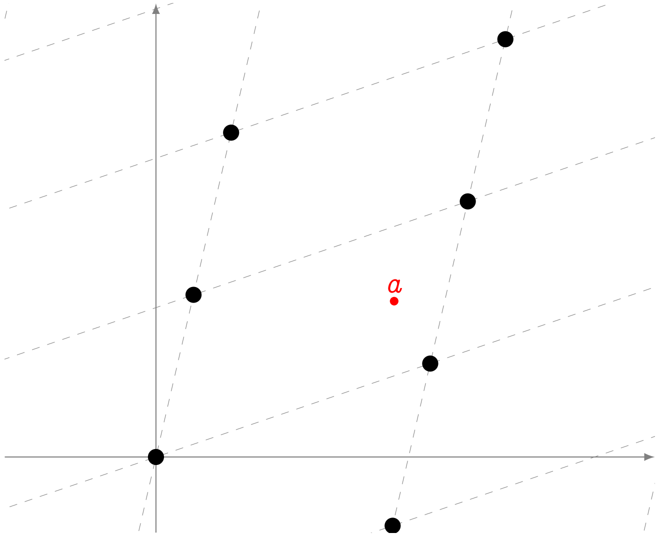
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

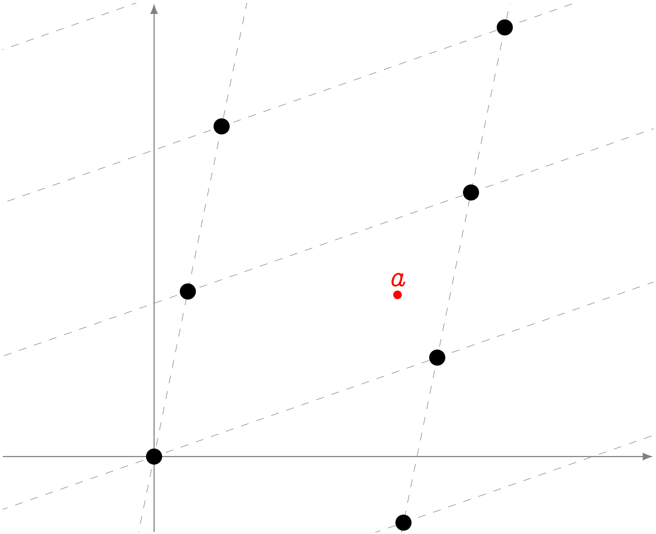
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

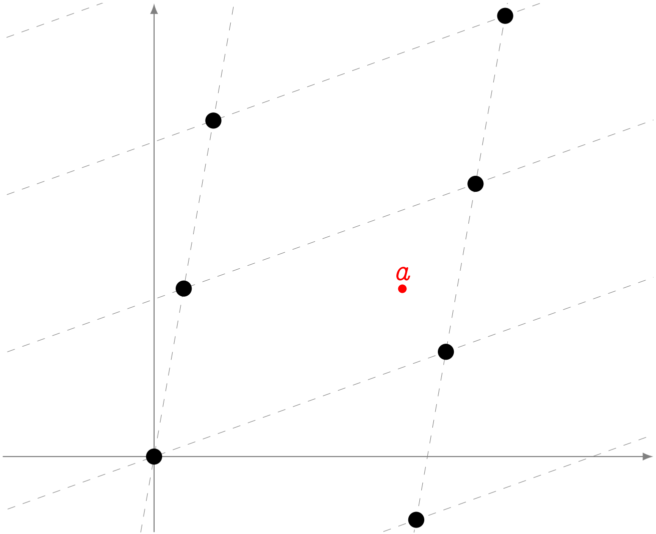
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

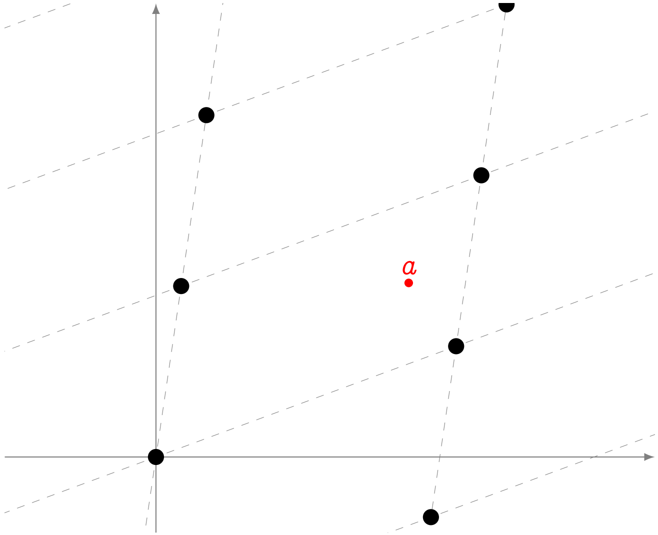
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

