BENJAMIN
WESOLOWSKI

GENERATING SUBGROUPS OF RAY CLASS GROUPS with small prime ideals

AT ANTS-XIII, MADISON, WI,USA, ON THE 19/07/2018 BY BENJAMIN WESOLOWSKI, EPFL, LAUSANNE, SWITZERLAND

NOTE

The entire talk assumes the extended Riemann hypothesis

1 GENERATING CLASS GROUPS

RAY CLASS GROUPS

- Let K be a number field, with ring of integers $\mathcal{O}_K$

RAY CLASS GROUPS

- Let K be a number field, with ring of integers $\mathcal{O}_K$
- The class group $\mathrm{Cl}(K)$ is the quotient

$$\mathcal{I}(K) \;/\; P(K) = (\text{ideals in } \mathcal{O}_K) \;/\; (\text{principal ideals})$$

RAY CLASS GROUPS

- Let K be a number field, with ring of integers $\mathcal{O}_K$
- The class group $\mathrm{Cl}(K)$ is the quotient

$$\mathcal{I}(K) \,/\, P(K) = (\text{ideals in } \mathcal{O}_K) \,/\, (\text{principal ideals})$$

- More generally any order $\mathcal{O}$ in K has a class group $\mathrm{Cl}(\mathcal{O})$

RAY CLASS GROUPS

- Let K be a number field, with ring of integers $\mathcal{O}_K$
- The class group $\mathrm{Cl}(K)$ is the quotient

$$\mathcal{I}(K) \,/\, P(K) = (\text{ideals in } \mathcal{O}_K) \,/\, (\text{principal ideals})$$

- More generally any order $\mathcal{O}$ in K has a class group $\mathrm{Cl}(\mathcal{O})$
- All these are ray class groups (or quotients thereof)

RAY CLASS GROUPS

- Let K be a number field, with ring of integers $\mathcal{O}_K$
- The class group $\mathrm{Cl}(K)$ is the quotient

$$\mathcal{I}(K) / P(K) = (\text{ideals in } \mathcal{O}_K) / (\text{principal ideals})$$

- More generally any order $\mathcal{O}$ in K has a class group $\mathrm{Cl}(\mathcal{O})$
- All these are ray class groups (or quotients thereof)
- Fix a modulus $\mathfrak{m}$ (essentially an ideal of $\mathcal{O}_K$). The **$\mathfrak{m}$-ray class group** $\mathrm{Cl}_{\mathfrak{m}}(K)$ is the quotient

$$\mathcal{I}_{\mathfrak{m}}(K) / P_{\mathfrak{m}}(K) = (\text{ideals in } \mathcal{O}_K \text{ coprime to } \mathfrak{m}) / (\text{some principal ideals})$$

GENERATING RAY CLASS GROUPS

- Given an ideal $\mathfrak{a}$ coprime to $\mathfrak{m}$, we write $[\mathfrak{a}]_{\mathfrak{m}}$ for the class of $\mathfrak{a}$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$

GENERATING RAY CLASS GROUPS

- Given an ideal $\mathfrak{a}$ coprime to $\mathfrak{m}$, we write $[\mathfrak{a}]_{\mathfrak{m}}$ for the class of $\mathfrak{a}$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$

- Fix a bound $B > 0$, consider the set of classes of "small" prime ideals

$$S = \{[\mathfrak{p}]_{\mathfrak{m}} \mid \mathfrak{p} \text{ an ideal of prime norm}, (\mathfrak{p}, \mathfrak{m}) = 1, N(\mathfrak{p}) < B\}$$

GENERATING RAY CLASS GROUPS

- Given an ideal $\mathfrak{a}$ coprime to $\mathfrak{m}$, we write $[\mathfrak{a}]_{\mathfrak{m}}$ for the class of $\mathfrak{a}$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$
- Fix a bound $B > 0$, consider the set of classes of "small" prime ideals

$$S = \{[\mathfrak{p}]_{\mathfrak{m}} \mid \mathfrak{p} \text{ an ideal of prime norm}, (\mathfrak{p}, \mathfrak{m}) = 1, N(\mathfrak{p}) < B\}$$

- For which bound B does S generate $\mathrm{Cl}_{\mathfrak{m}}(K)$?

GENERATING RAY CLASS GROUPS

- Given an ideal $\mathfrak{a}$ coprime to $\mathfrak{m}$, we write $[\mathfrak{a}]_{\mathfrak{m}}$ for the class of $\mathfrak{a}$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$
- Fix a bound $B > 0$, consider the set of classes of "small" prime ideals

