NTNU | Norwegian University of Science and Technology

Supersingular Endomorphism Rings: Algorithms and Applications

Jonathan Komada Eriksen,
23.08.2024

Overview

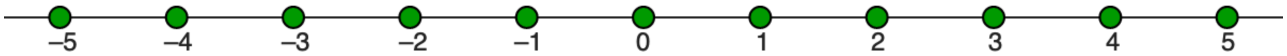
- The Deuring correspondence
  - Numberfields, quaternion algebras and orders
  - Elliptic curves, and endomorphism rings
- Papers about the constructive deuring correspondence
  - **Deuring for the People**
- Papers about orientations
  - **PEARL-SCALLOP**

Background: The Deuring Correspondence

The focal point of this thesis

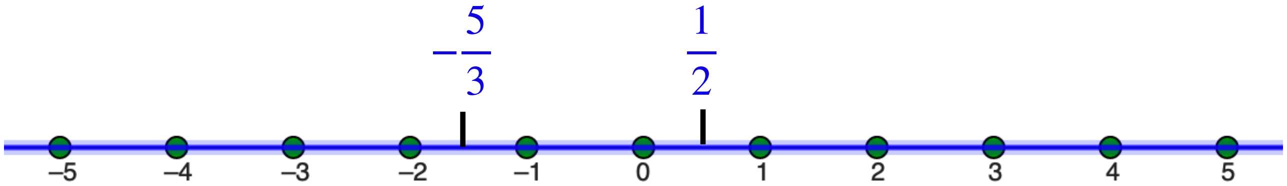
The Number Line

$\mathbb{Z}$



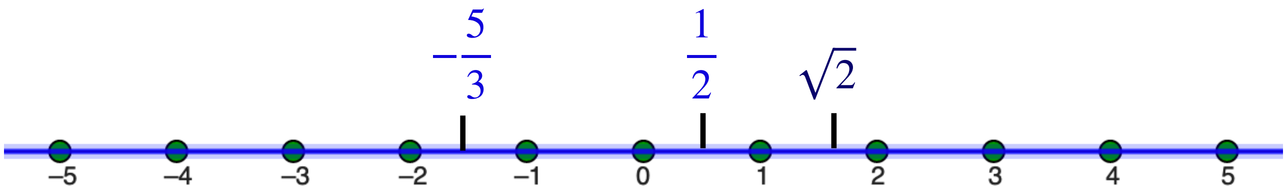
The Number Line

$$\mathbb{Z} \subset \mathbb{Q}$$



