

Computational  
algebraic number theory  
tackles lattice-based cryptography

Daniel J. Bernstein  
University of Illinois at Chicago &  
Technische Universiteit Eindhoven

---

*Moving to the left*

*Moving to the right*

*Big generator*

*Moving through the night*

—Yes, “Big Generator”, 1987

---

## The short-generator problem

Take degree- $n$  number field  $K$ .  
i.e. field  $K \subseteq \mathbf{C}$  with  $\text{len}_{\mathbf{Q}} K = n$ .

(Weaker specification: field  $K$   
with  $\mathbf{Q} \subseteq K$  and  $\text{len}_{\mathbf{Q}} K = n$ .)

e.g.  $n = 2$ ;  $K = \mathbf{Q}(i) =$   
 $\mathbf{Q} \oplus \mathbf{Q}i \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$ .

e.g.  $n = 256$ ;  $\zeta = \exp(\pi i/n)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + 1)$ .

e.g.  $n = 660$ ;  $\zeta = \exp(2\pi i/661)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + \dots + 1)$ .

e.g.  $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

ational  
c number theory  
attice-based cryptography  
. Bernstein  
ty of Illinois at Chicago &  
che Universiteit Eindhoven

---

*Moving to the left*  
*Moving to the right*  
*Big generator*  
*Moving through the night*  
Yes, "Big Generator", 1987

---

## The short-generator problem

Take degree- $n$  number field  $K$ .  
i.e. field  $K \subseteq \mathbf{C}$  with  $\text{len}_{\mathbf{Q}} K = n$ .

(Weaker specification: field  $K$   
with  $\mathbf{Q} \subseteq K$  and  $\text{len}_{\mathbf{Q}} K = n$ .)

e.g.  $n = 2$ ;  $K = \mathbf{Q}(i) =$

$\mathbf{Q} \oplus \mathbf{Q}i \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$ .

e.g.  $n = 256$ ;  $\zeta = \exp(\pi i/n)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + 1)$ .

e.g.  $n = 660$ ;  $\zeta = \exp(2\pi i/661)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + \dots + 1)$ .

e.g.  $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

Define  $\mathcal{O}$

$\mathcal{O} \hookrightarrow \mathbf{Z}^n$

Nonzero

factor un

powers o

e.g.  $K =$

$\Rightarrow \mathcal{O} =$

e.g.  $\zeta =$

$\Rightarrow \mathcal{O} =$

e.g.  $\zeta =$

$\Rightarrow \mathcal{O} =$

e.g.  $K =$

$\mathbf{Z}[(1 + \sqrt{2})]$

theory  
ed cryptography  
n  
is at Chicago &  
siteit Eindhoven

*Moving to the left  
moving to the right  
Big generator  
through the night  
Generator", 1987*

## The short-generator problem

Take degree- $n$  number field  $K$ .

i.e. field  $K \subseteq \mathbf{C}$  with  $\text{len}_{\mathbf{Q}} K = n$ .

(Weaker specification: field  $K$   
with  $\mathbf{Q} \subseteq K$  and  $\text{len}_{\mathbf{Q}} K = n$ .)

e.g.  $n = 2$ ;  $K = \mathbf{Q}(i) =$

$\mathbf{Q} \oplus \mathbf{Q}i \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$ .

e.g.  $n = 256$ ;  $\zeta = \exp(\pi i/n)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + 1)$ .

e.g.  $n = 660$ ;  $\zeta = \exp(2\pi i/661)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + \dots + 1)$ .

e.g.  $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

Define  $\mathcal{O} = \bar{\mathbf{Z}} \cap K$

$\mathcal{O} \hookrightarrow \mathbf{Z}^n$  as  $\mathbf{Z}$ -mod

Nonzero ideals of

factor uniquely as

powers of prime id

e.g.  $K = \mathbf{Q}(i) \hookrightarrow$

$\Rightarrow \mathcal{O} = \mathbf{Z}[i] \hookrightarrow \mathbf{Z}$

e.g.  $\zeta = \exp(\pi i/25)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}$

e.g.  $\zeta = \exp(2\pi i/661)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \dots$

e.g.  $K = \mathbf{Q}(\sqrt{5}) =$

$\mathbf{Z}[(1 + \sqrt{5})/2] \hookrightarrow \mathbf{Z}$

## The short-generator problem

Take degree- $n$  number field  $K$ .

i.e. field  $K \subseteq \mathbf{C}$  with  $\text{len}_{\mathbf{Q}} K = n$ .

(Weaker specification: field  $K$   
with  $\mathbf{Q} \subseteq K$  and  $\text{len}_{\mathbf{Q}} K = n$ .)

e.g.  $n = 2$ ;  $K = \mathbf{Q}(i) =$   
 $\mathbf{Q} \oplus \mathbf{Q}i \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$ .

e.g.  $n = 256$ ;  $\zeta = \exp(\pi i/n)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + 1)$ .

e.g.  $n = 660$ ;  $\zeta = \exp(2\pi i/661)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + \dots + 1)$ .

e.g.  $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

Define  $\mathcal{O} = \bar{\mathbf{Z}} \cap K$ ; subring  
 $\mathcal{O} \hookrightarrow \mathbf{Z}^n$  as  $\mathbf{Z}$ -modules.