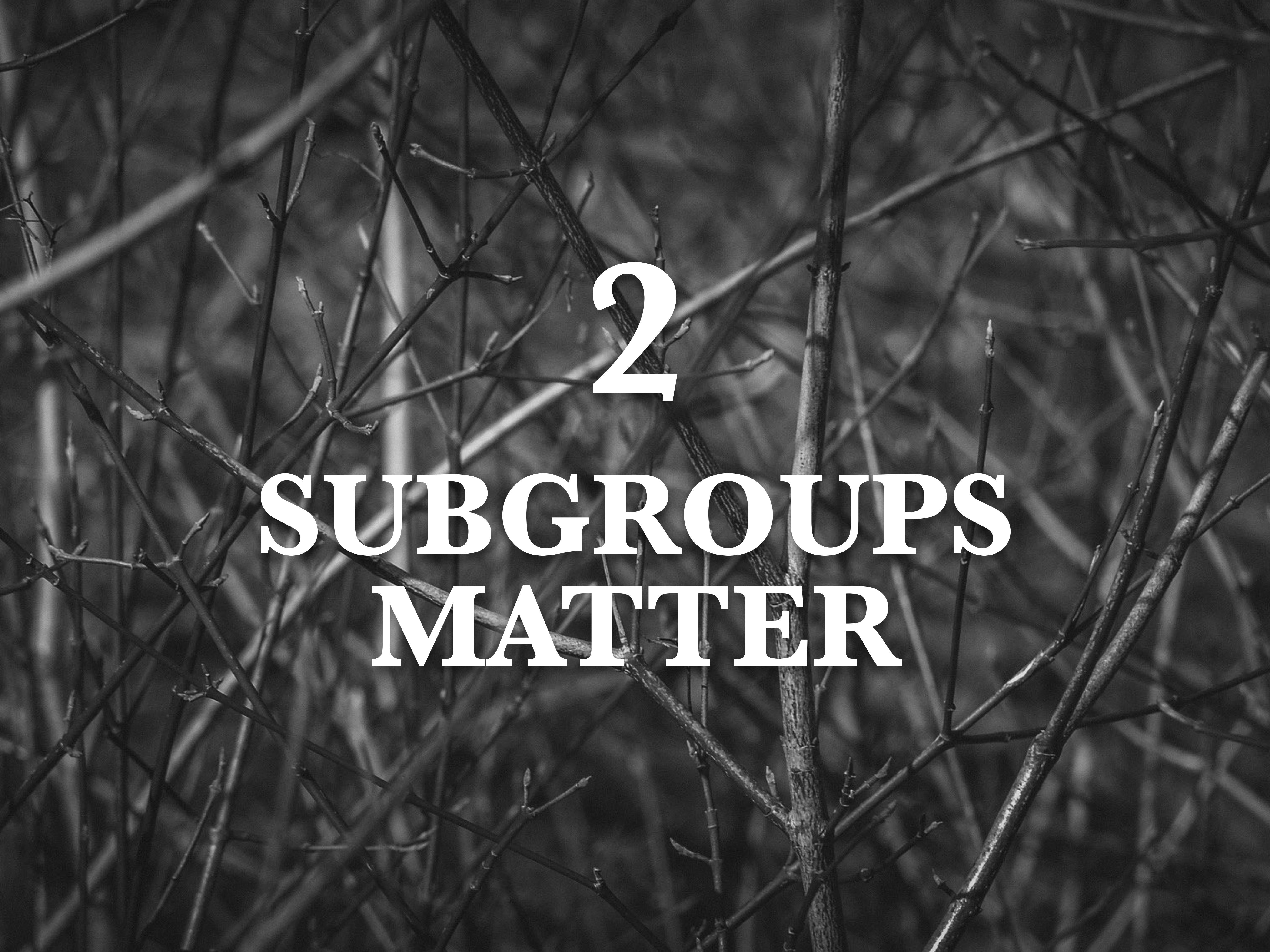
$$S = \{[\mathfrak{p}]_{\mathfrak{m}} \mid \mathfrak{p} \text{ an ideal of prime norm}, (\mathfrak{p}, \mathfrak{m}) = 1, N(\mathfrak{p}) < B\}$$

- For which bound B does S generate $\mathrm{Cl}_{\mathfrak{m}}(K)$?
- Answer from [Bach90]: $B = 18 \log(\mathrm{Disc}(K)^2 N(\mathfrak{m}))^2$ works!

[Bach90] Eric Bach. *Explicit bounds for primality testing and related problems*, Mathematics of Computation, 1990.

GENERATING SUBGROUPS OF RAY CLASS GROUPS

- What if we want generators of a **subgroup** of $\mathrm{Cl}_{\mathfrak{m}}(K)$, are small prime ideals still sufficient?