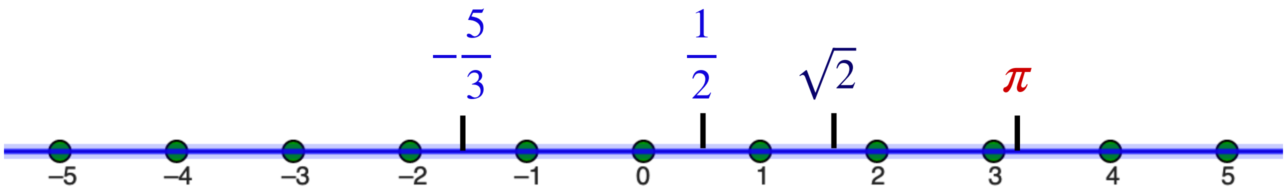
The Number Line

$$\mathbb{Z} \subset \mathbb{Q}$$



The Number Line

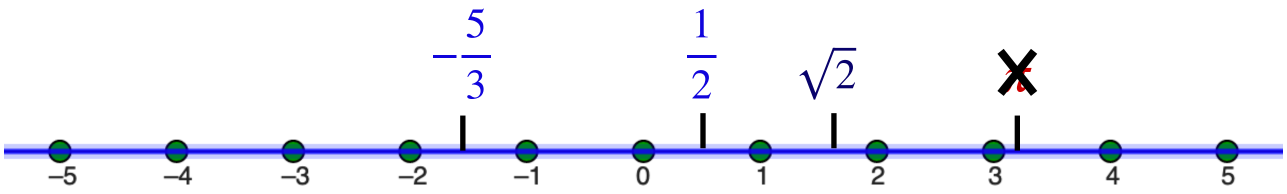
$$\mathbb{Z} \subset \mathbb{Q}$$



$$\mathbb{R}$$

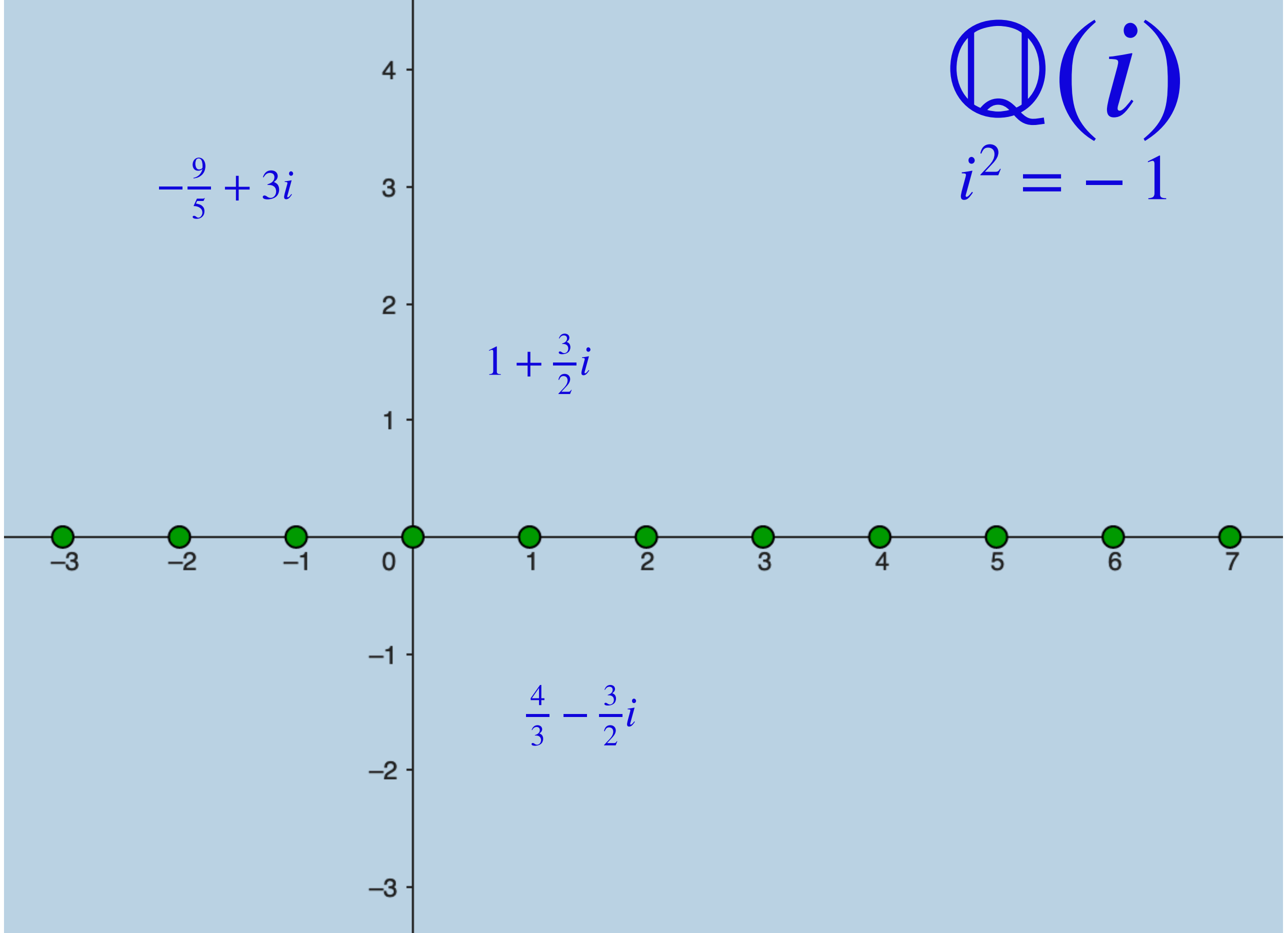
The Number Line

$$\mathbb{Z} \subset \mathbb{Q}$$



$$\cancel{\mathbb{R}}$$

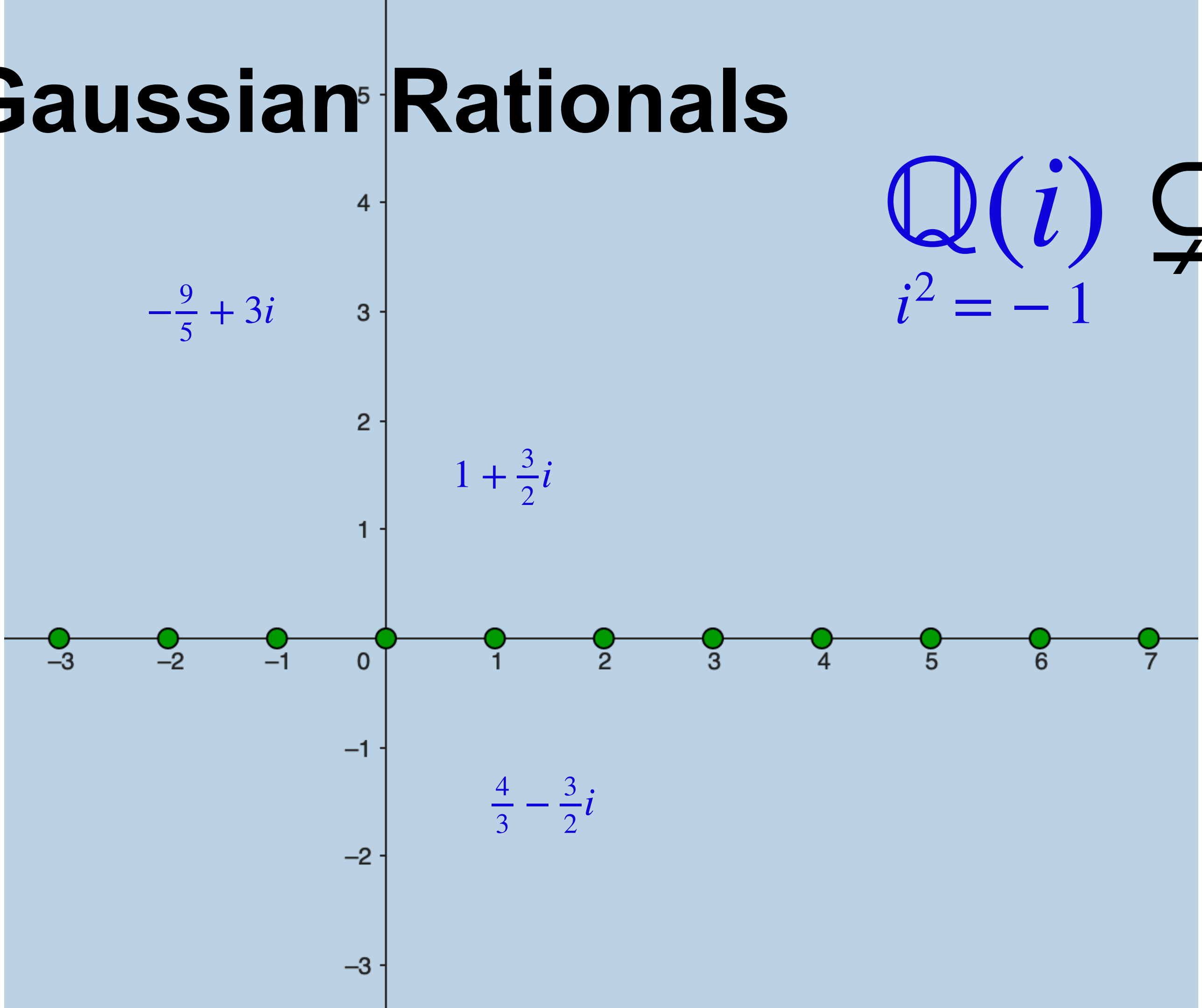
The Gaussian Rationals



The Gaussian Rationals

$\mathbb{Q}(i) \subsetneq \mathbb{C}$

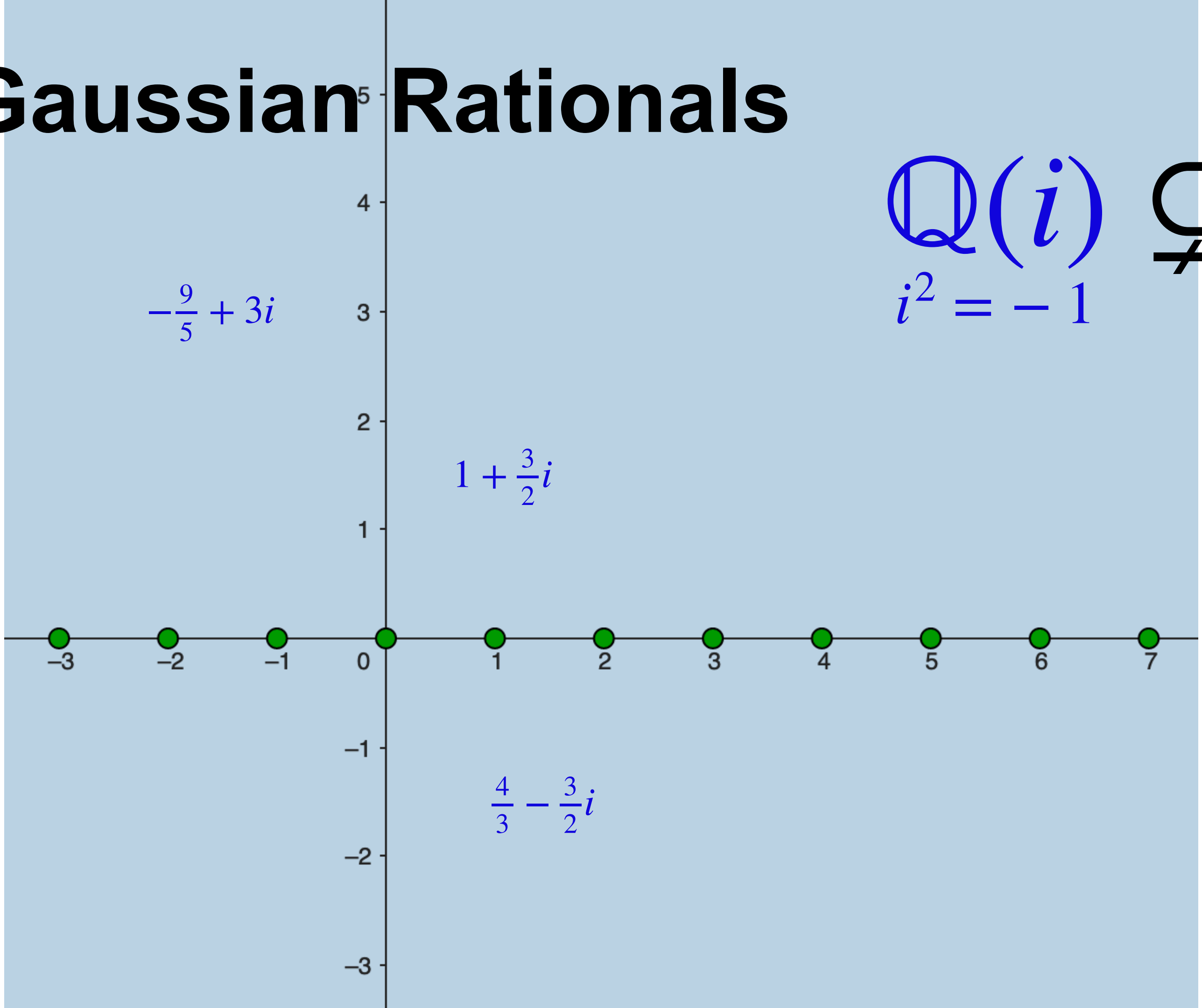
$i^2 = -1$



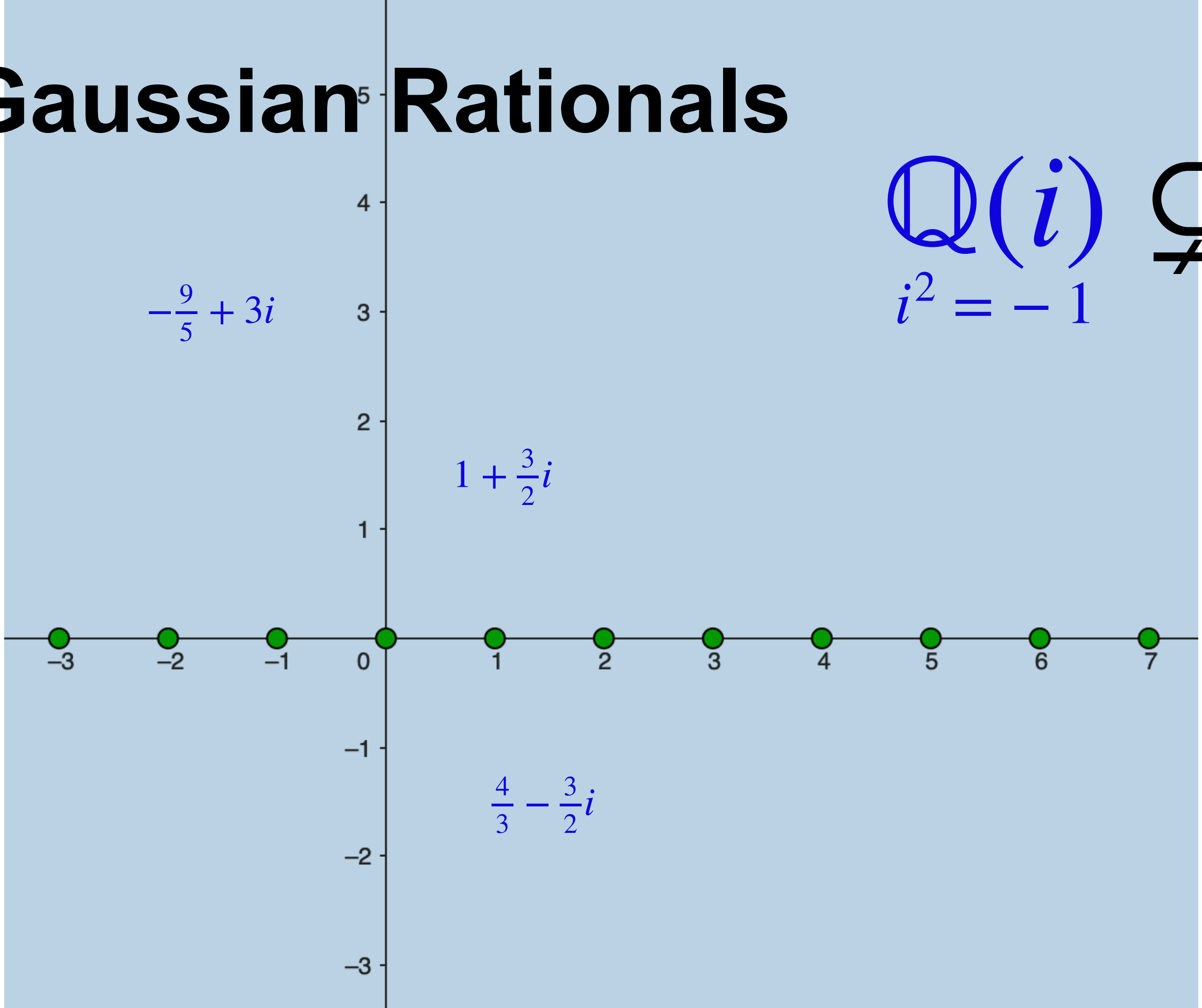
The Gaussian Rationals

$$\mathbb{Q}(i) \subsetneq \cancel{\mathbb{C}}$$

$$i^2 = -1$$



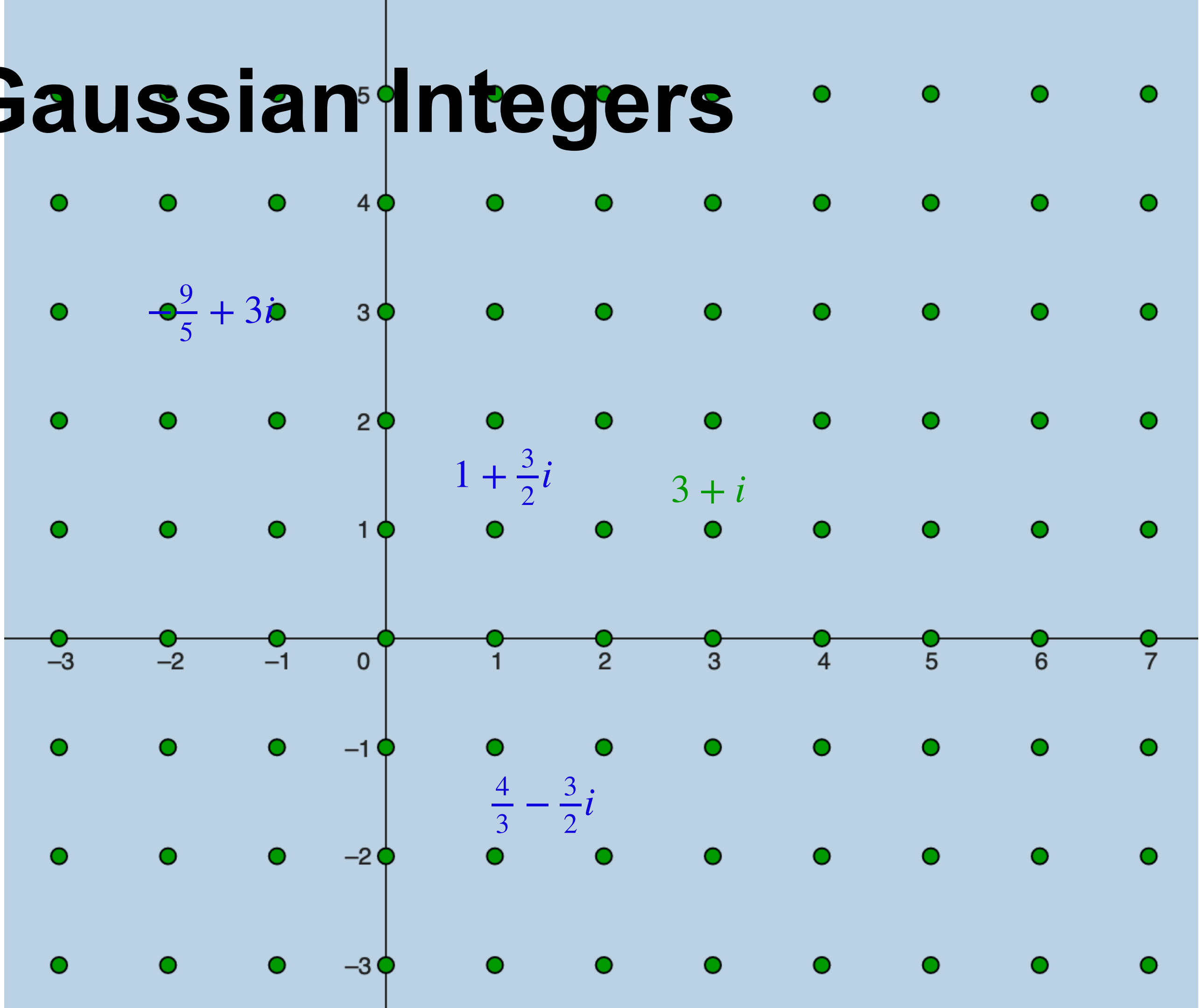
The Gaussian Rationals