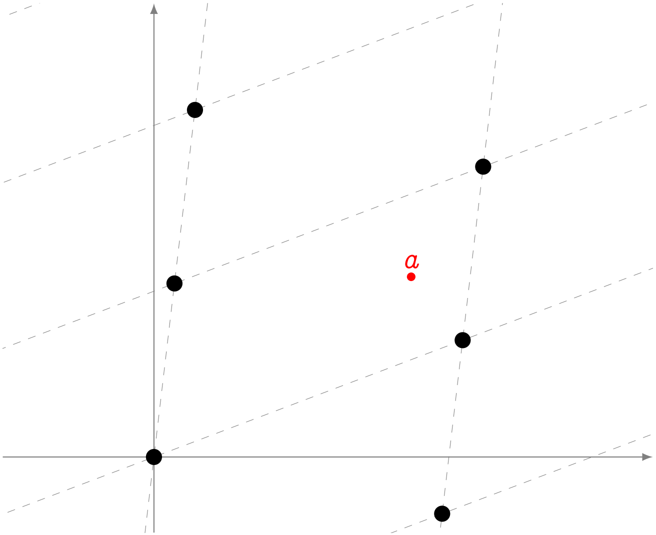
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

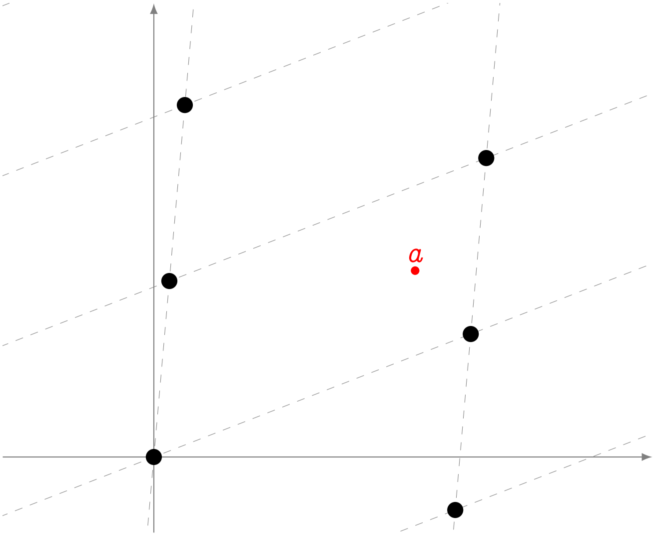
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

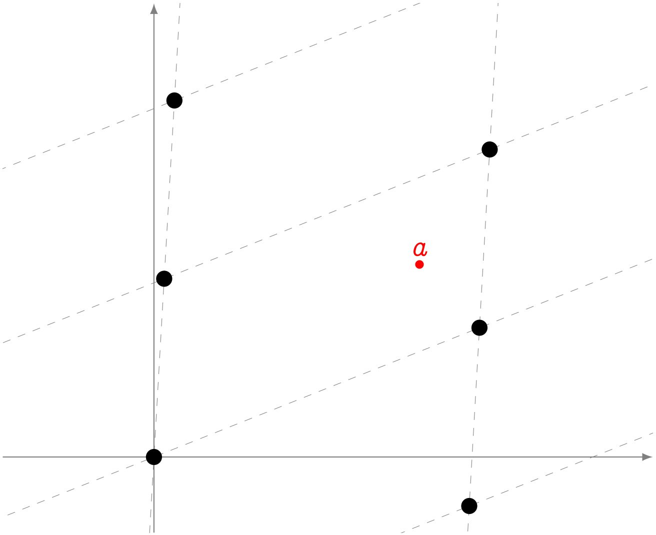
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

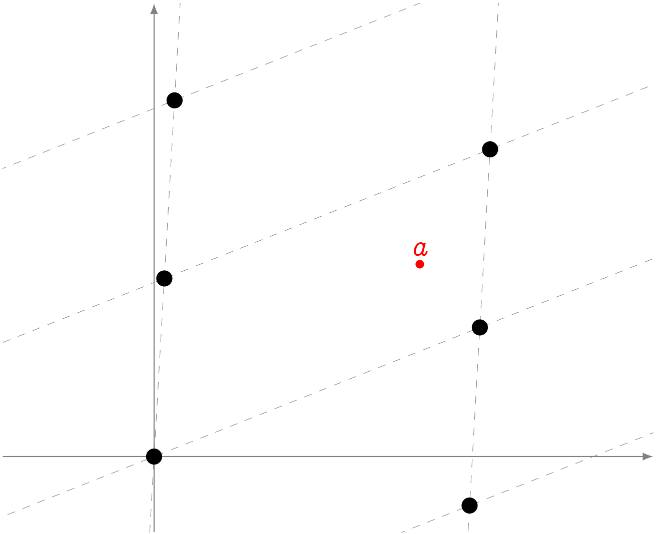
Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

Homotheties



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

$$\alpha\Lambda_1 = \Lambda_2$$

Uniformization theorem

One to one correspondence: Complex tori $\leftrightarrow$ Elliptic curves over $\mathbb{C}$