2

SUBGROUPS MATTER

WHY SUBGROUPS OF RAY CLASS GROUPS

Some applications need generators of subgroups. We give two examples

WHY SUBGROUPS OF RAY CLASS GROUPS

Some applications need generators of subgroups. We give two examples

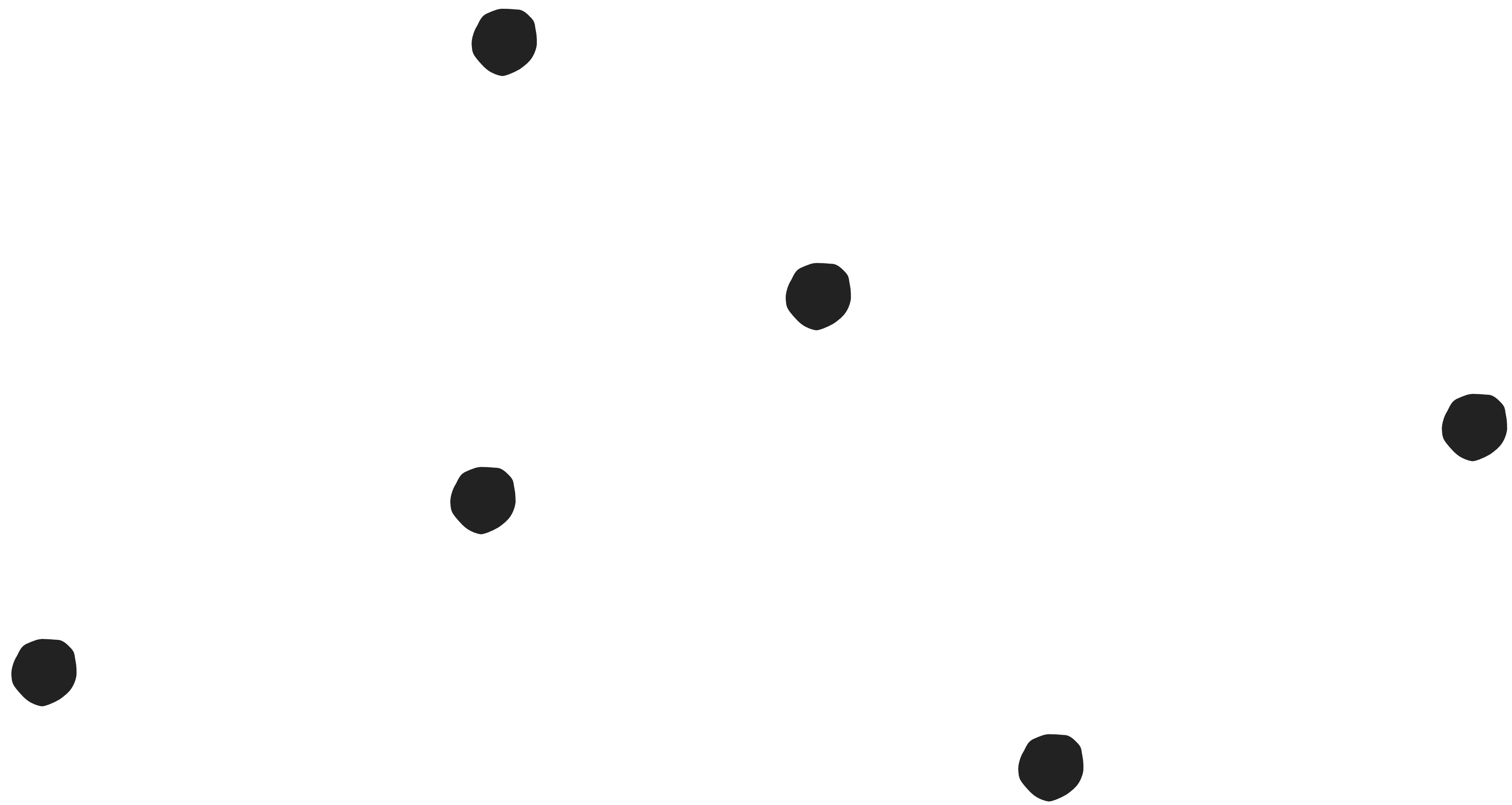
- Bounds on degrees of computable isogenies to get connected isogeny graphs

WHY SUBGROUPS OF RAY CLASS GROUPS

Some applications need generators of subgroups. We give two examples

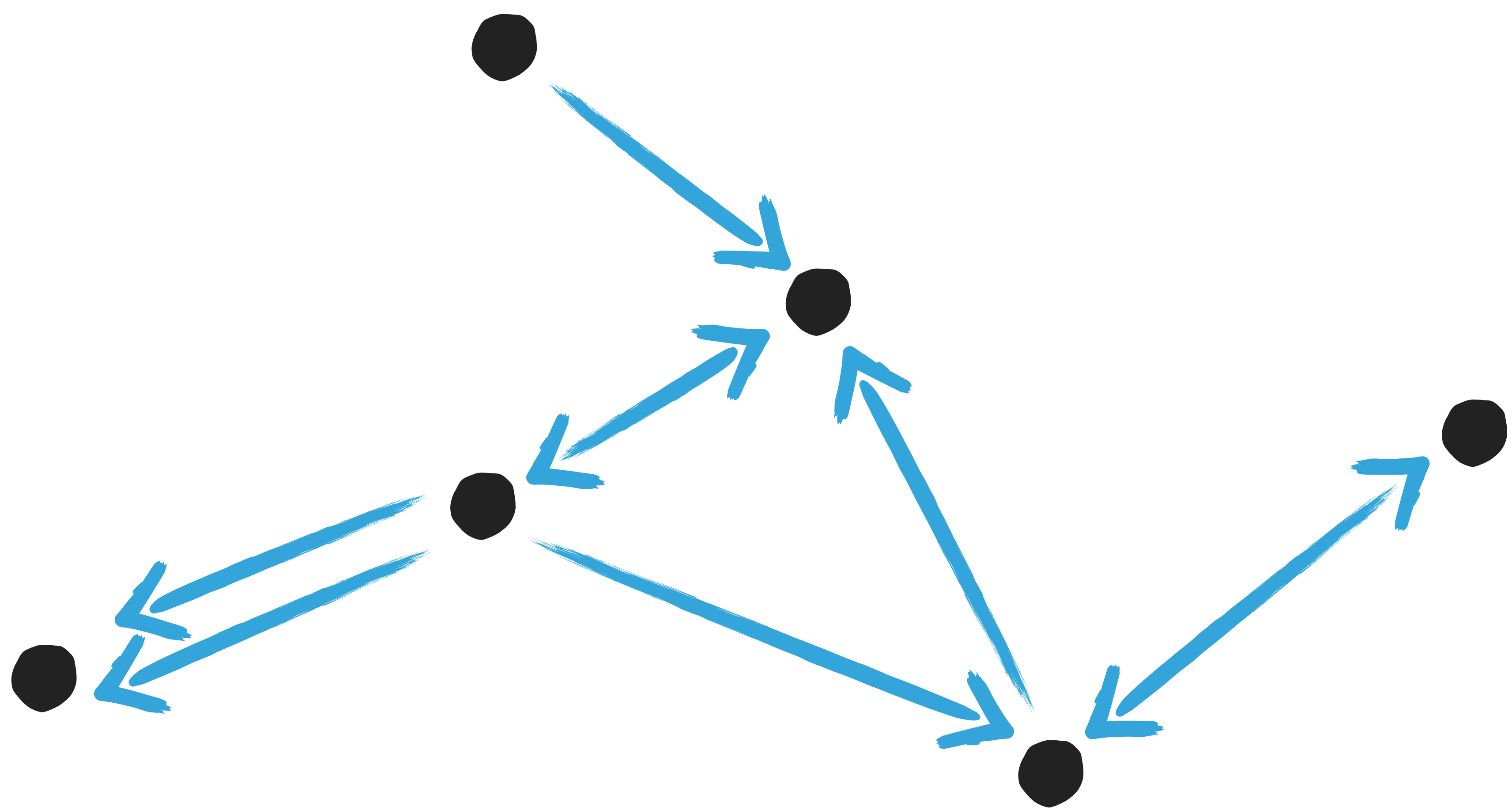
- Bounds on degrees of computable isogenies to get connected isogeny graphs
- An algorithm to find short vectors in cyclotomic ideal lattices