$$\mathbb{Q}(i) \subsetneq \cancel{\mathbb{C}}$$

$$i^2 = -1$$

The Gaussian Integers

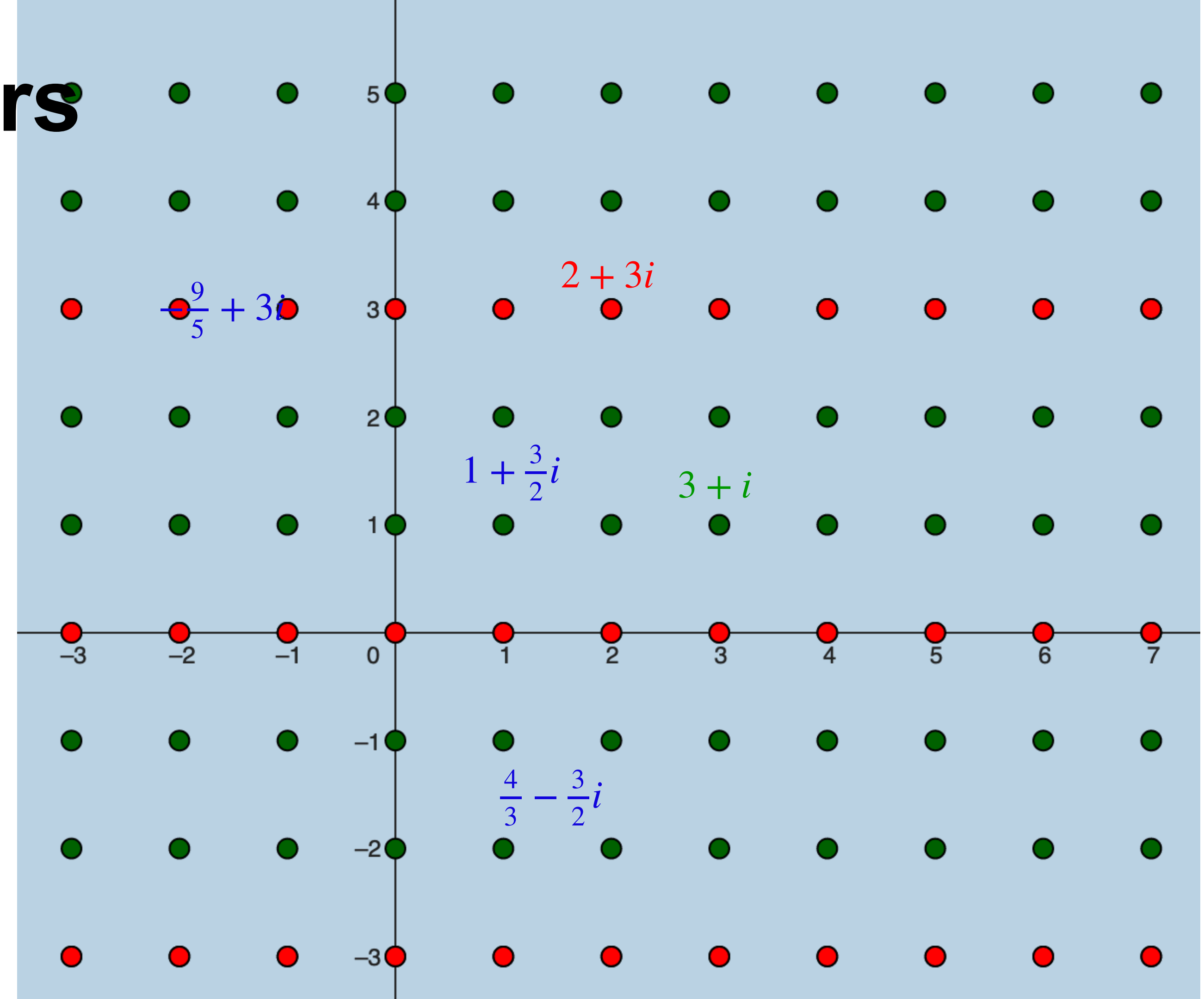


$$\mathbb{Z}[i]$$

$$\mathbb{Q}(i)$$

$$i^2 = -1$$

Orders



$\mathbb{Z}[3i]$

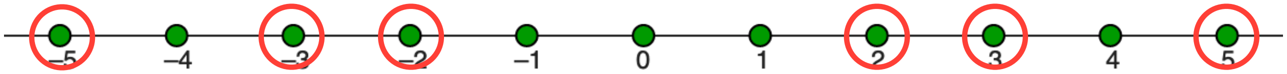
$\mathbb{Z}[i]$

$\mathbb{Q}(i)$

$i^2 = -1$

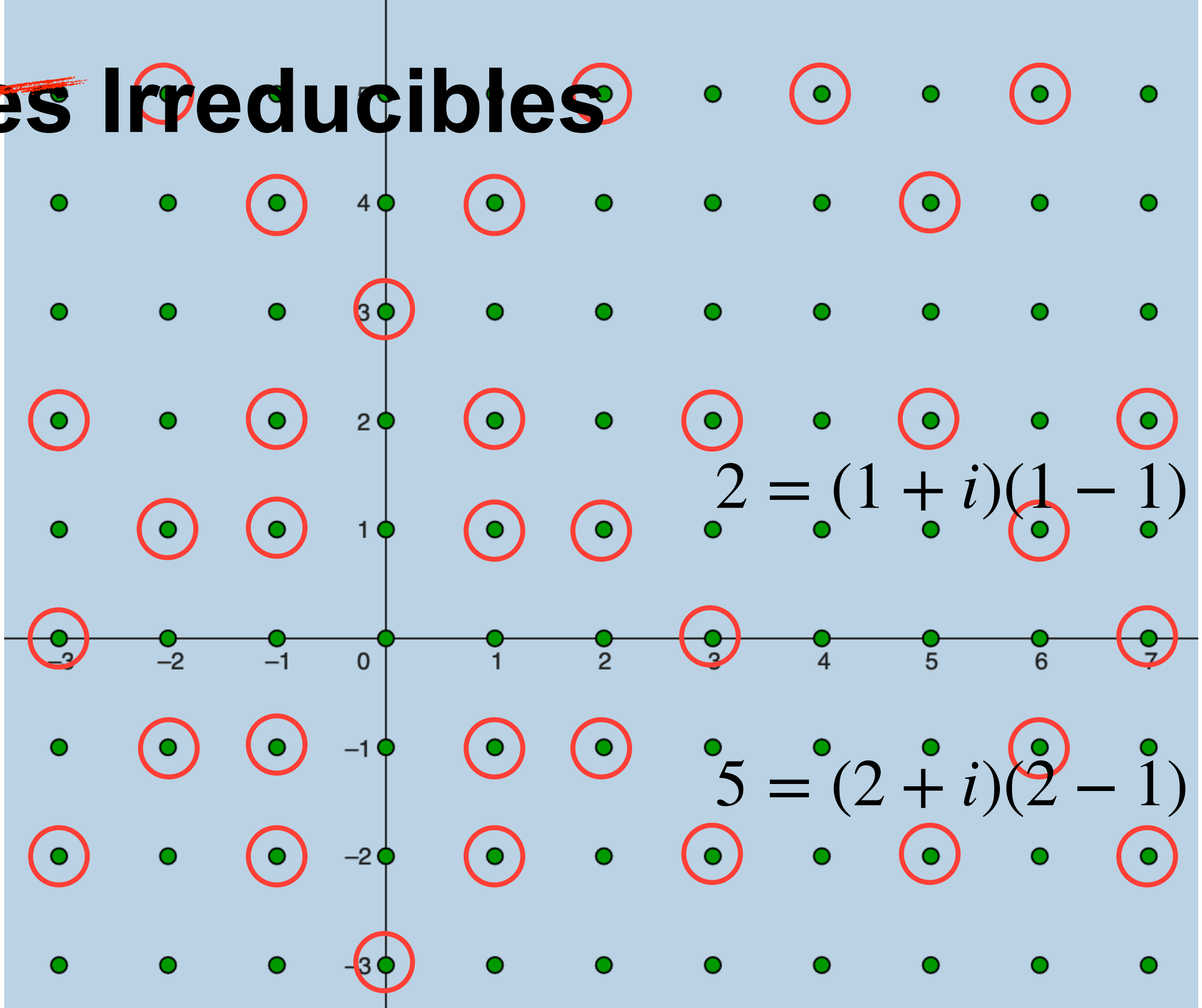
~~Primes~~ Irreducibles

$$\mathbb{Z}$$



Unique way of writing any integer as a product of primes!

~~Primes~~ Irreducibles



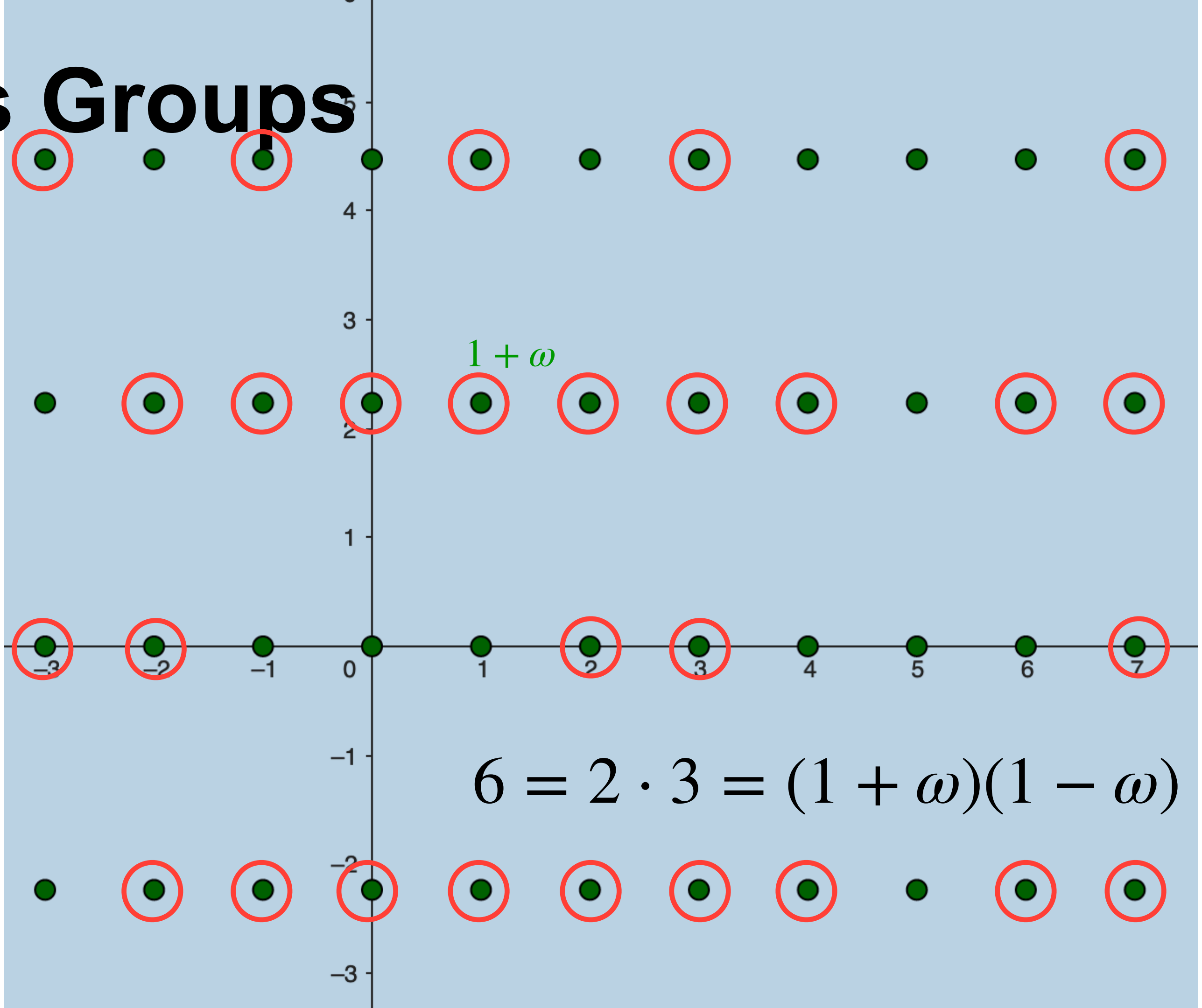
$$2 = (1 + i)(1 - 1)$$

$$5 = (2 + i)(2 - 1)$$

$$\mathbb{Z}[i]$$

$$i^2 = -1$$

Class Groups



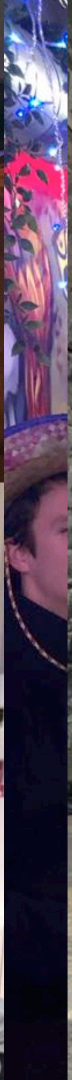
$\mathbb{Z}[\omega]$

$\mathbb{Q}(\omega)$

$\omega^2 = -5$

4.5 years ago...

4.5 years ago...