Nonzero ideals of  $\mathcal{O}$   
factor uniquely as products  
of powers of prime ideals of  $\mathcal{O}$ .

e.g.  $K = \mathbf{Q}(i) \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$   
 $\Rightarrow \mathcal{O} = \mathbf{Z}[i] \hookrightarrow \mathbf{Z}[x]/(x^2 + 1)$

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$   
 $\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^{256} + 1)$

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$   
 $\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \dots$

e.g.  $K = \mathbf{Q}(\sqrt{5}) \Rightarrow \mathcal{O} =$   
 $\mathbf{Z}[(1 + \sqrt{5})/2] \hookrightarrow \mathbf{Z}[x]/(x^2 - 5)$

## The short-generator problem

Take degree- $n$  number field  $K$ .

i.e. field  $K \subseteq \mathbf{C}$  with  $\text{len}_{\mathbf{Q}} K = n$ .

(Weaker specification: field  $K$  with  $\mathbf{Q} \subseteq K$  and  $\text{len}_{\mathbf{Q}} K = n$ .)

e.g.  $n = 2$ ;  $K = \mathbf{Q}(i) = \mathbf{Q} \oplus \mathbf{Q}i \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$ .

e.g.  $n = 256$ ;  $\zeta = \exp(\pi i/n)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + 1)$ .

e.g.  $n = 660$ ;  $\zeta = \exp(2\pi i/661)$ ;

$K = \mathbf{Q}(\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + \dots + 1)$ .

e.g.  $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

Define  $\mathcal{O} = \bar{\mathbf{Z}} \cap K$ ; subring of  $K$ .

$\mathcal{O} \hookrightarrow \mathbf{Z}^n$  as  $\mathbf{Z}$ -modules.

Nonzero ideals of  $\mathcal{O}$

factor uniquely as products of powers of prime ideals of  $\mathcal{O}$ .

e.g.  $K = \mathbf{Q}(i) \hookrightarrow \mathbf{Q}[x]/(x^2 + 1) \Rightarrow \mathcal{O} = \mathbf{Z}[i] \hookrightarrow \mathbf{Z}[x]/(x^2 + 1)$ .

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta) \Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^{256} + 1)$ .

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta) \Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \dots$ .

e.g.  $K = \mathbf{Q}(\sqrt{5}) \Rightarrow \mathcal{O} = \mathbf{Z}[(1 + \sqrt{5})/2] \hookrightarrow \mathbf{Z}[x]/(x^2 - x - 1)$ .

## Art-generator problem

degree- $n$  number field  $K$ .

$K \subseteq \mathbf{C}$  with  $\text{len}_{\mathbf{Q}} K = n$ .

specification: field  $K$

$\subseteq K$  and  $\text{len}_{\mathbf{Q}} K = n$ .)

2;  $K = \mathbf{Q}(i) =$   
 $\hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$ .

256;  $\zeta = \exp(\pi i/n)$ ;

$\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + 1)$ .

660;  $\zeta = \exp(2\pi i/661)$ ;

$\zeta) \hookrightarrow \mathbf{Q}[x]/(x^n + \dots + 1)$ .

$= \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

Define  $\mathcal{O} = \overline{\mathbf{Z}} \cap K$ ; subring of  $K$ .

$\mathcal{O} \hookrightarrow \mathbf{Z}^n$  as  $\mathbf{Z}$ -modules.

Nonzero ideals of  $\mathcal{O}$

factor uniquely as products of powers of prime ideals of  $\mathcal{O}$ .

e.g.  $K = \mathbf{Q}(i) \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$   
 $\Rightarrow \mathcal{O} = \mathbf{Z}[i] \hookrightarrow \mathbf{Z}[x]/(x^2 + 1)$ .

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$   
 $\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^{256} + 1)$ .

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$   
 $\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \dots$ .

e.g.  $K = \mathbf{Q}(\sqrt{5}) \Rightarrow \mathcal{O} =$   
 $\mathbf{Z}[(1 + \sqrt{5})/2] \hookrightarrow \mathbf{Z}[x]/(x^2 - x - 1)$ .

The sho

Find "sh

given th

e.g.  $\zeta =$

$\mathcal{O} = \mathbf{Z}[\zeta]$

The  $\mathbf{Z}$ -s

201 - 23

935 - 10

979 - 11

718 - 82

is an ide

Can you

such tha

or problem

number field  $K$ .

with  $\text{len}_{\mathbf{Q}} K = n$ .

tion: field  $K$

$\text{len}_{\mathbf{Q}} K = n$ .)

$\mathbf{Q}(i) =$

$\mathbf{Z}[x]/(x^2 + 1)$ .

$\exp(\pi i/n)$ ;

$\mathbf{Z}[x]/(x^n + 1)$ .