WHAT IS AN ISOGENY GRAPH?



Vertices represent abelian varieties (up to isomorphism)

WHAT IS AN ISOGENY GRAPH?



Vertices represent abelian varieties (up to isomorphism)

Edges represent isogenies between them

CONNECTED ISOGENY GRAPHS

- Consider an ordinary, absolutely simple abelian variety A over a finite field

CONNECTED ISOGENY GRAPHS

- Consider an ordinary, absolutely simple abelian variety A over a finite field
- Its endomorphism ring $\mathrm{End}(A)$ is an order in a number field of degree $2\dim(A)$

CONNECTED ISOGENY GRAPHS

- Consider an ordinary, absolutely simple abelian variety A over a finite field
- Its endomorphism ring End(A) is an order in a number field of degree 2dim(A)
- A **horizontal isogeny** is an isogeny $A \longrightarrow A'$ such that End(A) = End(A')

CONNECTED ISOGENY GRAPHS

- Consider an ordinary, absolutely simple abelian variety A over a finite field
- Its endomorphism ring End(A) is an order in a number field of degree 2dim(A)
- A **horizontal isogeny** is an isogeny $A \longrightarrow A'$ such that End(A) = End(A')
- Let Hor(A) be the set of abelian varieties isogenous to A with same endomorphism ring

CONNECTED ISOGENY GRAPHS

- Consider an ordinary, absolutely simple abelian variety A over a finite field
- Its endomorphism ring End(A) is an order in a number field of degree 2dim(A)
- A **horizontal isogeny** is an isogeny $A \longrightarrow A'$ such that End(A) = End(A')
- Let Hor(A) be the set of abelian varieties isogenous to A with same endomorphism ring
- For any invertible ideal $\mathfrak{l}$ in End(A), the isogeny $A \longrightarrow A/A[\mathfrak{l}]$ is horizontal, of degree $N(\mathfrak{l})$

CONNECTED ISOGENY GRAPHS

Graph with vertices $\mathrm{Hor}(A)$, and edges isogenies of prime norm at most B	$\cong$	Cayley graph of $\mathrm{Cl}(\mathrm{End}(A))$, with generators the ideals of prime norm at most B

CONNECTED ISOGENY GRAPHS

Graph with vertices Hor(A), and edges isogenies of prime norm at most B	$\cong$	Cayley graph of Cl(End(A)), with generators the ideals of prime norm at most B

If End(A) is Gorenstein

CONNECTED ISOGENY GRAPHS

- We can only compute isogenies between **principally polarisable** abelian varieties

CONNECTED ISOGENY GRAPHS

- We can only compute isogenies between **principally polarisable** abelian varieties
- They correspond to a subgroup of $\mathrm{Cl}(\mathrm{End}(A))$, and the corresponding subgraph of the Cayley graph

CONNECTED ISOGENY GRAPHS

- We can only compute isogenies between **principally polarisable** abelian varieties
- They correspond to a subgroup of Cl(End(A)), and the corresponding subgraph of the Cayley graph
- Bound B on the degree of isogenies to get a connected graph where the isogenies can be computed?

ISOGENY GRAPHS TO STUDY THE DLP

Isogeny graphs are a central tool for studying the DLP

- Galbraith, Hess, and Smart, *Extending the GHS Weil descent attack*, EUROCRYPT 2002
- Jao, Miller, and Venkatesan, *Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?*, ASIACRYPT 2005
- Smith, *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*, EUROCRYPT 2008
- Jetchev and Wesolowski, *Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem* (preprint)

SVP IN CYCLOTOMIC IDEAL LATTICES

- A typical choice of lattices for lattice-based cryptographic schemes: ideals in a cyclotomic field K (seen as lattices via the Minkowski embedding)

SVP IN CYCLOTOMIC IDEAL LATTICES

- A typical choice of lattices for lattice-based cryptographic schemes: ideals in a cyclotomic field K (seen as lattices via the Minkowski embedding)
- Security based on difficulty of finding short vectors in lattice

SVP IN CYCLOTOMIC IDEAL LATTICES

- A typical choice of lattices for lattice-based cryptographic schemes: ideals in a cyclotomic field K (seen as lattices via the Minkowski embedding)
- Security based on difficulty of finding short vectors in lattice
- It was shown how to heuristically find unusually short vectors in **principal ideals** in quantum polynomial time [CDPR16]

[CDPR16] R. Cramer, L. Ducas, C. Peikert, and O. Regev. *Recovering short generators of principal ideals in cyclotomic rings*, EUROCRYPT 2016.