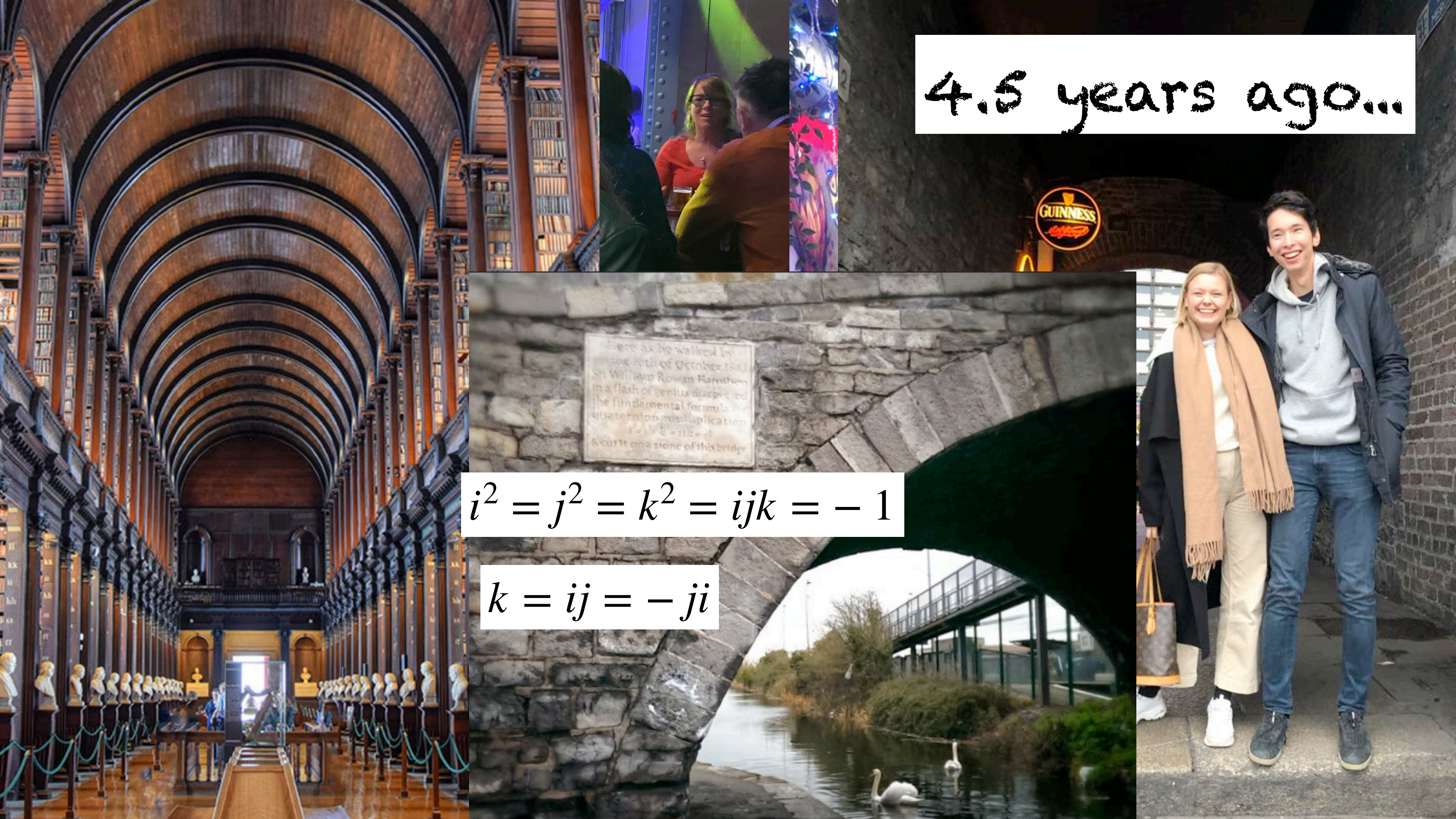



4.5 years ago...
GUINNESS

4.5 years ago...


GUINNESS


as he walked by
of October
Rowan
in a flash of genius
the fundamental formula
quaternion multiplication
& cut it on a stone of this bridge


4.5 years ago...
GUINNESS
Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication
& cut it on a stone of this bridge
$i^2 = j^2 = k^2 = ijk = -1$
$k = ij = -ji$

Quaternion Algebras

$$B_{p,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k \text{ where}$$
$$i^2 = -1, \quad j^2 = -p, \quad k = ij = -ji$$

- Some 4-dimensional thing
- Orders: E.g. $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ (not maximal)
- Typically many maximal orders!

Elliptic Curves

Solutions of

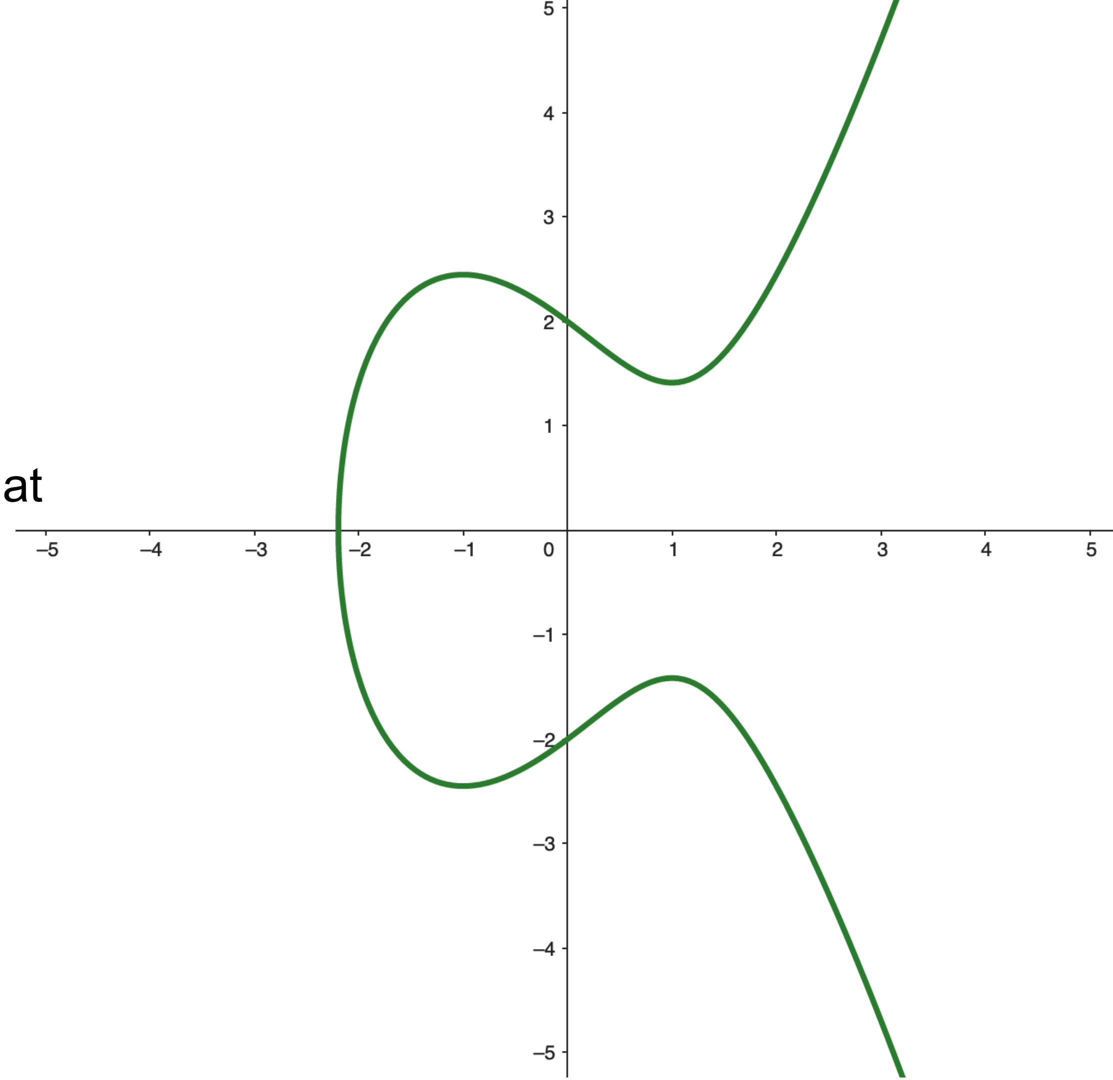
$$y^2 = x^3 + Ax + B$$

Plus an extra point ∞

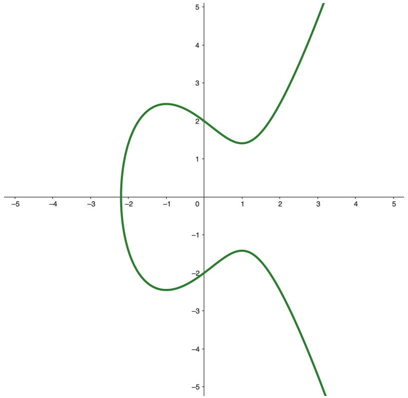
Where A, B are "numbers" such that

$$4A^3 + 27B^2 \neq 0$$

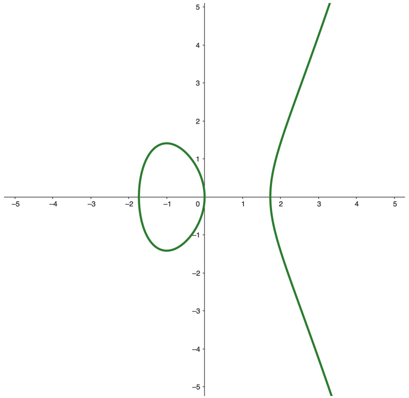
(For us: $A, B \in \mathbb{F}_q$)



Elliptic Curves

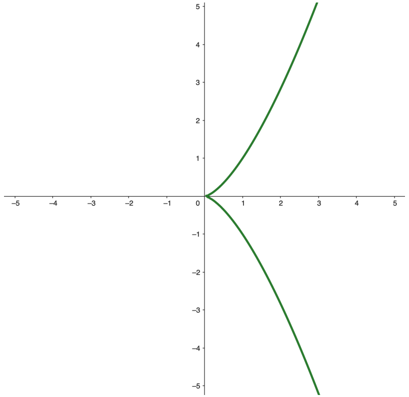


$$y^2 = x^3 - 3x + 4$$



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

Not an elliptic curve

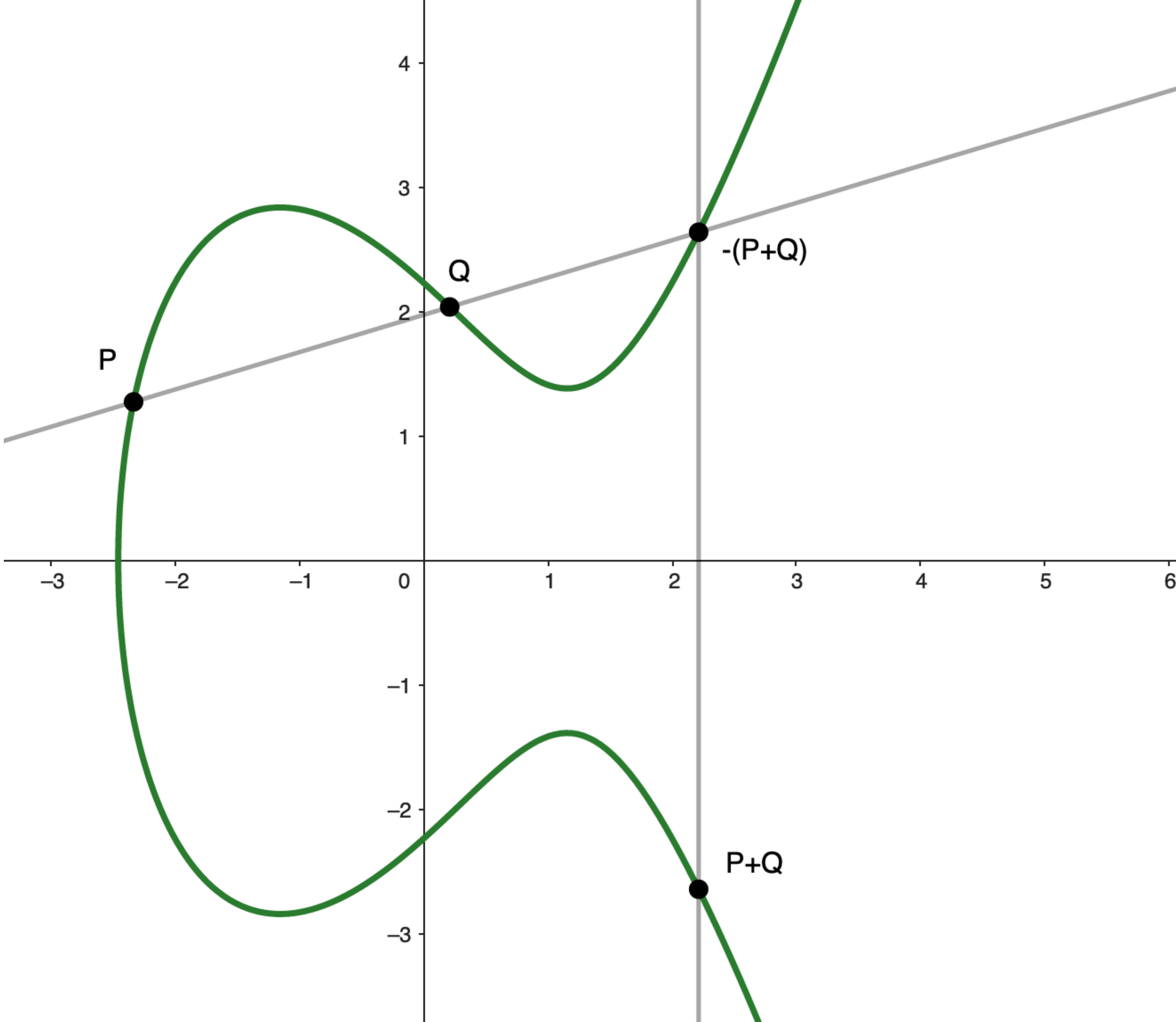


$$y^2 = x^3$$

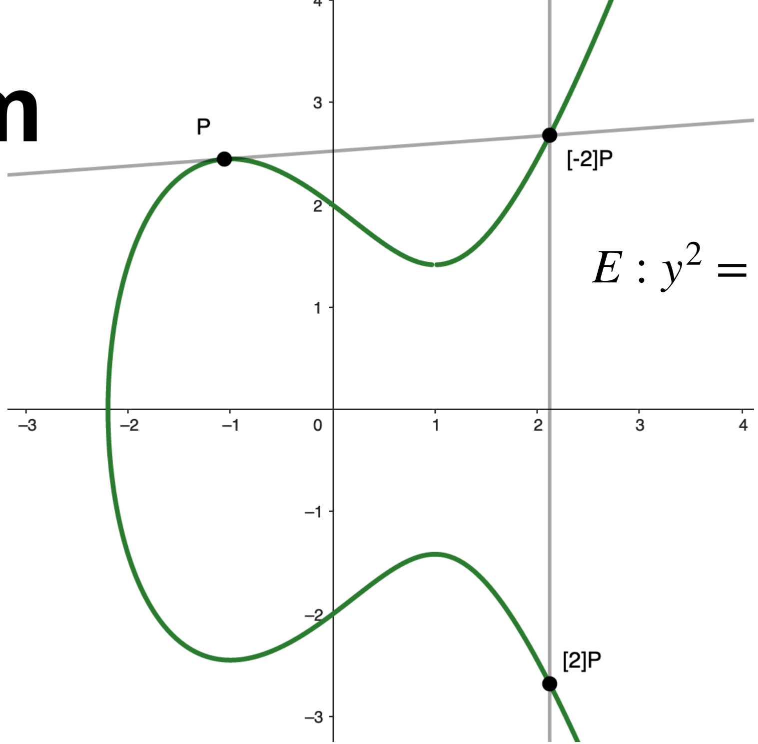
Addition

Points form an abelian group!