$\exp(2\pi i/661)$ ;

$\mathbf{Z}[x]/(x^n + \dots + 1)$ .

$\sqrt{3}, \sqrt{5}, \dots, \sqrt{29}$ ).

Define  $\mathcal{O} = \bar{\mathbf{Z}} \cap K$ ; subring of  $K$ .

$\mathcal{O} \hookrightarrow \mathbf{Z}^n$  as  $\mathbf{Z}$ -modules.

Nonzero ideals of  $\mathcal{O}$

factor uniquely as products of powers of prime ideals of  $\mathcal{O}$ .

e.g.  $K = \mathbf{Q}(i) \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[i] \hookrightarrow \mathbf{Z}[x]/(x^2 + 1)$ .

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^{256} + 1)$ .

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \dots$ .

e.g.  $K = \mathbf{Q}(\sqrt{5}) \Rightarrow \mathcal{O} =$

$\mathbf{Z}[(1 + \sqrt{5})/2] \hookrightarrow \mathbf{Z}[x]/(x^2 - x - 1)$ .

The short-generators

Find "short" nonzero

given the principal

e.g.  $\zeta = \exp(\pi i/4)$

$\mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]$ ,

The  $\mathbf{Z}$ -submodule

$201 - 233\zeta - 430\zeta^2$

$935 - 1063\zeta - 198\zeta^2$

$979 - 1119\zeta - 209\zeta^2$

$718 - 829\zeta - 153\zeta^2$

is an ideal  $I$  of  $\mathcal{O}$ .

Can you find a short

such that  $I = g\mathcal{O}$

Define  $\mathcal{O} = \bar{\mathbf{Z}} \cap K$ ; subring of  $K$ .

$\mathcal{O} \hookrightarrow \mathbf{Z}^n$  as  $\mathbf{Z}$ -modules.

Nonzero ideals of  $\mathcal{O}$

factor uniquely as products of powers of prime ideals of  $\mathcal{O}$ .

e.g.  $K = \mathbf{Q}(i) \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[i] \hookrightarrow \mathbf{Z}[x]/(x^2 + 1)$ .

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^{256} + 1)$ .

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \dots$

e.g.  $K = \mathbf{Q}(\sqrt{5}) \Rightarrow \mathcal{O} =$

$\mathbf{Z}[(1 + \sqrt{5})/2] \hookrightarrow \mathbf{Z}[x]/(x^2 - x - 1)$ .

The short-generator problem

Find "short" nonzero  $g \in \mathcal{O}$

given the principal ideal  $g\mathcal{O}$

e.g.  $\zeta = \exp(\pi i/4)$ ;  $K = \mathbf{Q}(\zeta)$

$\mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^4 + 1)$ .

The  $\mathbf{Z}$ -submodule of  $\mathcal{O}$  gen

$201 - 233\zeta - 430\zeta^2 - 712\zeta^3$

$935 - 1063\zeta - 1986\zeta^2 - 329\zeta^3$

$979 - 1119\zeta - 2092\zeta^2 - 347\zeta^3$

$718 - 829\zeta - 1537\zeta^2 - 254\zeta^3$

is an ideal  $I$  of  $\mathcal{O}$ .

Can you find a short  $g \in \mathcal{O}$

such that  $I = g\mathcal{O}$ ?

Define  $\mathcal{O} = \overline{\mathbf{Z}} \cap K$ ; subring of  $K$ .

$\mathcal{O} \hookrightarrow \mathbf{Z}^n$  as  $\mathbf{Z}$ -modules.

Nonzero ideals of  $\mathcal{O}$

factor uniquely as products of powers of prime ideals of  $\mathcal{O}$ .

e.g.  $K = \mathbf{Q}(i) \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[i] \hookrightarrow \mathbf{Z}[x]/(x^2 + 1)$ .

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^{256} + 1)$ .

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$

$\Rightarrow \mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \dots$ .

e.g.  $K = \mathbf{Q}(\sqrt{5}) \Rightarrow \mathcal{O} =$

$\mathbf{Z}[(1+\sqrt{5})/2] \hookrightarrow \mathbf{Z}[x]/(x^2 - x - 1)$ .

The short-generator problem:

Find “short” nonzero  $g \in \mathcal{O}$

given the principal ideal  $g\mathcal{O}$ .

e.g.  $\zeta = \exp(\pi i/4)$ ;  $K = \mathbf{Q}(\zeta)$ ;

$\mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^4 + 1)$ .

The  $\mathbf{Z}$ -submodule of  $\mathcal{O}$  gen by

$201 - 233\zeta - 430\zeta^2 - 712\zeta^3$ ,

$935 - 1063\zeta - 1986\zeta^2 - 3299\zeta^3$ ,

$979 - 1119\zeta - 2092\zeta^2 - 3470\zeta^3$ ,

$718 - 829\zeta - 1537\zeta^2 - 2546\zeta^3$

is an ideal  $I$  of  $\mathcal{O}$ .

Can you find a short  $g \in \mathcal{O}$

such that  $I = g\mathcal{O}$ ?