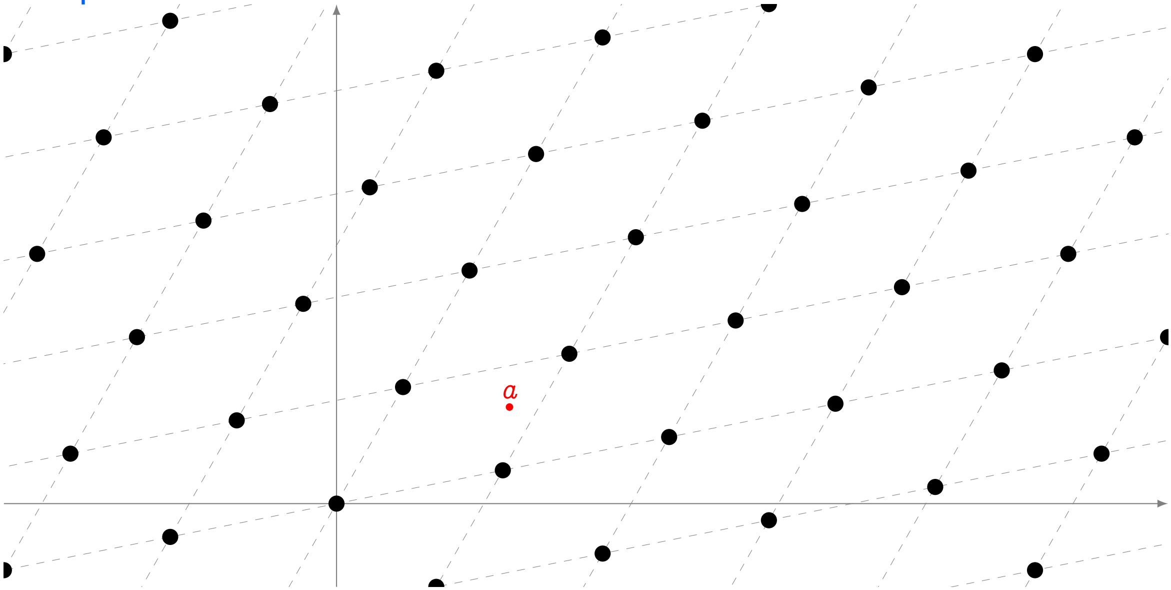
- Isomorphic as Riemann surfaces,
- Isomorphic as groups,
- Homotheties of lattices = Isomorphisms of elliptic curves.

The j-invariant

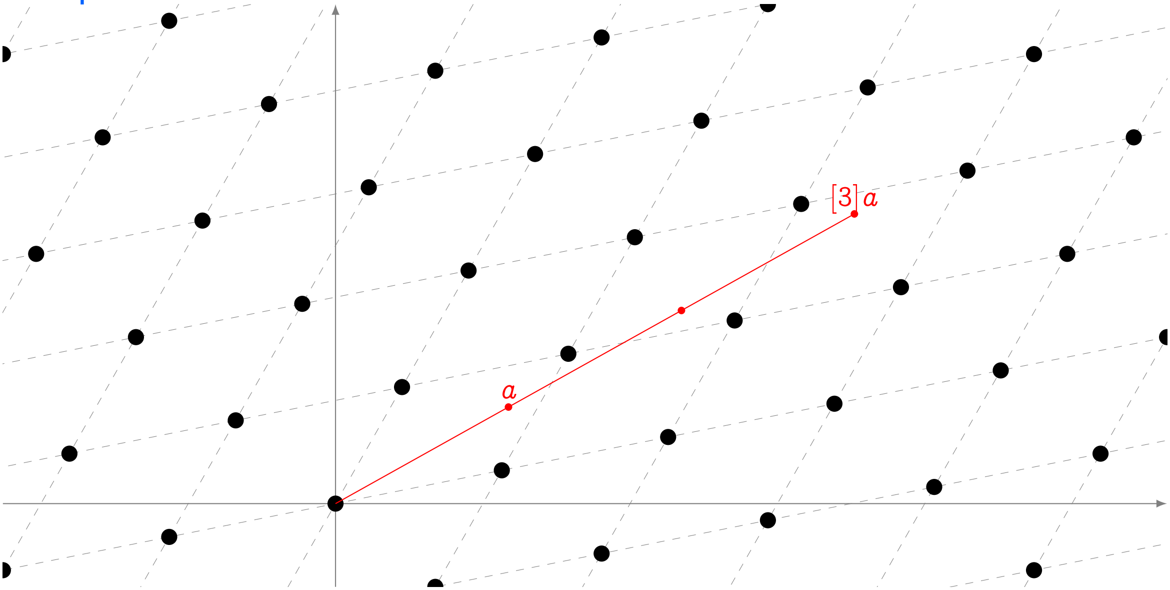
$$j(E) = 1728\frac{4a^3}{4a^3 - 27b^2}$$

classifies curves/tori up to isomorphism/homothety.