I.e. we can "add" points in a meaningful way



Multiplication-by-m



$$E : y^2 = x^3 - 3x + 4$$

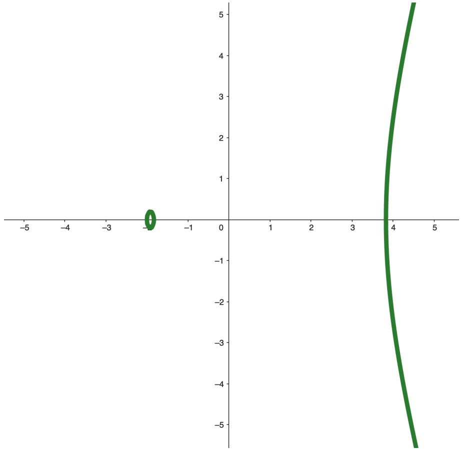
$$[2] : E \to E$$

$$[2]P = P + P$$

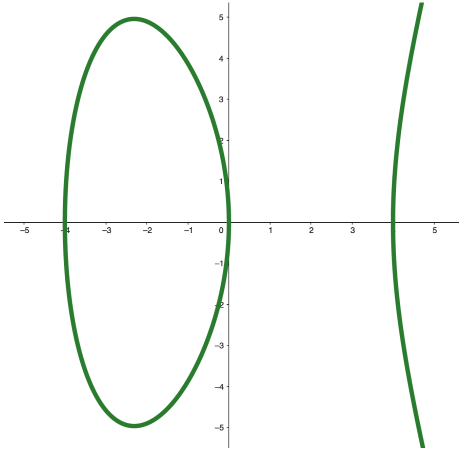
$$[2](x, y) = \left(\frac{1/4x^4 + 3/2x^2 - 8x + 9/4}{x^3 - 3x + 4}, \frac{1/8x^6y - 15/8x^4y + 10x^3y - 45/8x^2y + 6xy - 101/8y}{x^6 - 6x^4 + 8x^3 + 9x^2 - 24x + 16} \right)$$

Isogenies

$\phi :$



$\rightarrow$



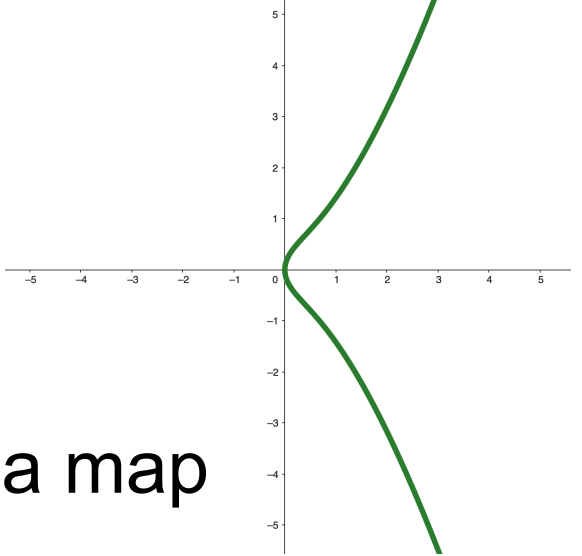
$$y^2 = x^3 - 11x - 14 \qquad\qquad y^2 = x^3 - 16x$$

$$\phi(x, y) = \left(\frac{x^2 + 2x + 1}{x + 2}, \frac{x^2y + 4xy + 3y}{x^2 + 4x + 4} \right)$$

Endomorphisms

- An isogeny $\phi : E \to E$ from a curve to itself
- Can be "added" (point wise):
  - $(\phi + \psi)(P) = \phi(P) + \psi(P)$
- Can be "multiplied" (composition):
  - $(\phi \cdot \psi)(P) = \phi(\psi(P))$
- This gives the **endomorphism ring!**

Example:



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

$$\mathbb{Z} \subseteq \mathrm{End}(E)$$

- For every integer $n \in \mathbb{Z}_{>0}$ there is a map

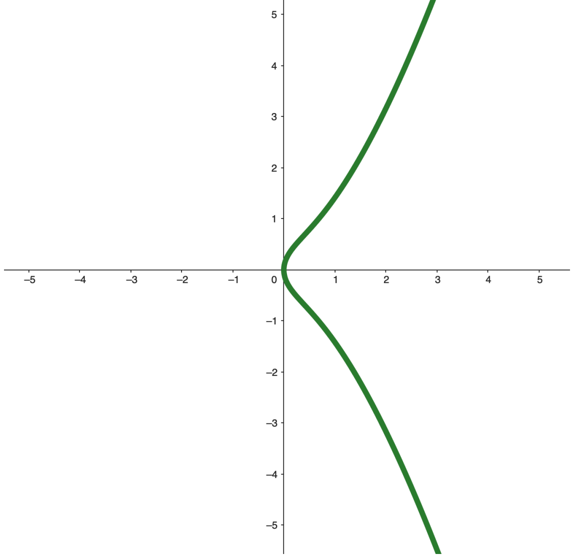
$$[n] : E \to E$$

$$[n]P = \underbrace{P + \ldots + P}_{n}$$

Example:

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

$$\mathbb{Z}[\imath] \subseteq \mathrm{End}(E)$$



- There is another map:

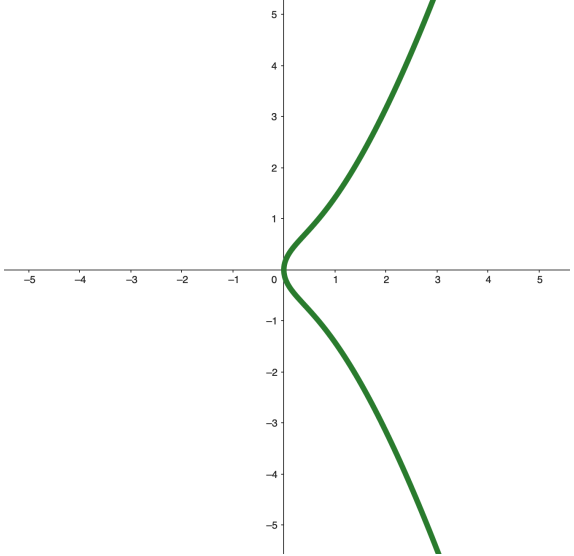
$$\imath : E \to E$$

$$\imath(x, y) = (-x, y\sqrt{-1})$$

- What is $\imath^2$?

$$\imath^2(P) = \imath(\imath(P)) = [-1]P$$

Example:



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

$$\mathbb{Z}\langle \iota, \pi \rangle \subseteq \mathrm{End}(E)$$

- Let $p \equiv 3 \pmod 4$, and let $E/\mathbb{F}_p$

$$\pi : E \to E$$

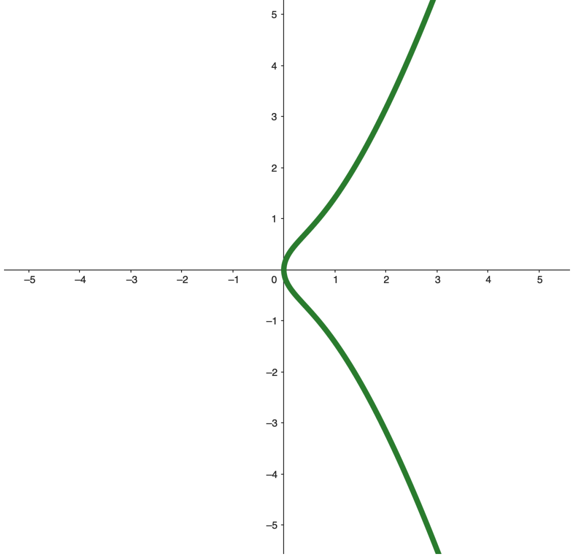
$$\pi(x, y) = (x^p, y^p)$$

$$\pi\iota(P) = [-1]\iota\pi(P) \qquad \pi^2(P) = \pi(\pi(P)) = [-p]P$$

A bit more work: $\mathbb{Z} + \iota\mathbb{Z} + \pi\mathbb{Z} + \iota\pi\mathbb{Z} \subseteq \mathrm{End}(E)$

Example:

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



- Let $p \equiv 3 \pmod 4$, and let $E/\mathbb{F}_p$
- Then $\mathrm{End}(E) = \mathbb{Z} + \iota\mathbb{Z} + \dfrac{\iota + \pi}{2}\mathbb{Z} + \dfrac{1 + \iota\pi}{2}\mathbb{Z}$,

  a maximal order in a quaternion algebra.

Endomorphism Rings Are Orders

- General **theorem:** $\mathrm{End}(E)$ is either:
  - $\mathbb{Z}$
  - An imaginary quadratic order (e.g. $\mathbb{Z}[i]$)
  - A maximal order in a quaternion algebra

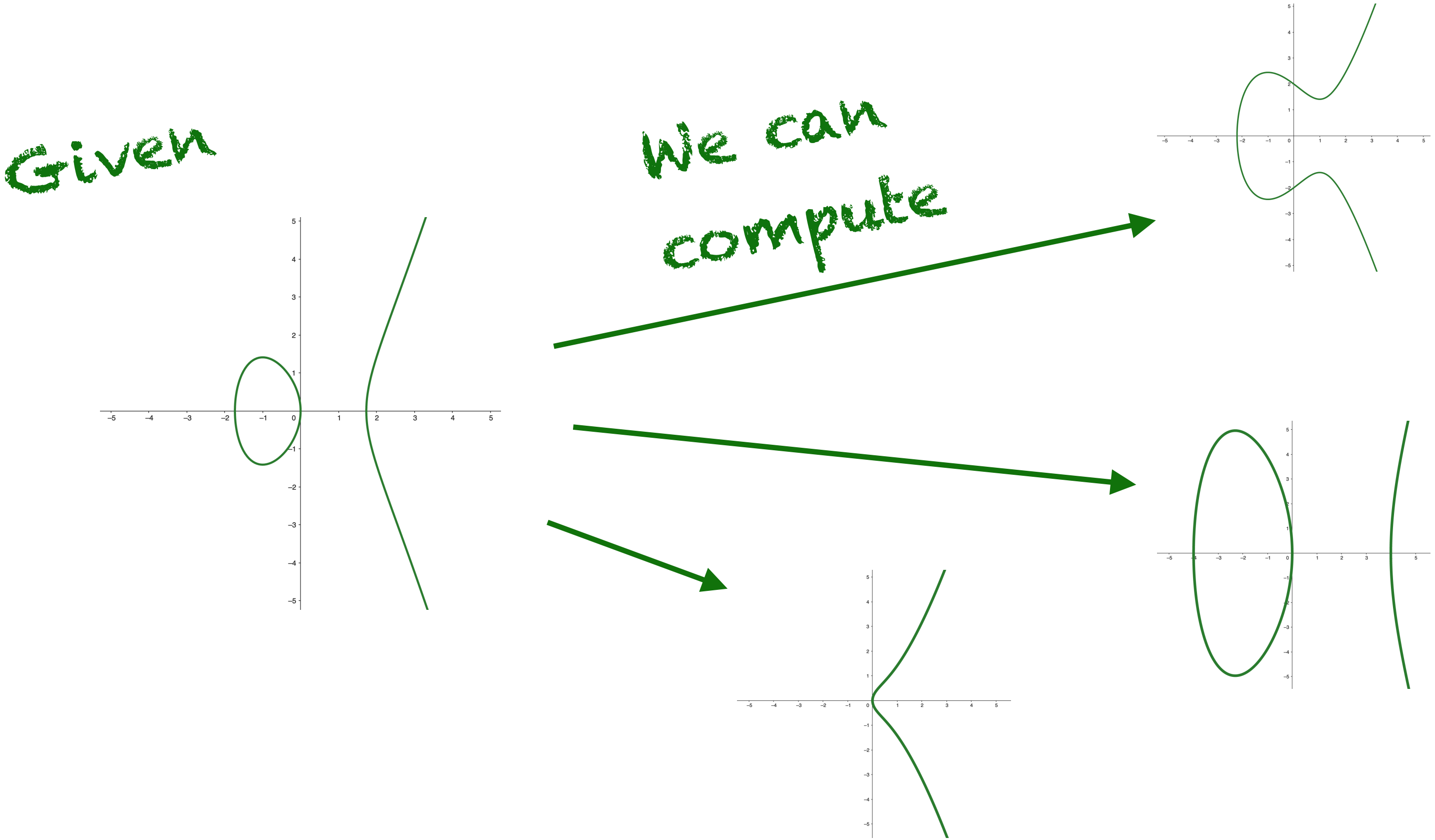
Ordinary

Supersingular

The Deuring Correspondence

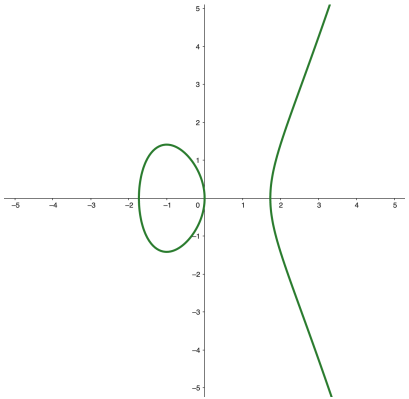
- This is only the beginning!
- Supersingular case:
  exact correspondence
  ideals ⇔ isogenies
- Almost exact correspondence
  SS. curves ⇔ Maximal orders