$\mathcal{O} = \overline{\mathbf{Z}} \cap K$ ; subring of  $K$ .

' as  $\mathbf{Z}$ -modules.

ideals of  $\mathcal{O}$

uniquely as products of

of prime ideals of  $\mathcal{O}$ .

$$= \mathbf{Q}(i) \hookrightarrow \mathbf{Q}[x]/(x^2 + 1)$$

$$\mathbf{Z}[i] \hookrightarrow \mathbf{Z}[x]/(x^2 + 1).$$

$$\exp(\pi i/256), K = \mathbf{Q}(\zeta)$$

$$\mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^{256} + 1).$$

$$\exp(2\pi i/661), K = \mathbf{Q}(\zeta)$$

$$\mathbf{Z}[\zeta] \hookrightarrow \dots$$

$$= \mathbf{Q}(\sqrt{5}) \Rightarrow \mathcal{O} =$$

$$\sqrt{5})/2] \hookrightarrow \mathbf{Z}[x]/(x^2 - x - 1).$$

The short-generator problem:

Find "short" nonzero  $g \in \mathcal{O}$

given the principal ideal  $g\mathcal{O}$ .

e.g.  $\zeta = \exp(\pi i/4)$ ;  $K = \mathbf{Q}(\zeta)$ ;

$$\mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^4 + 1).$$

The  $\mathbf{Z}$ -submodule of  $\mathcal{O}$  gen by

$$201 - 233\zeta - 430\zeta^2 - 712\zeta^3,$$

$$935 - 1063\zeta - 1986\zeta^2 - 3299\zeta^3,$$

$$979 - 1119\zeta - 2092\zeta^2 - 3470\zeta^3,$$

$$718 - 829\zeta - 1537\zeta^2 - 2546\zeta^3$$

is an ideal  $I$  of  $\mathcal{O}$ .

Can you find a short  $g \in \mathcal{O}$

such that  $I = g\mathcal{O}$ ?

The latt

Use LLL

short ele

$\mathbf{Z}A + \mathbf{Z}B$

$$A = (20$$

$$B = (93$$

$$C = (97$$

$$D = (71$$

$\mathcal{O}$ ; subring of  $K$ .

modules.

$\mathcal{O}$

products of

ideals of  $\mathcal{O}$ .

$$\mathbf{Q}[x]/(x^2 + 1)$$

$$\mathbf{Z}[x]/(x^2 + 1).$$

$$(56), K = \mathbf{Q}(\zeta)$$

$$\mathbf{Z}[x]/(x^{256} + 1).$$

$$(661), K = \mathbf{Q}(\zeta)$$

...

$$\Rightarrow \mathcal{O} =$$

$$\mathbf{Z}[x]/(x^2 - x - 1).$$

The short-generator problem:

Find "short" nonzero  $g \in \mathcal{O}$

given the principal ideal  $g\mathcal{O}$ .

e.g.  $\zeta = \exp(\pi i/4)$ ;  $K = \mathbf{Q}(\zeta)$ ;

$$\mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^4 + 1).$$

The  $\mathbf{Z}$ -submodule of  $\mathcal{O}$  gen by

$$201 - 233\zeta - 430\zeta^2 - 712\zeta^3,$$

$$935 - 1063\zeta - 1986\zeta^2 - 3299\zeta^3,$$

$$979 - 1119\zeta - 2092\zeta^2 - 3470\zeta^3,$$

$$718 - 829\zeta - 1537\zeta^2 - 2546\zeta^3$$

is an ideal  $I$  of  $\mathcal{O}$ .

Can you find a short  $g \in \mathcal{O}$

such that  $I = g\mathcal{O}$ ?

The lattice perspective

Use LLL to quickly

find short elements of

$$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C +$$

$$A = (201, -233, -$$

$$B = (935, -1063,$$

$$C = (979, -1119,$$

$$D = (718, -829, -$$

The short-generator problem:

Find “short” nonzero  $g \in \mathcal{O}$   
given the principal ideal  $g\mathcal{O}$ .

e.g.  $\zeta = \exp(\pi i/4)$ ;  $K = \mathbf{Q}(\zeta)$ ;

$\mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^4 + 1)$ .

The  $\mathbf{Z}$ -submodule of  $\mathcal{O}$  gen by

$201 - 233\zeta - 430\zeta^2 - 712\zeta^3$ ,

$935 - 1063\zeta - 1986\zeta^2 - 3299\zeta^3$ ,

$979 - 1119\zeta - 2092\zeta^2 - 3470\zeta^3$ ,

$718 - 829\zeta - 1537\zeta^2 - 2546\zeta^3$

is an ideal  $I$  of  $\mathcal{O}$ .

Can you find a short  $g \in \mathcal{O}$

such that  $I = g\mathcal{O}$ ?