SVP IN CYCLOTOMIC IDEAL LATTICES

- A typical choice of lattices for lattice-based cryptographic schemes: ideals in a cyclotomic field K (seen as lattices via the Minkowski embedding)
- Security based on difficulty of finding short vectors in lattice
- It was shown how to heuristically find unusually short vectors in **principal ideals** in quantum polynomial time [CDPR16]
- Recently extended to **arbitrary ideals**, by transferring the problem to a principal ideal [CDW17]

[CDPR16] R. Cramer, L. Ducas, C. Peikert, and O. Regev. *Recovering short generators of principal ideals in cyclotomic rings*, EUROCRYPT 2016.

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski. *Short Stickelberger class relations and applications to Ideal-SVP*, EUROCRYPT 2017.

SVP IN CYCLOTOMIC IDEAL LATTICES

- Recently extended to **arbitrary ideals**, by transferring the problem to a principal ideal [CDW17]
- The transferring assumes the **relative class group** is generated by a small number of small prime ideals

$$\mathrm{Cl}^{-}(K) = \ker(\mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(K_0))$$

SVP IN CYCLOTOMIC IDEAL LATTICES

- Recently extended to **arbitrary ideals**, by transferring the problem to a principal ideal [CDW17]
- The transferring assumes the **relative class group** is generated by a small number of small prime ideals

$$\mathrm{Cl}^{-}(K) = \ker(\mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(K_0))$$