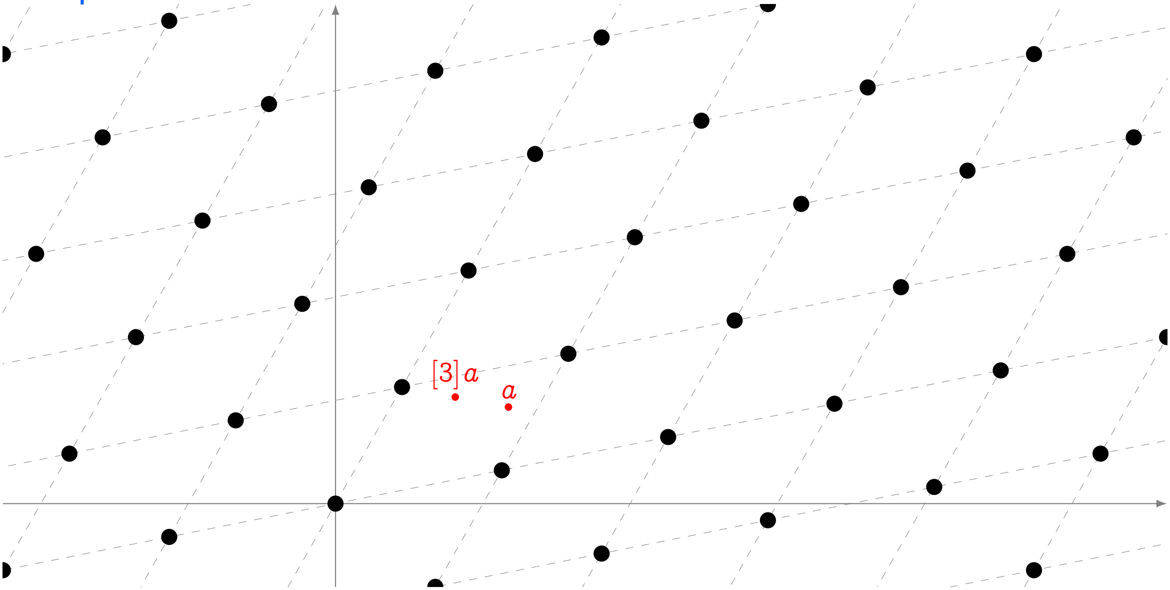
Multiplication



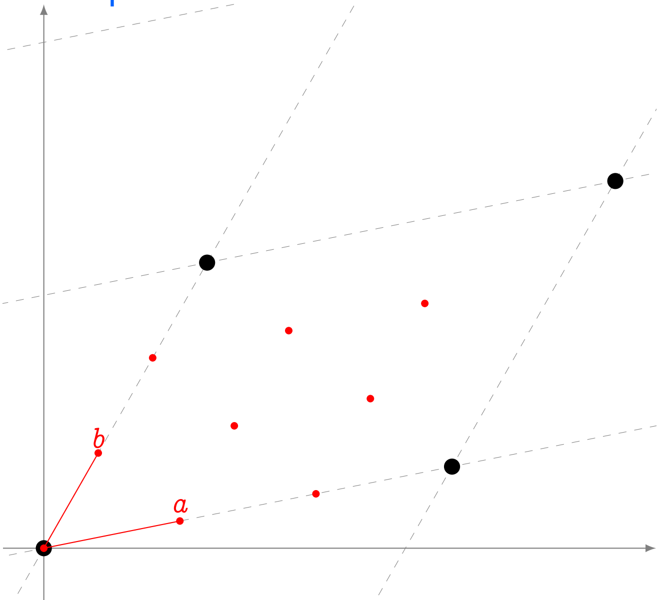
Multiplication



Multiplication



Endomorphisms



Let α be such that $\alpha\Lambda \subset \Lambda$, then

$$\phi_\alpha \ : \ z \mapsto \alpha z \mod \Lambda$$

is an endomorphism of $\mathbb{C}/\Lambda$.

Let ℓ be an integer, the kernel of ϕ_ℓ is:

$$\begin{aligned}(\mathbb{C}/\Lambda)[\ell] &= \langle a, b\rangle \\ &\simeq (\mathbb{Z}/\ell\mathbb{Z})^2\end{aligned}$$

Complex Multiplication (CM)

Endomorphisms form a subring of $\mathbb{C}$: indeed $\alpha\Lambda \subset \Lambda$ and $\beta\Lambda \subset \Lambda$ imply

- $(\alpha + \beta)\Lambda \subset \Lambda$,
- $(\alpha\beta)\Lambda \subset \Lambda$.