The lattice perspective

Use LLL to quickly find  
short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$A = (201, -233, -430, -712)$

$B = (935, -1063, -1986, -3299)$

$C = (979, -1119, -2092, -3470)$

$D = (718, -829, -1537, -2546)$

The short-generator problem:

Find “short” nonzero  $g \in \mathcal{O}$   
given the principal ideal  $g\mathcal{O}$ .

e.g.  $\zeta = \exp(\pi i/4)$ ;  $K = \mathbf{Q}(\zeta)$ ;

$\mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^4 + 1)$ .

The  $\mathbf{Z}$ -submodule of  $\mathcal{O}$  gen by

$201 - 233\zeta - 430\zeta^2 - 712\zeta^3$ ,

$935 - 1063\zeta - 1986\zeta^2 - 3299\zeta^3$ ,

$979 - 1119\zeta - 2092\zeta^2 - 3470\zeta^3$ ,

$718 - 829\zeta - 1537\zeta^2 - 2546\zeta^3$

is an ideal  $I$  of  $\mathcal{O}$ .

Can you find a short  $g \in \mathcal{O}$

such that  $I = g\mathcal{O}$ ?

The lattice perspective

Use LLL to quickly find  
short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$A = (201, -233, -430, -712)$ ,

$B = (935, -1063, -1986, -3299)$ ,

$C = (979, -1119, -2092, -3470)$ ,

$D = (718, -829, -1537, -2546)$ .

The short-generator problem:

Find “short” nonzero  $g \in \mathcal{O}$   
given the principal ideal  $g\mathcal{O}$ .

e.g.  $\zeta = \exp(\pi i/4)$ ;  $K = \mathbf{Q}(\zeta)$ ;

$\mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^4 + 1)$ .

The  $\mathbf{Z}$ -submodule of  $\mathcal{O}$  gen by

$201 - 233\zeta - 430\zeta^2 - 712\zeta^3$ ,

$935 - 1063\zeta - 1986\zeta^2 - 3299\zeta^3$ ,

$979 - 1119\zeta - 2092\zeta^2 - 3470\zeta^3$ ,

$718 - 829\zeta - 1537\zeta^2 - 2546\zeta^3$

is an ideal  $I$  of  $\mathcal{O}$ .

Can you find a short  $g \in \mathcal{O}$

such that  $I = g\mathcal{O}$ ?

The lattice perspective

Use LLL to quickly find  
short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$A = (201, -233, -430, -712)$ ,

$B = (935, -1063, -1986, -3299)$ ,

$C = (979, -1119, -2092, -3470)$ ,

$D = (718, -829, -1537, -2546)$ .

Find  $(3, 1, 4, 1)$  as

$-37A + 3B - 7C + 16D$ .

This was my original  $g$ .

The short-generator problem:

Find “short” nonzero  $g \in \mathcal{O}$   
given the principal ideal  $g\mathcal{O}$ .

e.g.  $\zeta = \exp(\pi i/4)$ ;  $K = \mathbf{Q}(\zeta)$ ;  
 $\mathcal{O} = \mathbf{Z}[\zeta] \hookrightarrow \mathbf{Z}[x]/(x^4 + 1)$ .

The  $\mathbf{Z}$ -submodule of  $\mathcal{O}$  gen by

$$201 - 233\zeta - 430\zeta^2 - 712\zeta^3,$$

$$935 - 1063\zeta - 1986\zeta^2 - 3299\zeta^3,$$

$$979 - 1119\zeta - 2092\zeta^2 - 3470\zeta^3,$$

$$718 - 829\zeta - 1537\zeta^2 - 2546\zeta^3$$

is an ideal  $I$  of  $\mathcal{O}$ .

Can you find a short  $g \in \mathcal{O}$

such that  $I = g\mathcal{O}$ ?

The lattice perspective

Use LLL to quickly find  
short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$$A = (201, -233, -430, -712),$$

$$B = (935, -1063, -1986, -3299),$$

$$C = (979, -1119, -2092, -3470),$$

$$D = (718, -829, -1537, -2546).$$

Find  $(3, 1, 4, 1)$  as

$$-37A + 3B - 7C + 16D.$$

This was my original  $g$ .

Also find, e.g.,  $(-4, -1, 3, 1)$ .

Multiplying by root of unity

(here  $\zeta^2$ ) preserves shortness.

Short-generator problem:

Find a "short" nonzero  $g \in \mathcal{O}$

such that the principal ideal  $g\mathcal{O}$ .

$\zeta = \exp(\pi i/4)$ ;  $K = \mathbf{Q}(\zeta)$ ;

$\mathcal{O} \cong \mathbf{Z}[x]/(x^4 + 1)$ .

$I$  is a submodule of  $\mathcal{O}$  gen by

$33\zeta - 430\zeta^2 - 712\zeta^3$ ,

$1063\zeta - 1986\zeta^2 - 3299\zeta^3$ ,

$1119\zeta - 2092\zeta^2 - 3470\zeta^3$ ,

$129\zeta - 1537\zeta^2 - 2546\zeta^3$

is a principal ideal  $I$  of  $\mathcal{O}$ .

How to find a short  $g \in \mathcal{O}$

such that  $I = g\mathcal{O}$ ?