K_0 is the maximal real subfield of K

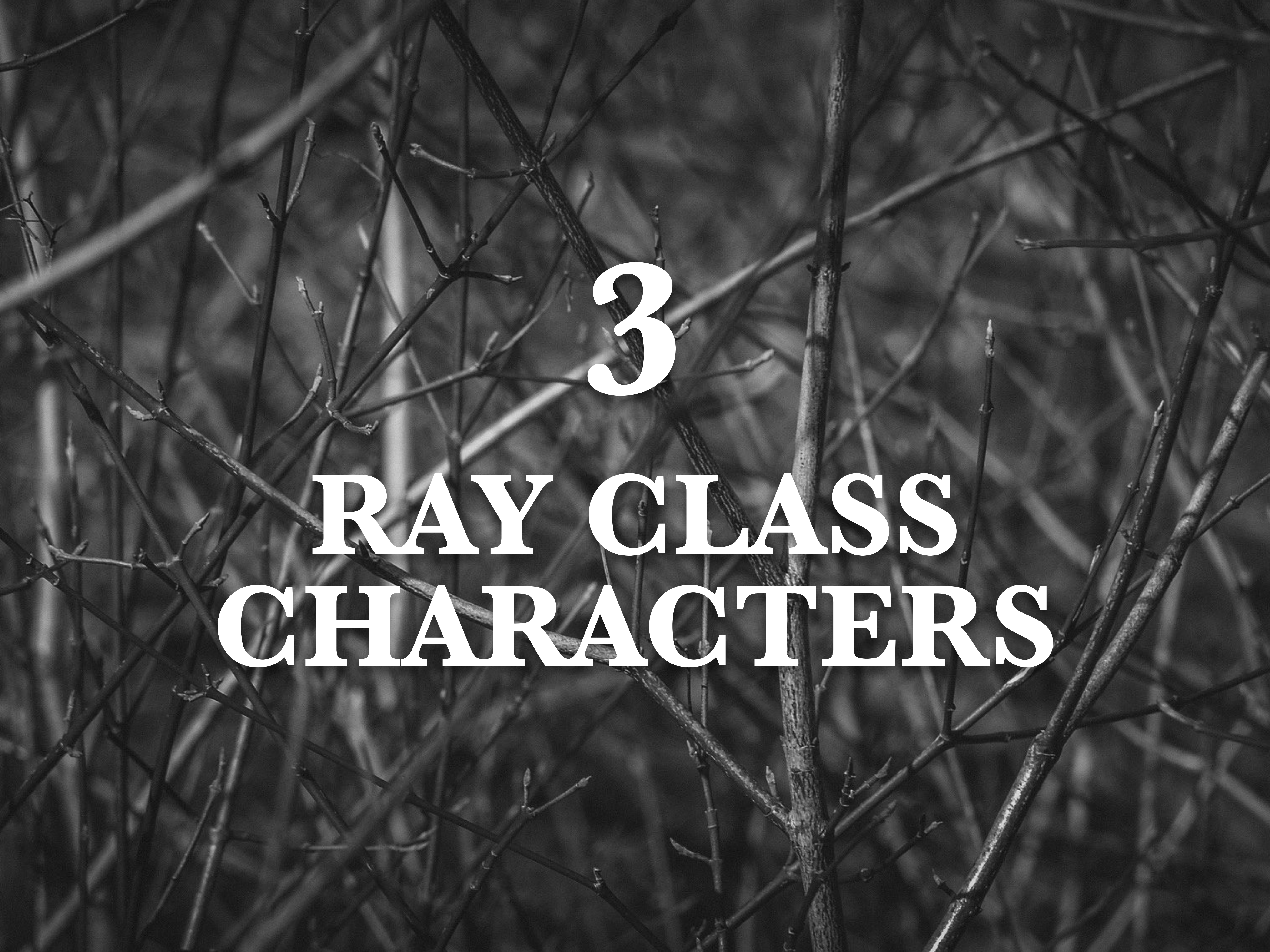
SVP IN CYCLOTOMIC IDEAL LATTICES

- Recently extended to **arbitrary ideals**, by transferring the problem to a principal ideal [CDW17]
- The transferring assumes the **relative class group** is generated by a small number of small prime ideals

$$\mathrm{Cl}^{-}(K) = \ker(\mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(K_0))$$

= the relative class group, a subgroup of Cl(K)

K_0 is the maximal real subfield of K



3

RAY CLASS CHARACTERS

MAIN THEOREM

Theorem: Let H be any subgroup of $\mathrm{Cl}_{\mathfrak{m}}(K)$, and consider a character $\chi\colon \mathrm{Cl}_{\mathfrak{m}}(K) \longrightarrow \mathbb{C}^\times$ that is not trivial on H. Then, there is an ideal $\mathfrak{p}$ such that

- $N(\mathfrak{p})$ is prime,
- $(\mathfrak{p}, \mathfrak{m}) = 1$,
- $[\mathfrak{p}]_{\mathfrak{m}} \in H$,
- $\chi(\mathfrak{p}) \neq 1$,
- $N(\mathfrak{p}) \leq ([\mathrm{Cl}_{\mathfrak{m}}(K) : H]\,(2.71 \log(\mathrm{Disc}(K)\, N(\mathfrak{m})) + 1.29\, |\mathfrak{m}_\infty|$
  $+ 1.38\, \omega(\mathfrak{m})) + 4.13)^2$

This bound is $O\big([\mathrm{Cl}_{\mathfrak{m}}(K) : H]^2 \log(\mathrm{Disc}(K)\, N(\mathfrak{m}))^2 \big)$

MAIN THEOREM

- Proof uses analytic methods similar to [Bach90]
- Play with characters of $\mathrm{Cl}_{\mathfrak{m}}(K)/H$ to account for the extra condition that the ideals to consider are in the subgroup H

MAIN THEOREM IMPLIES SMALL GENERATORS

- Let S be the set of all ideals $\mathfrak{p}$ of prime norm smaller than the bound B from the theorem, and such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$

MAIN THEOREM IMPLIES SMALL GENERATORS

- Let S be the set of all ideals $\mathfrak{p}$ of prime norm smaller than the bound B from the theorem, and such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$
- Suppose S generates a subgroup $N \neq H$

MAIN THEOREM IMPLIES SMALL GENERATORS

- Let S be the set of all ideals $\mathfrak{p}$ of prime norm smaller than the bound B from the theorem, and such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$
- Suppose S generates a subgroup $N \neq H$
- There is a non-trivial character of H that is trivial on N