Hard problems for cryptography

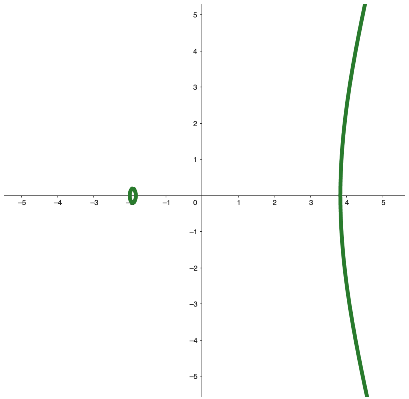


Hard problems for cryptography

Given

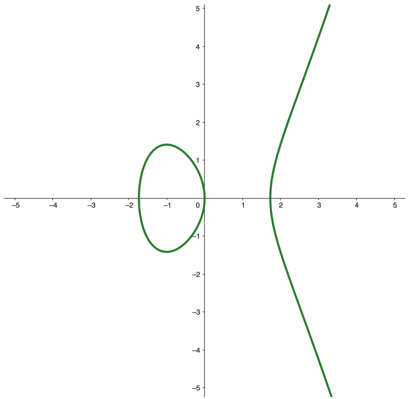


And



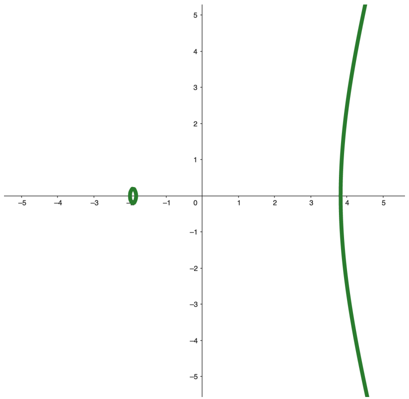
Hard problems for cryptography

Given



Seems hard to compute

And



The isogeny problem ⇔ The endomorphism ring problem

Part 2:
The Constructive Deuring Correspondence

Efficiently computing the easy way of the Deuring correspondence,
and cryptographic applications

Deuring for the People:

Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic

Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková and Mattia Veroni

Motivation

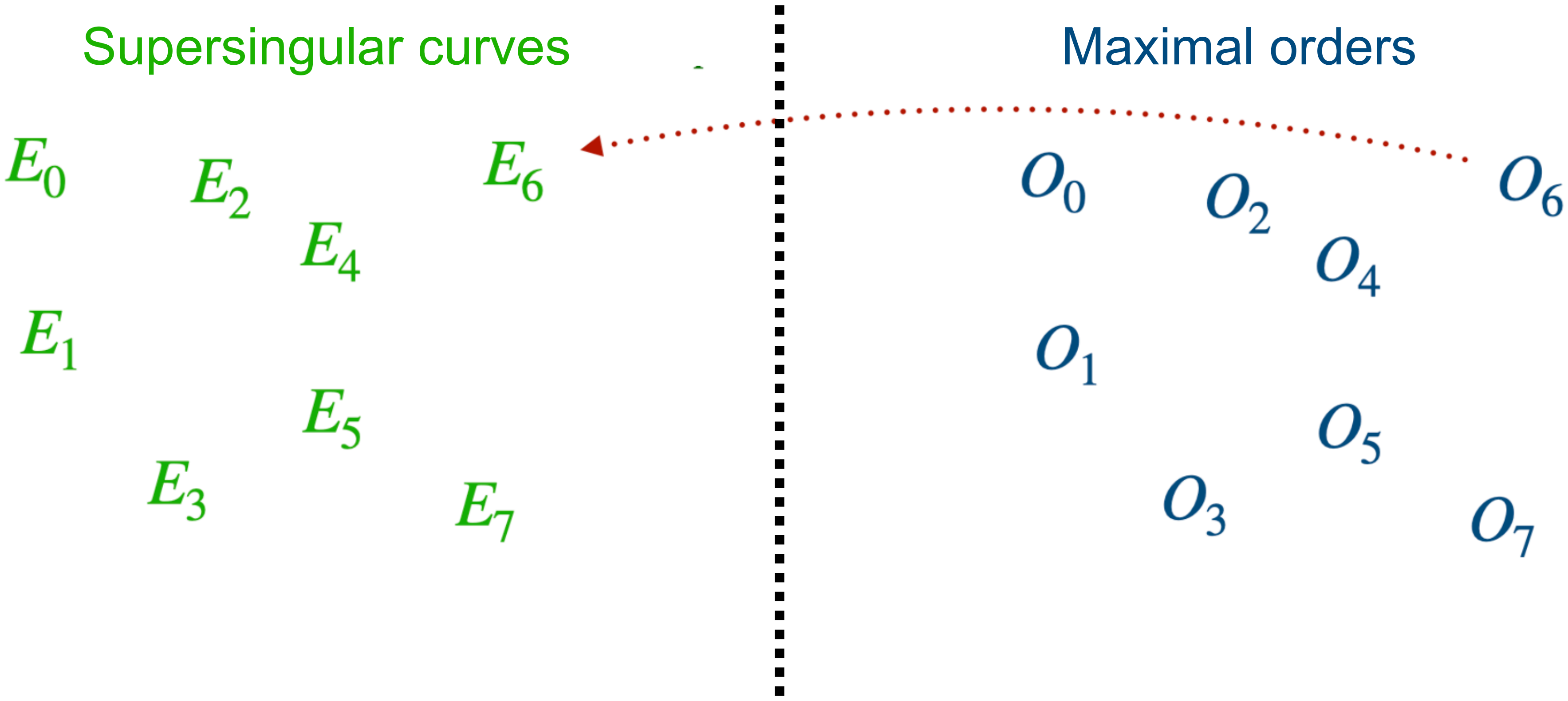
$$E \xrightarrow{\text{Hard}} \mathcal{O}$$

$$E \xleftarrow{\text{"Easy"}} \mathcal{O}$$

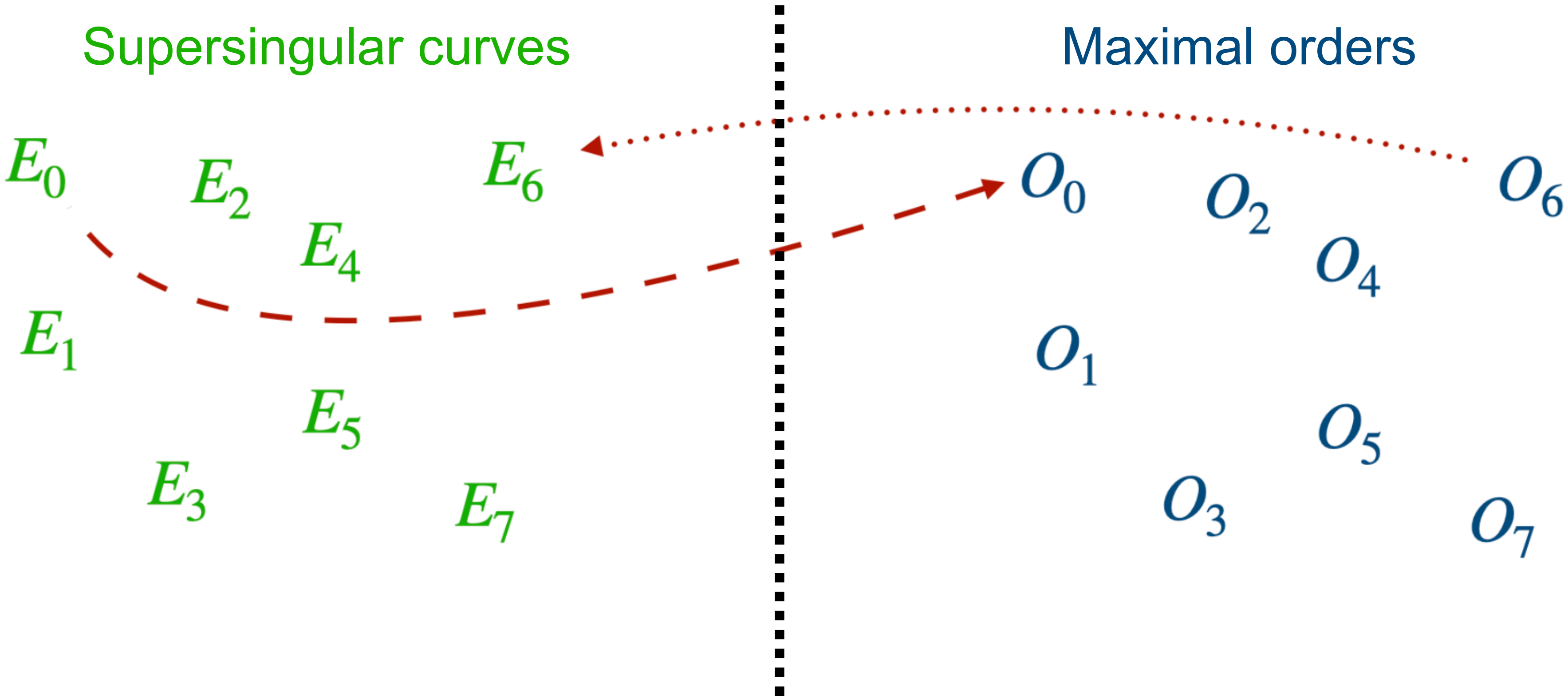
"Easy" = Polynomial time

- SQIsign: Efficient by carefully choosing p
- Should work for any p
  - Previous attempts: Up to $p \sim 30$ bits