## The lattice perspective

Use LLL to quickly find short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$A = (201, -233, -430, -712)$ ,

$B = (935, -1063, -1986, -3299)$ ,

$C = (979, -1119, -2092, -3470)$ ,

$D = (718, -829, -1537, -2546)$ .

Find  $(3, 1, 4, 1)$  as

$-37A + 3B - 7C + 16D$ .

This was my original  $g$ .

Also find, e.g.,  $(-4, -1, 3, 1)$ .

Multiplying by root of unity

(here  $\zeta^2$ ) preserves shortness.

For much

LLL alms

Big gap

and size

that LLL

or problem:

zero  $g \in \mathcal{O}$

ideal  $g\mathcal{O}$ .

$\mathcal{O}$ ;  $K = \mathbf{Q}(\zeta)$ ;

$\mathcal{O}/(x^4 + 1)$ .

of  $\mathcal{O}$  gen by

$\zeta^2 - 712\zeta^3$ ,

$86\zeta^2 - 3299\zeta^3$ ,

$92\zeta^2 - 3470\zeta^3$ ,

$7\zeta^2 - 2546\zeta^3$

ort  $g \in \mathcal{O}$

?

## The lattice perspective

Use LLL to quickly find

short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$A = (201, -233, -430, -712)$ ,

$B = (935, -1063, -1986, -3299)$ ,

$C = (979, -1119, -2092, -3470)$ ,

$D = (718, -829, -1537, -2546)$ .

Find  $(3, 1, 4, 1)$  as

$-37A + 3B - 7C + 16D$ .

This was my original  $g$ .

Also find, e.g.,  $(-4, -1, 3, 1)$ .

Multiplying by root of unity

(here  $\zeta^2$ ) preserves shortness.

For much larger  $n$

LLL almost never

Big gap between  $s$

and size of “short”

that LLL typically

## The lattice perspective

Use LLL to quickly find short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$$A = (201, -233, -430, -712),$$

$$B = (935, -1063, -1986, -3299),$$

$$C = (979, -1119, -2092, -3470),$$

$$D = (718, -829, -1537, -2546).$$

Find  $(3, 1, 4, 1)$  as

$$-37A + 3B - 7C + 16D.$$

This was my original  $g$ .

Also find, e.g.,  $(-4, -1, 3, 1)$ .

Multiplying by root of unity (here  $\zeta^2$ ) preserves shortness.

For much larger  $n$ :

LLL almost never finds  $g$ .  
Big gap between size of  $g$  and size of “short” vectors that LLL typically finds in  $I$ .

## The lattice perspective

Use LLL to quickly find short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$$A = (201, -233, -430, -712),$$

$$B = (935, -1063, -1986, -3299),$$

$$C = (979, -1119, -2092, -3470),$$

$$D = (718, -829, -1537, -2546).$$

Find  $(3, 1, 4, 1)$  as

$$-37A + 3B - 7C + 16D.$$

This was my original  $g$ .

Also find, e.g.,  $(-4, -1, 3, 1)$ .

Multiplying by root of unity (here  $\zeta^2$ ) preserves shortness.

For much larger  $n$ :

LLL almost never finds  $g$ .

Big gap between size of  $g$  and size of “short” vectors that LLL typically finds in  $I$ .

## The lattice perspective

Use LLL to quickly find short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$$A = (201, -233, -430, -712),$$

$$B = (935, -1063, -1986, -3299),$$

$$C = (979, -1119, -2092, -3470),$$

$$D = (718, -829, -1537, -2546).$$

Find  $(3, 1, 4, 1)$  as

$$-37A + 3B - 7C + 16D.$$

This was my original  $g$ .

Also find, e.g.,  $(-4, -1, 3, 1)$ .

Multiplying by root of unity (here  $\zeta^2$ ) preserves shortness.

For much larger  $n$ :

LLL almost never finds  $g$ .

Big gap between size of  $g$  and size of “short” vectors that LLL typically finds in  $I$ .

Increased BKZ block size: reduced gap but slower.

## The lattice perspective

Use LLL to quickly find short elements of lattice

$\mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}C + \mathbf{Z}D$  where

$$A = (201, -233, -430, -712),$$

$$B = (935, -1063, -1986, -3299),$$

$$C = (979, -1119, -2092, -3470),$$

$$D = (718, -829, -1537, -2546).$$

Find  $(3, 1, 4, 1)$  as

$$-37A + 3B - 7C + 16D.$$

This was my original  $g$ .

Also find, e.g.,  $(-4, -1, 3, 1)$ .

Multiplying by root of unity (here  $\zeta^2$ ) preserves shortness.

For much larger  $n$ :

LLL almost never finds  $g$ .

Big gap between size of  $g$  and size of “short” vectors that LLL typically finds in  $I$ .

Increased BKZ block size: reduced gap but slower.

Fancier lattice algorithms:

Under reasonable assumptions, 2015 Laarhoven–de Weger finds  $g$  in time  $\approx 1.23^n$ .