MAIN THEOREM IMPLIES SMALL GENERATORS

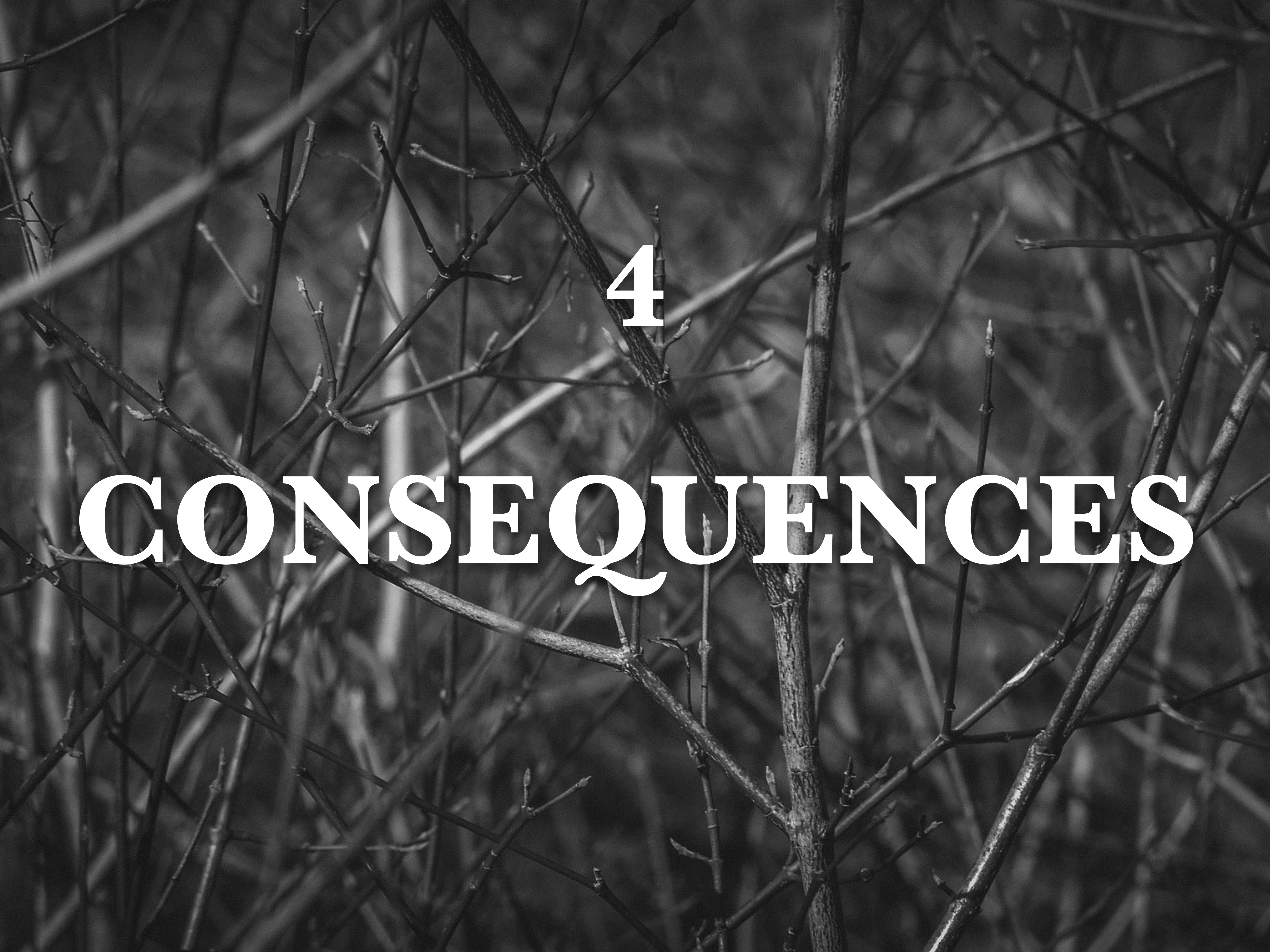
- Let S be the set of all ideals $\mathfrak{p}$ of prime norm smaller than the bound B from the theorem, and such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$
- Suppose S generates a subgroup $N \neq H$
- There is a non-trivial character of H that is trivial on N
- This character extends to a character $\chi\colon \mathrm{Cl}_{\mathfrak{m}}(K) \longrightarrow \mathbb{C}^{\times}$ that is not trivial on H

MAIN THEOREM IMPLIES SMALL GENERATORS

- Let S be the set of all ideals $\mathfrak{p}$ of prime norm smaller than the bound B from the theorem, and such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$
- Suppose S generates a subgroup $N \neq H$
- There is a non-trivial character of H that is trivial on N
- This character extends to a character $\chi\colon \mathrm{Cl}_{\mathfrak{m}}(K) \longrightarrow \mathbb{C}^\times$ that is not trivial on H
- From the theorem, there is an ideal $\mathfrak{p}$ in S such that $\chi(\mathfrak{p}) \neq 1$

MAIN THEOREM IMPLIES SMALL GENERATORS

- Let S be the set of all ideals $\mathfrak{p}$ of prime norm smaller than the bound B from the theorem, and such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$
- Suppose S generates a subgroup $N \neq H$
- There is a non-trivial character of H that is trivial on N
- This character extends to a character $\chi\colon \mathrm{Cl}_{\mathfrak{m}}(K) \longrightarrow \mathbb{C}^{\times}$ that is not trivial on H
- From the theorem, there is an ideal $\mathfrak{p}$ in S such that $\chi(\mathfrak{p}) \neq 1$
- So $\mathfrak{p}$ is in N and $\chi(\mathfrak{p}) \neq 1$, a contradiction, so $N = H$



4 CONSEQUENCES

ON INTEGERS

- Let m be a positive integer, and H a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$

ON INTEGERS

- Let m be a positive integer, and H a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$
- H is generated by the prime numbers p such that $p \bmod m$ is in H and $p \leq 16\,([(\mathbb{Z}/m\mathbb{Z})^\times : H] \log m)^2$

ON ISOGENY GRAPHS

- Let A be an absolutely simple, ordinary, principally polarised abelian variety (p.p.a.v.), with endomorphism algebra K

ON ISOGENY GRAPHS

- Let A be an absolutely simple, ordinary, principally polarised abelian variety (p.p.a.v.), with endomorphism algebra K
- Let V be the set of p.p.a.v.'s isogenous to A, and with same endomorphism ring (which we assume Gorenstein, and with conductor $\mathfrak{f}$)

ON ISOGENY GRAPHS

- Let A be an absolutely simple, ordinary, principally polarised abelian variety (p.p.a.v.), with endomorphism algebra K
- Let V be the set of p.p.a.v.'s isogenous to A, and with same endomorphism ring (which we assume Gorenstein, and with conductor $\mathfrak{f}$)
- For $B > 0$, let $G(B)$ be the isogeny graph on vertices V with edges the cyclic isogenies of prime degree smaller than B

ON ISOGENY GRAPHS

- Let A be an absolutely simple, ordinary, principally polarised abelian variety (p.p.a.v.), with endomorphism algebra K
- Let V be the set of p.p.a.v.'s isogenous to A, and with same endomorphism ring (which we assume Gorenstein, and with conductor $\mathfrak{f}$)
- For $B > 0$, let $G(B)$ be the isogeny graph on vertices V with edges the cyclic isogenies of prime degree smaller than B
- $G\left(26(h^+ \log(\mathrm{Disc}(K)N(\mathfrak{f})))^2\right)$ **is connected**, where h^+ is the narrow class number of the real suborder of $\mathrm{End}(A)$