Theorem

Let C/Λ be a complex torus, its endomorphism ring is one of:

- *The ring of integers $\mathbb{Z}$,*
- *An order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$.*[a]

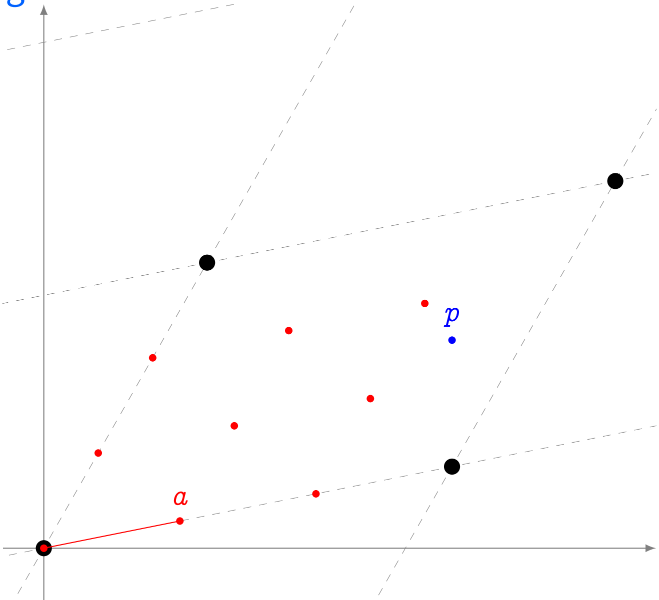
[a] A subring that is a lattice of dimension 2.

Corollary

For any endomorphism ϕ_α there exist integers t, n such that

$$\phi_\alpha^2 - t\phi_\alpha + n = 0.$$

Isogenies



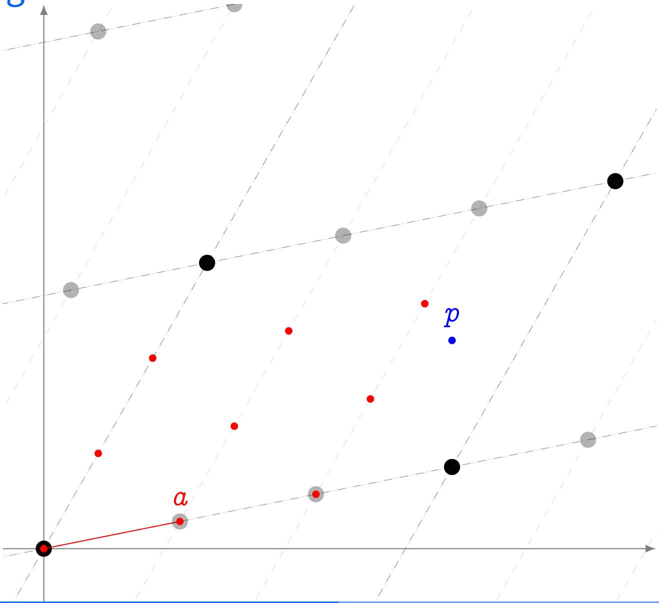
Let $\alpha\Lambda \subset \Lambda'$, the map

$$\begin{aligned} \phi_\alpha \;:\; \mathbb{C}/\Lambda &\to \mathbb{C}/\Lambda' \\ z &\mapsto \alpha z \mod \Lambda' \end{aligned}$$

is a morphism of complex Lie groups.

It is called an isogeny, and it is completely characterized by its kernel $\alpha^{-1}\Lambda'$.

Isogenies



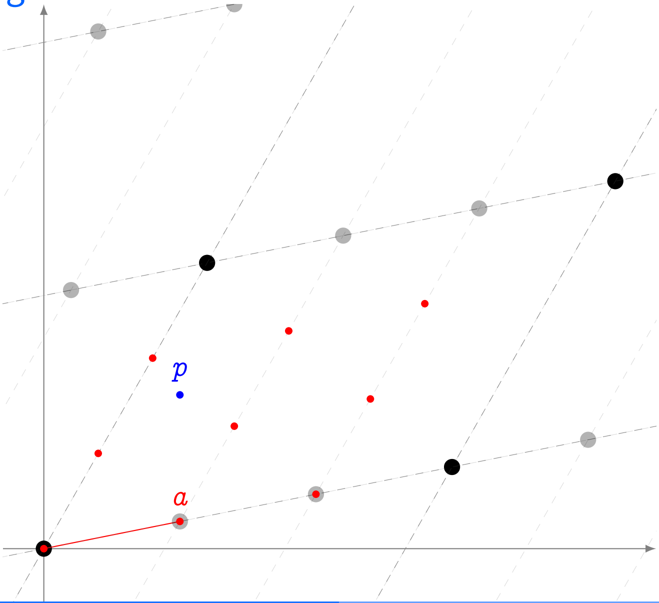
Let $\alpha\Lambda \subset \Lambda'$, the map

$$\begin{aligned}\phi_\alpha \;:\; \mathbb{C}/\Lambda &\to \mathbb{C}/\Lambda'\\ z &\mapsto \alpha z \mod \Lambda'\end{aligned}$$

is a morphism of complex Lie groups.

It is called an isogeny, and it is completely characterized by its kernel $\alpha^{-1}\Lambda'$.

Isogenies



Let $\alpha\Lambda \subset \Lambda'$, the map

$$\begin{aligned}\phi_\alpha \;:\; \mathbb{C}/\Lambda &\to \mathbb{C}/\Lambda'\\ z &\mapsto \alpha z \mod \Lambda'\end{aligned}$$

is a morphism of complex Lie groups.

It is called an isogeny, and it is completely characterized by its kernel $\alpha^{-1}\Lambda'$.