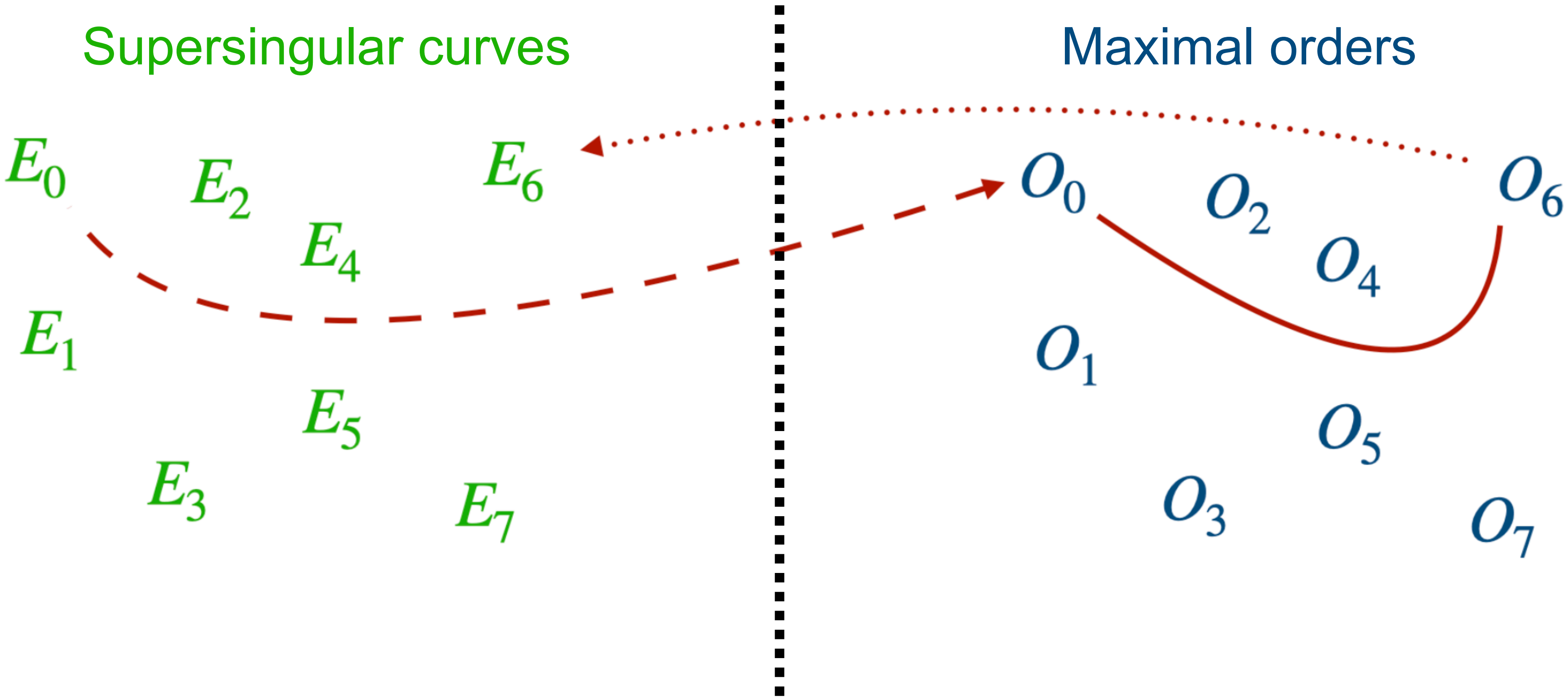
Algorithm: Task



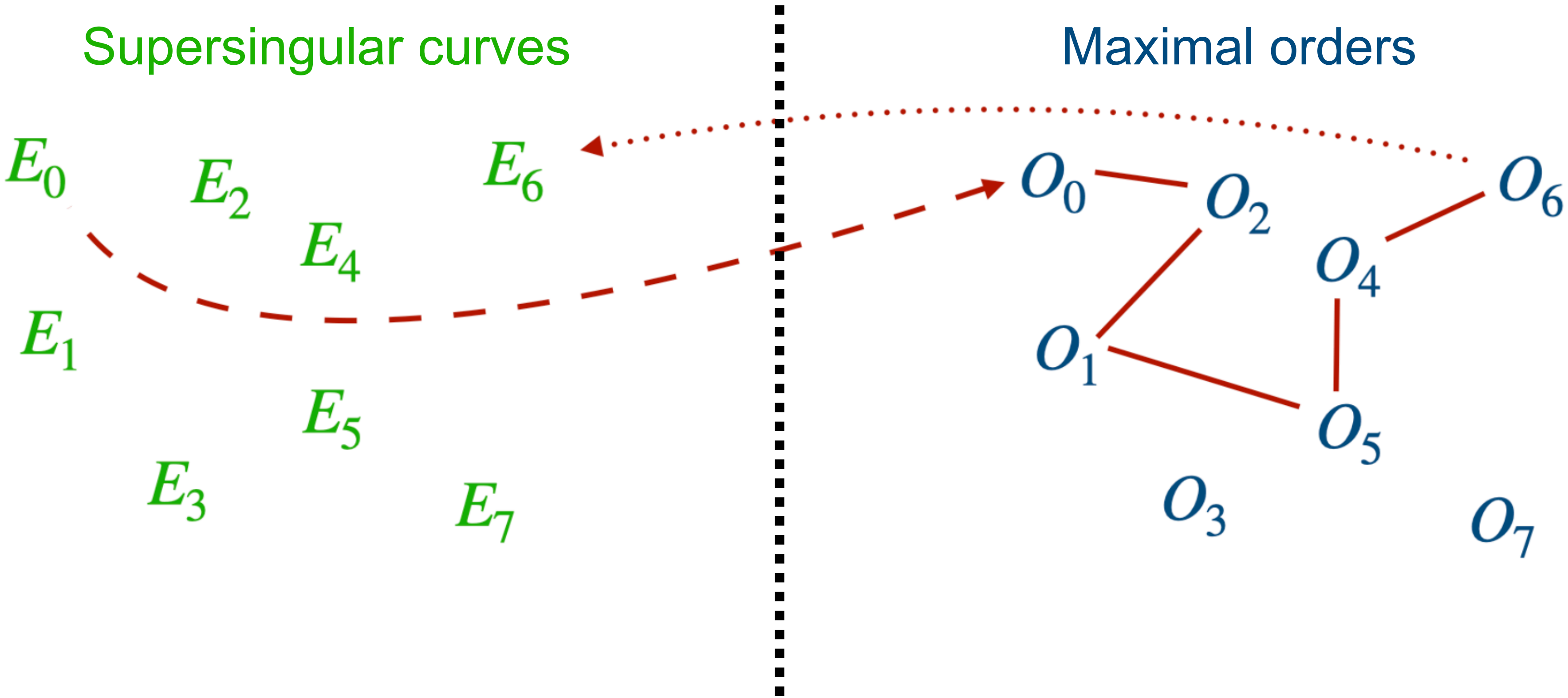
Algorithm: Fix Base Curve



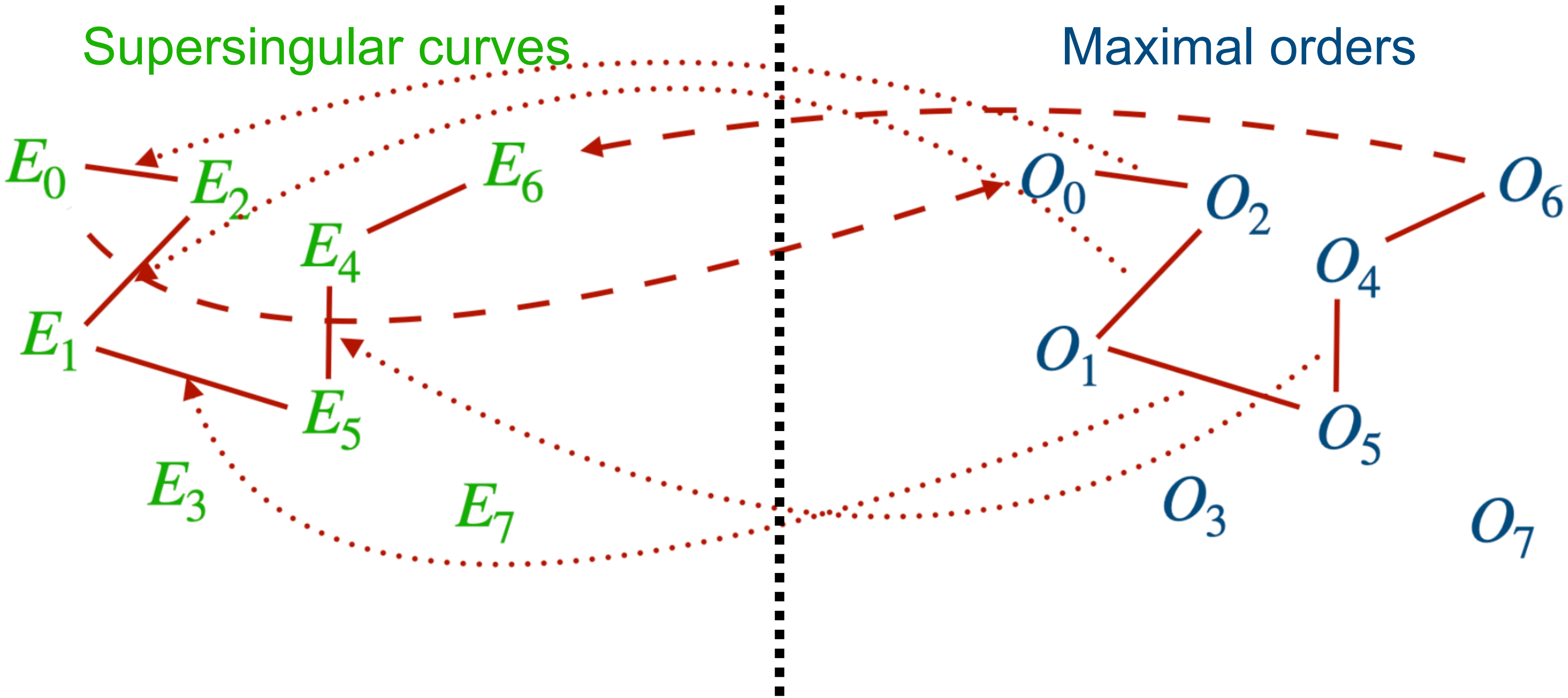
Algorithm: Solve on Quaternion Side



Algorithm: KLPT (!!!!)



Algorithm: Translate Back



Optimisations, and Results

- **Choose output norm of KLPT based on prime**
- **Combine known results**, and **optimise** the way to give a starting curve with known endomorphism ring in **any** characteristic p
- **Faster** computation of isogenies generated by points in **field-extensions**

Result: Can compute the Deuring correspondence for characteristic of any reasonable size, i.e. thousands of bits.

Cryptographic Smooth Neighbors

Giacomo Bruno, Maria Corte-Real Santos, Craig Costello, Jonathan Komada Eriksen, Michael Meyer, Michael Naehrig, and Bruno Sterner

AprèsSQI:

Extra Fast Verification for SQIsign Using Extension-Field Signing

Maria Corte-Real Santos, Jonathan Komada Eriksen, Michael Meyer, and Krijn Reijnders

Part 3:
Oriented Endomorphism Rings

Optimal Embeddings and Primitive Orientations

Optimal Embeddings

$$i^2 = -1, \quad j^2 = -p, \quad k = ij = -ji$$

Quaternion orders: $\mathcal{O}$ (e.g. $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$)

Imaginary Quadratic Orders: $\mathfrak{O}$ (e.g. $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$)

$$\mathfrak{O} \subset \mathcal{O}$$

Optimal Embeddings

$$i^2 = -1, \quad j^2 = -p, \quad k = ij = -ji$$

Quaternion orders: $\mathcal{O}$ (e.g. $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$)

Imaginary Quadratic Orders: $\mathfrak{O}$ (e.g. $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$)

(Optimal) embedding

$$\iota : \mathfrak{O} \hookrightarrow \mathcal{O}$$

$$\iota\left(\sqrt{-1}\right) = i$$

(Not optimal for $\mathfrak{O} = \mathbb{Z}[3\sqrt{-1}]$)

Primitive Orientations

$$i^2 = -1, \quad j^2 = -p, \quad k = ij = -ji$$

Quaternion orders: $\mathcal{O}$ (e.g. $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$)

Imaginary Quadratic Orders: $\mathfrak{O}$ (e.g. $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$)

(Optimal) embedding

$$\iota : \mathfrak{O} \hookrightarrow \cancel{\mathcal{O}}\,\mathrm{End}(E)$$

$$\iota\left(\sqrt{-1}\right) = i$$

(Not optimal for $\mathfrak{O} = \mathbb{Z}[3\sqrt{-1}]$)

Class Group Actions and Volcanoes

Through the orientation

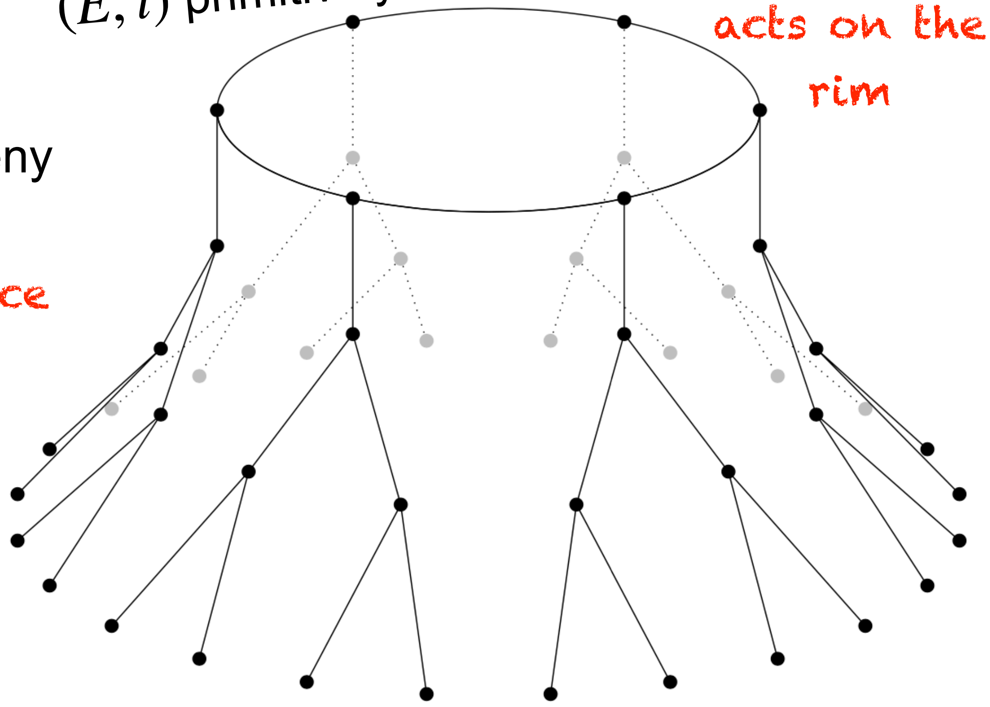
Im. Q. Ideal $\Rightarrow$ Quat. Ideal $\Leftrightarrow$ Isogeny

Deuring correspondence

$Cl(\mathfrak{O})$ acts free and (almost) transitively on curves prim. oriented by $\mathfrak{O}$

(E, ι) primitively oriented

Class group acts on the rim



Computing Orientations from the Endomorphism Ring of Supersingular Curves and Applications

Jonathan Komada Eriksen and Antonin Leroux

Generalized Class Group Actions on Oriented Elliptic Curves with Level Structure

Sarah Arpin, Wouter Castryck, Jonathan Komada Eriksen, Gioella Lorenzon and Fréderik Vercauteren

PEARL-SCALLOP:

Parameter Extension Applicable in Real Life for SCALLOP

Bill Allombert, Márton Tot Bagi, Jean-françois Biasse, Jonathan Komada Eriksen, Péter Kutas, Chris Leonardi, Aurel Page and Renate Scheidler

Motivation and Summary

Can do "Diffie-Hellman" on primitively oriented curves!