Big progress compared to, e.g., 2008 Nguyen–Vidick ( $\approx 1.33^n$ ) but still exponential time.

## Practical perspective

to quickly find  
elements of lattice

$B + \mathbf{Z}C + \mathbf{Z}D$  where

$(1, -233, -430, -712),$

$(5, -1063, -1986, -3299),$

$(9, -1119, -2092, -3470),$

$(8, -829, -1537, -2546).$

$(1, 4, 1)$  as

$3B - 7C + 16D.$

is my original  $g$ .

and, e.g.,  $(-4, -1, 3, 1).$

multiplication by root of unity

preserves shortness.

For much larger  $n$ :

LLL almost never finds  $g$ .

Big gap between size of  $g$   
and size of “short” vectors  
that LLL typically finds in  $I$ .

Increased BKZ block size:  
reduced gap but slower.

Fancier lattice algorithms:

Under reasonable assumptions,  
2015 Laarhoven–de Weger  
finds  $g$  in time  $\approx 1.23^n$ .

Big progress compared to, e.g.,  
2008 Nguyen–Vidick ( $\approx 1.33^n$ )  
but still exponential time.

## Exploiting

Use LLL  
generate

What ha

Pure lat

Work m

ctive

y find

lattice

$\mathbf{Z}D$  where

$(-430, -712),$

$(-1986, -3299),$

$(-2092, -3470),$

$(-1537, -2546).$

$+ 16D.$

nal  $g.$

$(4, -1, 3, 1).$

ot of unity

s shortness.

For much larger  $n$ :

LLL almost never finds  $g.$

Big gap between size of  $g$   
and size of “short” vectors  
that LLL typically finds in  $I.$

Increased BKZ block size:  
reduced gap but slower.

Fancier lattice algorithms:

Under reasonable assumptions,  
2015 Laarhoven–de Weger  
finds  $g$  in time  $\approx 1.23^n.$

Big progress compared to, e.g.,  
2008 Nguyen–Vidick ( $\approx 1.33^n$ )  
but still exponential time.

Exploiting factoriz

Use LLL, BKZ, etc  
generate rather sh

What happens if c

Pure lattice appro

Work much harder

For much larger  $n$ :

LLL almost never finds  $g$ .

Big gap between size of  $g$   
and size of “short” vectors  
that LLL typically finds in  $I$ .

Increased BKZ block size:  
reduced gap but slower.

Fancier lattice algorithms:

Under reasonable assumptions,  
2015 Laarhoven–de Weger  
finds  $g$  in time  $\approx 1.23^n$ .

Big progress compared to, e.g.,  
2008 Nguyen–Vidick ( $\approx 1.33^n$ )  
but still exponential time.

## Exploiting factorization

Use LLL, BKZ, etc. to  
generate rather short  $\alpha \in g\mathcal{O}$

What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard

Work much harder, find short

For much larger  $n$ :

LLL almost never finds  $g$ .  
Big gap between size of  $g$   
and size of “short” vectors  
that LLL typically finds in  $I$ .

Increased BKZ block size:  
reduced gap but slower.

Fancier lattice algorithms:  
Under reasonable assumptions,  
2015 Laarhoven–de Weger  
finds  $g$  in time  $\approx 1.23^n$ .  
Big progress compared to, e.g.,  
2008 Nguyen–Vidick ( $\approx 1.33^n$ )  
but still exponential time.

## Exploiting factorization

Use LLL, BKZ, etc. to  
generate rather short  $\alpha \in g\mathcal{O}$ .  
What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .  
Work much harder, find shorter  $\alpha$ .

For much larger  $n$ :

LLL almost never finds  $g$ .

Big gap between size of  $g$   
and size of “short” vectors  
that LLL typically finds in  $I$ .

Increased BKZ block size:  
reduced gap but slower.

Fancier lattice algorithms:

Under reasonable assumptions,  
2015 Laarhoven–de Weger  
finds  $g$  in time  $\approx 1.23^n$ .

Big progress compared to, e.g.,  
2008 Nguyen–Vidick ( $\approx 1.33^n$ )  
but still exponential time.

## Exploiting factorization

Use LLL, BKZ, etc. to  
generate rather short  $\alpha \in g\mathcal{O}$ .

What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .

Work much harder, find shorter  $\alpha$ .

Alternative: Gain information  
from factorization of ideals.

For much larger  $n$ :

LLL almost never finds  $g$ .  
Big gap between size of  $g$   
and size of “short” vectors  
that LLL typically finds in  $I$ .

Increased BKZ block size:  
reduced gap but slower.

Fancier lattice algorithms:  
Under reasonable assumptions,  
2015 Laarhoven–de Weger  
finds  $g$  in time  $\approx 1.23^n$ .

Big progress compared to, e.g.,  
2008 Nguyen–Vidick ( $\approx 1.33^n$ )  
but still exponential time.

## Exploiting factorization

Use LLL, BKZ, etc. to  
generate rather short  $\alpha \in g\mathcal{O}$ .  
What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .  
Work much harder, find shorter  $\alpha$ .