Isogenies $\leftrightarrow$ ideals

- Let E be an elliptic curve/complex torus with endomorphism ring $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$.
- Let $G \subset E(\mathbb{C})$ be a finite subgroup.

Define the kernel ideal

$$\mathrm{Ann}(G) = \{\alpha \in \mathcal{O} \mid \alpha(G) = 0\}.$$

Conversely, given an ideal $\mathfrak{a} \subset \mathcal{O}$, define

$$E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker \alpha.$$

Finally, let $\mathcal{I}(\mathcal{O})$ be the group of (fractional) ideals of $\mathcal{O}$ and let $\mathcal{P}(\mathcal{O})$ be the subgroup of principal ideals, define the class group

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

CM dictionary

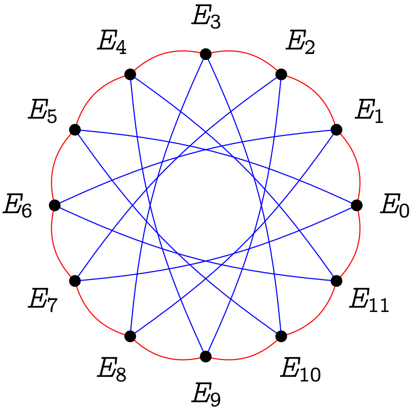
Quadratic imaginary fields	Elliptic curves
Integers of $\mathbb{Q}(\sqrt{-D})$	Endomorphisms of E
Integral ideals of $\mathbb{Q}(\sqrt{-D})$	Isogenies of E
Ideal classes in $\mathrm{Cl}(-D)$	Isogenies $\bullet \rightrightarrows \bullet$
Ideal norm	Isogeny degree
Conjugate ideal	Dual isogeny

The fundamental theorem of CM

- Let E be an elliptic curve with CM by a quadratic imaginary order $\mathcal{O}$.
- Let $\mathfrak{a} \subset \mathcal{O}$ be an integral ideal.
- Denote by $E/E[\mathfrak{a}]$ the image curve of the unique isogeny $\phi_{\mathfrak{a}}$ of kernel $E[\mathfrak{a}]$.

Theorem

The operator $\mathfrak{a} * E := E/E[\mathfrak{a}]$ defines a transitive action of the group of fractional ideals of $\mathcal{O}$ on the (finite) set $\mathcal{E}(\mathcal{O})$ of elliptic curves with complex multiplication by $\mathcal{O}$. The action factors through principal ideals. In other words, the class group $\mathrm{Cl}(\mathcal{O})$ acts regularly on $\mathcal{E}(\mathcal{O})$.



Reduction at $\mathfrak{p}$

Complex multiplication over $\mathbb{C}$ $\sim$ Discrete log in $\mathbb{Q}(e^{2i\pi/N})$

Theorem

Let E be an elliptic curve over a number field L, with CM by an order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$. Let p be a prime split in L, denote by E_p the reduction of E at a place above p, and assume that E_p is non-singular.

- *If $\left(\frac{-D}{p}\right) = 1$ then E_p is said to be ordinary and $\mathrm{End}(E_p) \simeq \mathcal{O}$.*
- *If $\left(\frac{-D}{p}\right) = -1$ then E_p is said to be supersingular and $\mathcal{O} \subsetneq \mathrm{End}(E_p)$.*

Complex multiplication over $\mathbb{F}_p$: Couveignes '06, Rostovtsev–Stolbunov '06, CSIDH '18, OSIDH '20, …

Key exchange from complex multiplication

Public parameters:

- A starting curve $E_0/\mathbb{F}_p$ with complex multiplication by $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$,
- …

Notation: $[\mathfrak{a}] := \mathfrak{a} * E_0$.

Alice | **Bob**

pick random ideal $\mathfrak{a}$ | pick random ideal $\mathfrak{b}$

$$\xrightarrow{[\mathfrak{a}]}$$

$$\xleftarrow[{[\mathfrak{b}]}]{}$$

Shared secret is $\mathfrak{a}[\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}] = \mathfrak{b}[\mathfrak{a}]$

A partial converse

Deuring's lifting theorem

Let E_p be an elliptic curve in characteristic p, with an endomorphism ω_p which is not trivial. Then there exists an elliptic curve E defined over a number field L, an endomorphism ω of E, and a non-singular reduction of E at a place $\mathfrak{p}$ of L lying above p, such that E_p is isomorphic to $E(\mathfrak{p})$, and ω_p corresponds to $\omega(\mathfrak{p})$ under the isomorphism.

The full endomorphism ring

Theorem (Deuring)

Let E be a supersingular elliptic curve, then

- E is isomorphic to a curve defined over $\mathbb{F}_{p^2}$;
- Every isogeny of E is defined over $\mathbb{F}_{p^2}$;
- Every endomorphism of E is defined over $\mathbb{F}_{p^2}$;
- $\mathrm{End}(E)$ is isomorphic to a maximal order in a quaternion algebra ramified at p and ∞.