BENJAMIN
WESOLOWSKI

GENERATING SUBGROUPS OF RAY CLASS GROUPS

with small prime ideals

AT ANTS-XIII, MADISON, WI,USA, ON THE 19/07/2018 BY BENJAMIN WESOLOWSKI, EPFL, LAUSANNE, SWITZERLAND

PROOF OF THE MAIN THEOREM

- For any $0 < a < 1$, $x > 0$ and ideal $\mathfrak{a}$, let

$$P(\mathfrak{a}, x) = \Lambda(\mathfrak{a}) \left(\frac{N(\mathfrak{a})}{x} \right)^a \log\left(\frac{x}{N(\mathfrak{a})} \right)$$

PROOF OF THE MAIN THEOREM

- For any $0 < a < 1, x > 0$ and ideal $\mathfrak{a}$, let

$$P(\mathfrak{a}, x) = \Lambda(\mathfrak{a}) \left(\frac{N(\mathfrak{a})}{x} \right)^a \log\left(\frac{x}{N(\mathfrak{a})} \right)$$

Lemma [Bach90]: For any character η,

$$\sum_{N(\mathfrak{a}) < x} \eta(\mathfrak{a}) P(\mathfrak{a}, x) = \frac{-1}{2\pi i} \int_{2 - i\infty}^{2 + i\infty} \frac{x^s}{(s + a)^2} \frac{L'_\eta}{L_\eta}(s)\, ds$$

PROOF OF THE MAIN THEOREM

- For any $0 < a < 1$, $x > 0$ and ideal $\mathfrak{a}$, let

$$P(\mathfrak{a}, x) = \Lambda(\mathfrak{a}) \left(\frac{N(\mathfrak{a})}{x} \right)^a \log\left(\frac{x}{N(\mathfrak{a})} \right)$$

Lemma [Bach90]: For any character η,

$$\sum_{N(\mathfrak{a}) < x} \eta(\mathfrak{a})\, P(\mathfrak{a}, x) = \frac{-1}{2\pi i} \int_{2 - i\infty}^{2 + i\infty} \frac{x^s}{(s + a)^2} \frac{L'_\eta}{L_\eta}(s)\, ds$$

Logarithmic derivative of the Hecke L-function associated to η

PROOF OF THE MAIN THEOREM

Lemma [Bach90]: For any character η,

$$\sum_{N(\mathfrak{a}) < x} \eta(\mathfrak{a})\, P(\mathfrak{a}, x) = \frac{-1}{2\pi i} \int_{2 - i\infty}^{2 + i\infty} \frac{x^s}{(s + a)^2} \frac{L'_\eta}{L_\eta}(s)\, ds$$

- **Proof of the bounds of [Bach90]:** consider the difference between two instances of this equality, at $\eta = 1$ and $\eta = \chi$

PROOF OF THE MAIN THEOREM

Lemma [Bach90]: For any character η,

$$\sum_{N(\mathfrak{a}) < x} \eta(\mathfrak{a})\, P(\mathfrak{a}, x) = \frac{-1}{2\pi i} \int_{2 - i\infty}^{2 + i\infty} \frac{x^s}{(s+a)^2} \frac{L'_\eta}{L_\eta}(s)\, ds$$

- **Proof of the bounds of [Bach90]:** consider the difference between two instances of this equality, at $\eta = 1$ and $\eta = \chi$
- The right-hand side is estimated as $x + O(x^{1/2})$

PROOF OF THE MAIN THEOREM

Lemma [Bach90]: For any character η,

$$\sum_{N(\mathfrak{a}) < x} \eta(\mathfrak{a})\, P(\mathfrak{a}, x) = \frac{-1}{2\pi i} \int_{2 - i\infty}^{2 + i\infty} \frac{x^s}{(s+a)^2} \frac{L'_\eta}{L_\eta}(s)\, ds$$

- **Proof of the bounds of [Bach90]:** consider the difference between two instances of this equality, at $\eta = 1$ and $\eta = \chi$
- The right-hand side is estimated as $x + O(x^{1/2})$
- The left-hand side is zero if χ is trivial on ideals of norm $< x$

PROOF OF THE MAIN THEOREM

Lemma [Bach90]: For any character η,

$$\sum_{N(\mathfrak{a}) < x} \eta(\mathfrak{a})\, P(\mathfrak{a}, x) = \frac{-1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2} \frac{L'_\eta}{L_\eta}(s)\, ds$$

- **Proof of the bounds of [Bach90]:** consider the difference between two instances of this equality, at $\eta = 1$ and $\eta = \chi$
- The right-hand side is estimated as $x + O(x^{1/2})$
- The left-hand side is zero if χ is trivial on ideals of norm $< x$
- So such an x cannot be too large

PROOF OF THE MAIN THEOREM

Lemma [Bach90]: For any character η,

$$\sum_{N(\mathfrak{a}) < x} \eta(\mathfrak{a})\, P(\mathfrak{a}, x) = \frac{-1}{2\pi i} \int_{2 - i\infty}^{2 + i\infty} \frac{x^s}{(s + a)^2} \frac{L'_\eta}{L_\eta}(s)\, ds$$

- **Proof of our new bounds:** similar ideas, but play with characters of $\mathrm{Cl}_{\mathfrak{m}}(K)/H$ to account for the extra condition that the ideals $\mathfrak{a}$ are in the subgroup H