Public

Secret $a \in \mathbb{Z}$

$[a]P$

Secret

$b \in \mathbb{Z}$

$[b]P$

$[a][b]P$

$[b][a]P$

Motivation and Summary

Can do "Diffie-Hellman" on primitively oriented curves!

Public

Secret $\mathfrak{a} \in Cl(\mathfrak{O})$ $\xrightarrow{\mathfrak{a} \star (E, \iota)}$ $\mathfrak{b} \in Cl(\mathfrak{O})$ Secret

$\mathfrak{a} \star \mathfrak{b} \star (E, \iota)$ $\xleftarrow{\mathfrak{b} \star (E, \iota)}$

$\mathfrak{a} \star \mathfrak{b} \star (E, \iota)$ $\qquad$ $\mathfrak{b} \star \mathfrak{a} \star (E, \iota)$

Motivation and Summary

Can do "Diffie-Hellman" on primitively oriented curves!

Secret $\mathfrak{a} \in Cl(\mathfrak{O})$

Public

$\mathfrak{a} \star (E, \iota)$

Secret $\mathfrak{b} \in Cl(\mathfrak{O})$

$\mathfrak{b} \star (E, \iota)$

$\mathfrak{a} \star \mathfrak{b} \star (E, \iota)$

$\mathfrak{b} \star \mathfrak{a} \star (E, \iota)$

CSIDH

+ Fast*

- Don't know class group

SCALLOP

- Slooooooow

- Do know class group

Comparison

	SCALLOP	SCALLOP-HD	PEARL-SCALLOP
Instantiate higher security levels	NO	YES	Yes, with some effort
Transfer orientation	Complicated	Easy	Easy
$\iota(\omega)$	$\prod_i \ell_i$	$(2^e, 2^e)$-isogeny	2^e-isogeny

Thank you

Appendix: A bit more on each paper

Cryptographic Smooth Neighbors

Giacomo Bruno, Maria Corte-Real Santos, Craig Costello, Jonathan Komada Eriksen, Michael Meyer, Michael Naehrig, and Bruno Sterner

Motivation and Summary

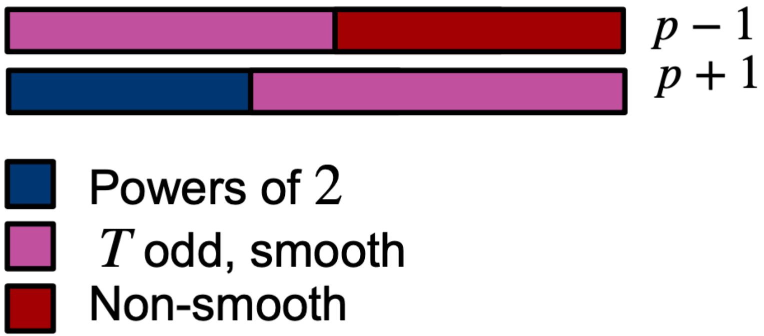
Application: SQIsign

KLPT: Need a "nice" $T > p^{\cancel{3}\ 5/4}$

- T should be a product of small primes
- Every $\ell^r \mid T$ should also satisfy $\ell^r \mid p^{2k} - 1$ for small k

When designing protocols we get to pick p!

$2^f \mid p+1$ $T \mid p^2 - 1$



This paper: Find p such that

$2^f T \mid p^2 - 1$ for "nice" T

How to find nice primes?

Observation: $a - X \in \mathbb{Q}[X]/f(X)$, where $f(X) = X^2 + bX + c$ satisfies

$$N(a - X) = f(a)$$

Roughly, "size" of element

Step 1: Find all $a - X \in \mathbb{Z}[X]/f(X)$, with $N(a - X) < B$
Step 2: Keep multiplying such elements until no more are found

Result: $a \in \mathbb{Z}$ such that no prime factor of $f(a)$ is bigger than B

Results:

Example: Found

$$\alpha = 80240624836977330528483315920954987 51$$

with

$$\alpha^2 - 1 = 2^{10} \cdot 3^2 \cdot 5^4 \cdot 7 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 29 \cdot 31^2 \cdot 41 \cdot 43^2 \cdot 47^2 \cdot 83^2 \cdot 103^2 \cdot 109 \cdot 163 \cdot 173 \cdot 239 \cdot 241^2 \cdot 271 \cdot 283 \cdot 311^2 \cdot 479^2 \cdot 499 \cdot 509 \cdot 523^2$$

Not useful for protocols yet

Simple trick: Given $(r, r+1)$ twin smooth, try $p = 2r^n - 1$

Found lots of primes useful for SQIsign

Caveat: No real way of controlling power of 2

AprèsSQI:

Extra Fast Verification for SQIsign Using Extension-Field Signing

Maria Corte-Real Santos, Jonathan Komada Eriksen, Michael Meyer, and Krijn Reijnders

NTNU | Norwegian University of Science and Technology

Motivation and Summary

Lessons:

Cryptographic Smooth Neighbors

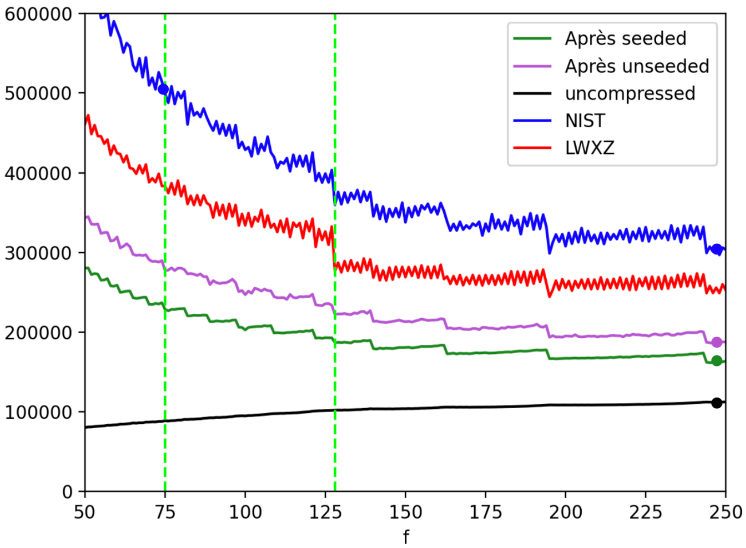
- The nicest SQIsign primes are still pretty bad...
- Working over extension fields is okay! Deuring for the People

Corresponds to allowing $\ell^e \mid p^{2k} - 1$ where $k > 1$

Result: We give a version of SQIsign with significantly faster verification, and comparable signing.

Why it works

Recall: $2^f \mid p+1$



- Increasing f:
  - 1.68x faster
- Optimised:
  - 2.65x faster
- Seeded (+10 B)
  - 3.04x faster
- Uncomp. (2x B)
  - 4.40x faster

- Larger f from using extension fields.
- Signing still okay:
  - DftP tricks
  - Most expensive stuff can be done as pre-computation
  - Larger f also helps signing

Computing Orientations from the Endomorphism Ring of Supersingular Curves and Applications

Jonathan Komada Eriksen and Antonin Leroux

Motivation and Summary

Problem: Given $\mathfrak{O}$ and $\mathcal{O}$ compute an optimal embedding $\iota : \mathfrak{O} \hookrightarrow \mathcal{O}$

$$\Leftrightarrow aX^2 + bY^2 + cZ^2 + eXY + fXZ + gYZ = d$$

History: First solvable when $d < p^{1/2}$

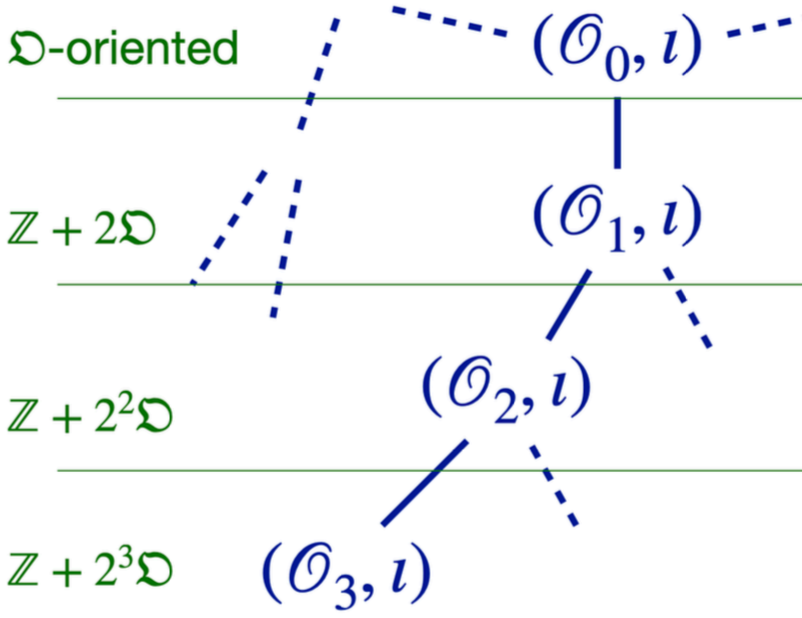
Later improved to $d < p$

Result: Many improvements to this (e.g. solving for $d < p^{4/3}$).

Further, we connect the theory to isogeny-problems.

Applications:

- Greatly simplify and generalise:
  Vectorisation -> EndRing
- Computing isogenies of fixed degree d.
  - Recall, KLPT: when $d > p^3$
    What about $p^{1/2} < d < p^3$?
  - We solve for $d < p^{2/3}$



(IMO) One of the most important open questions in isogeny-based crypto

Generalized Class Group Actions on Oriented Elliptic Curves with Level Structure

Sarah Arpin, Wouter Castryck, Jonathan Komada Eriksen, Gioella Lorenzon and Fréderik Vercauteren

NTNU | Norwegian University of Science and Technology

Motivation and Summary

Admittedly, this talk has not covered enough background to go through this paper in this short time

Recall: $Cl(\mathfrak{O})$ acts freely and transitively on primitively $\mathfrak{O}$-oriented curves

Result: A generalisation of this classical result

	Group		**Acting on set**
Classic	$Cl(\mathfrak{O}) := I(\mathfrak{O})/P(\mathfrak{O})$	$\longleftrightarrow$	(E, ι)
NEW!	Generalised class groups: Replace $P(\mathfrak{O})$ by a smaller subgroup	$\longleftrightarrow$	(E, Γ, ι), extra information of Γ-level structure.

Technique

Lemma: Let $\mathfrak{O} \hookrightarrow \mathrm{End}(E)$ or $\mathfrak{O} = \mathrm{End}(E)$.
Then $\mathfrak{O}/\mathfrak{m} \cong E[\mathfrak{m}]$ as $\mathfrak{O}$-modules for ideals $\mathfrak{m} \subset \mathfrak{O}$
(under certain conditions* on $\mathfrak{m}$)

* Proper, and coprime to characteristic p of underlying field (of E) is sufficient

Main ideal: The isomorphism above allows us to connect
gen. class groups $\Leftrightarrow H < GL(\mathfrak{O}/\mathfrak{m}) \Leftrightarrow \Gamma$-level structures