In particular:

- If E is defined over $\mathbb{F}_p$, then $\mathrm{End}_{\mathbb{F}_p}(E)$ is strictly contained in $\mathrm{End}(E)$.
- Some endomorphisms do not commute!

An example

The curve of j-invariant 1728

$$E : y^2 = x^3 + x$$

is supersingular over $\mathbb{F}_p$ iff $p = -1 \mod 4$.

Endomorphisms

$\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}\langle \iota, \pi \rangle$, with:

- π the Frobenius endomorphism, s.t. $\pi^2 = -p$;
- ι the map

  $$\iota(x, y) = (-x, iy),$$

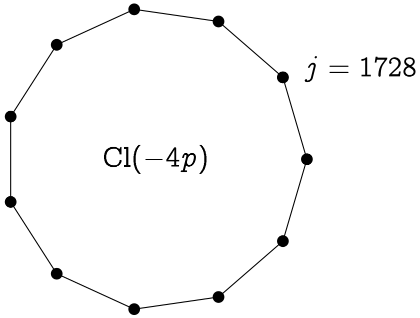
  where $i \in \mathbb{F}_{p^2}$ is a 4-th root of unity. Clearly, $\iota^2 = -1$.

And $\iota\pi = -\pi\iota$.

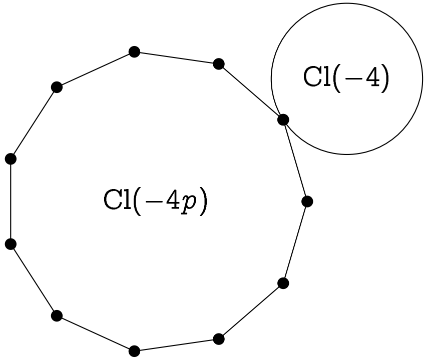
Class group action party

$\bullet\ j = 1728$

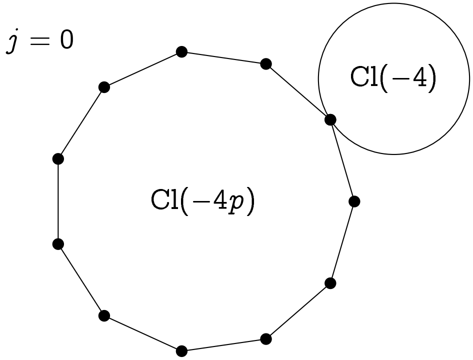
Class group action party



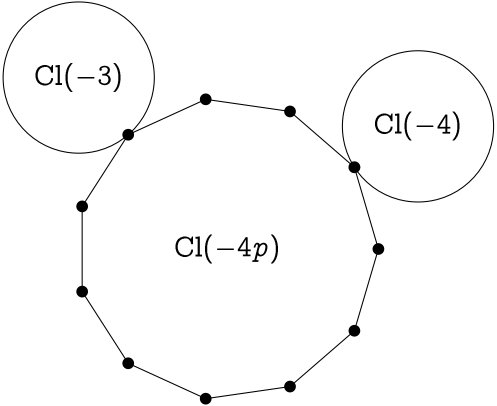
Class group action party



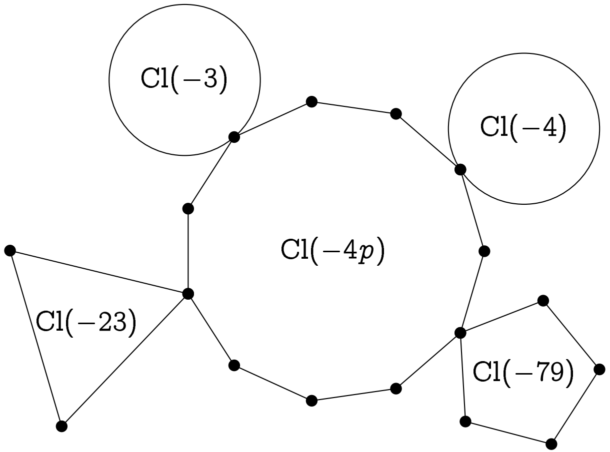
Class group action party



Class group action party



Class group action party



Quaternion algebra?! WTF?[2]

The quaternion algebra $B_{p,\infty}$ is:

- A 4-dimensional $\mathbb{Q}$-vector space with basis $(1, i, j, k)$.
- A non-commutative division algebra[1] $B_{p,\infty} = \mathbb{Q}\langle i, j\rangle$ with the relations:

$$i^2 = a, \quad j^2 = -p, \quad ij = -ji = k,$$

  for some $a < 0$ (depending on p).
- All elements of $B_{p,\infty}$ are quadratic algebraic numbers.
- $B_{p,\infty} \otimes \mathbb{Q}_\ell \simeq \mathcal{M}_{2\times 2}(\mathbb{Q}_\ell)$ for all $\ell \neq p$.
  I.e., endomorphisms restricted to $E[\ell^e]$ are just 2×2 matrices mod ℓ^e.
- $B_{p,\infty} \otimes \mathbb{R}$ is isomorphic to Hamilton's quaternions.
- $B_{p,\infty} \otimes \mathbb{Q}_p$ is a division algebra.

---

[1] All elements have inverses.
[2] What The Field?

The Deuring correspondence

Let $\mathcal{O}, \mathcal{O}' \subset B_{p,\infty}$ be two maximal orders. They have the same type if there exists α s.t.

$$\mathcal{O} = \alpha\mathcal{O}'\alpha^{-1}.$$

Theorem (Deuring)

Maximal order types of $B_{p,\infty}$ are in one-to-one correspondence with supersingular curves up to Galois conjugation in $\mathbb{F}_{p^2}/\mathbb{F}_p$.

The Deuring correspondence

Two left ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}$ are in the same class if there exists β s.t. $\mathfrak{a} = \mathfrak{b}\beta$.

An equivalence of categories (Kohel, roughly)

$$
\begin{tikzcd}
\substack{\{\alpha \in B_{p,\infty} \mid \alpha\mathfrak{a} = \mathfrak{a}\} \\ \text{left order}} \arrow[dr, dashed] & \text{connecting ideal (class)} & \substack{\{\alpha \in B_{p,\infty} \mid \mathfrak{a}\alpha = \mathfrak{a}\} \\ \text{right order}} \arrow[dl, dashed] \\
& \mathcal{O} \arrow[r, "\mathfrak{a}"] & \mathcal{O}' \\
& E \arrow[r, "\phi_{\mathfrak{a}}"'] & E' \\
\text{supersingular curve} \arrow[ur, dashed] & \text{isogeny (class)} & \text{supersingular curve} \arrow[ul, dashed]
\end{tikzcd}
$$

Supersingular isogeny graphs

- There is a unique isogeny class of supersingular curves over $\bar{\mathbb{F}}_p$ of size $\approx p/12$.
- The graph of isogenies of degree ℓ is $(\ell+1)$-regular.
- It is a Ramanujan graphs, i.e., an optimal expander.
- Related to Hecke operators, modular forms, Brandt matrices…

Applications:

- Hash functions,
- Key exchange (SIDH/SIKE),
- …

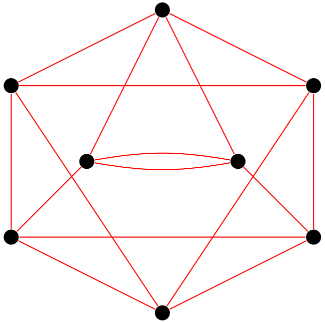


Figure: 3-isogeny graph on $\mathbb{F}_{97^2}$.

SQISign: Signatures from the effective Deuring correspondence

$$\begin{tikzcd} E_0 \arrow[d, dashed, "\tau"'] \\ E_A \end{tikzcd}$$

- - - - - secret key isogeny

Most compact PQ signature scheme: PK + Signature combined **5 × smaller** than Falcon.

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
16	64	204	NIST-1

SQISign: Signatures from the effective Deuring correspondence

$$\begin{tikzcd} E_0 \arrow[r, "\psi"] \arrow[d, dashed, "\tau"'] & E_1 \\ E_A & \end{tikzcd}$$

$\longrightarrow$ commitment isogeny (prover)

$\dashrightarrow$ secret key isogeny

Most compact PQ signature scheme: PK + Signature combined **5 $\times$ smaller** than Falcon.

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
16	64	204	NIST-1

SQISign: Signatures from the effective Deuring correspondence

$$
\begin{tikzcd}
 & E_0 \arrow[r, "\psi"] \arrow[dl, dashed, "\tau"'] & E_1 \arrow[d, "\varphi"] \\
E_A & & E_2
\end{tikzcd}
$$

$\longrightarrow$ commitment isogeny (prover)

$\longrightarrow$ challenge isogeny (verifier)

$- - - - -$ secret key isogeny

Most compact PQ signature scheme: PK + Signature combined **5** $\times$ **smaller** than Falcon.

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
16	64	204	NIST-1

SQISign: Signatures from the effective Deuring correspondence

$$\begin{tikzcd}
E_0 \arrow[r, "\psi"] \arrow[d, dashed, "\tau"'] & E_1 \arrow[d, "\varphi"] \\
E_A \arrow[r, "\sigma"] & E_2
\end{tikzcd}$$

commitment isogeny (prover)

challenge isogeny (verifier)

response isogeny (prover)

secret key isogeny

Most compact PQ signature scheme: PK + Signature combined **5 $\times$ smaller** than Falcon.

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
16	64	204	NIST-1

Effective correspondences (over finite fields)

Discrete log: $g \xrightarrow{\quad\text{exp}\quad} g^n$

- schoolbook method

Complex multiplication: $E \xrightarrow{\quad\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})\quad} E'$

- Vélu '71, Elkies '92, and many others…

Deuring correspondence: $E \xrightarrow{\quad\mathfrak{a} \subset B_{p,\infty}\quad} E'$

- all of the above,
- Kohel, Lauter, Petit, Tignol '14 (KLPT),
- D., Kohel, Leroux, Petit, Wesolowski '20 (part of SQISign).

Thank you

`https://defeo.lu/`

@luca_defeo