Alternative: Gain information  
from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$

For much larger  $n$ :

LLL almost never finds  $g$ .  
Big gap between size of  $g$   
and size of “short” vectors  
that LLL typically finds in  $I$ .

Increased BKZ block size:  
reduced gap but slower.

Fancier lattice algorithms:  
Under reasonable assumptions,  
2015 Laarhoven–de Weger  
finds  $g$  in time  $\approx 1.23^n$ .

Big progress compared to, e.g.,  
2008 Nguyen–Vidick ( $\approx 1.33^n$ )  
but still exponential time.

## Exploiting factorization

Use LLL, BKZ, etc. to  
generate rather short  $\alpha \in g\mathcal{O}$ .  
What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .  
Work much harder, find shorter  $\alpha$ .

Alternative: Gain information  
from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$   
and  $\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$

For much larger  $n$ :

LLL almost never finds  $g$ .  
Big gap between size of  $g$   
and size of “short” vectors  
that LLL typically finds in  $I$ .

Increased BKZ block size:  
reduced gap but slower.

Fancier lattice algorithms:  
Under reasonable assumptions,  
2015 Laarhoven–de Weger  
finds  $g$  in time  $\approx 1.23^n$ .  
Big progress compared to, e.g.,  
2008 Nguyen–Vidick ( $\approx 1.33^n$ )  
but still exponential time.

## Exploiting factorization

Use LLL, BKZ, etc. to  
generate rather short  $\alpha \in g\mathcal{O}$ .  
What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .  
Work much harder, find shorter  $\alpha$ .

Alternative: Gain information  
from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$   
and  $\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$   
and  $\alpha_3\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^2$

For much larger  $n$ :

LLL almost never finds  $g$ .  
Big gap between size of  $g$   
and size of “short” vectors  
that LLL typically finds in  $I$ .

Increased BKZ block size:  
reduced gap but slower.

Fancier lattice algorithms:  
Under reasonable assumptions,  
2015 Laarhoven–de Weger  
finds  $g$  in time  $\approx 1.23^n$ .  
Big progress compared to, e.g.,  
2008 Nguyen–Vidick ( $\approx 1.33^n$ )  
but still exponential time.

## Exploiting factorization

Use LLL, BKZ, etc. to  
generate rather short  $\alpha \in g\mathcal{O}$ .  
What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .  
Work much harder, find shorter  $\alpha$ .

Alternative: Gain information  
from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$   
and  $\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$   
and  $\alpha_3\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^2$  then  
 $P = \alpha_1\alpha_3^{-1}\mathcal{O}$  and  $Q = \alpha_2\alpha_3^{-1}\mathcal{O}$   
and  $g\mathcal{O} = \alpha_1^{-1}\alpha_2^{-2}\alpha_3^4\mathcal{O}$ .

h larger  $n$ :

ost never finds  $g$ .

between size of  $g$

of “short” vectors

typically finds in  $I$ .

d BKZ block size:

gap but slower.

lattice algorithms:

reasonable assumptions,

arhoven–de Weger

n time  $\approx 1.23^n$ .

gress compared to, e.g.,

guyen–Vidick ( $\approx 1.33^n$ )

exponential time.

## Exploiting factorization

Use LLL, BKZ, etc. to

generate rather short  $\alpha \in g\mathcal{O}$ .

What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .

Work much harder, find shorter  $\alpha$ .

Alternative: Gain information  
from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$

and  $\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$

and  $\alpha_3\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^2$  then

$P = \alpha_1\alpha_3^{-1}\mathcal{O}$  and  $Q = \alpha_2\alpha_3^{-1}\mathcal{O}$

and  $g\mathcal{O} = \alpha_1^{-1}\alpha_2^{-2}\alpha_3^4\mathcal{O}$ .

General

factor  $\alpha$

of some

Solve sys

to find  $g$

as produ

## Exploiting factorization

Use LLL, BKZ, etc. to generate rather short  $\alpha \in g\mathcal{O}$ .

What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .

Work much harder, find shorter  $\alpha$ .

Alternative: Gain information from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$

and  $\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$

and  $\alpha_3\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^2$  then

$P = \alpha_1\alpha_3^{-1}\mathcal{O}$  and  $Q = \alpha_2\alpha_3^{-1}\mathcal{O}$

and  $g\mathcal{O} = \alpha_1^{-1}\alpha_2^{-2}\alpha_3^4\mathcal{O}$ .

General strategy:

factor  $\alpha\mathcal{O}$  into product of some primes and

Solve system of equations

to find generator  $g$

as product of powers

## Exploiting factorization

Use LLL, BKZ, etc. to generate rather short  $\alpha \in g\mathcal{O}$ .

What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .  
Work much harder, find shorter  $\alpha$ .

Alternative: Gain information from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$

and  $\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$

and  $\alpha_3\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^2$  then

$P = \alpha_1\alpha_3^{-1}\mathcal{O}$  and  $Q = \alpha_2\alpha_3^{-1}\mathcal{O}$

and  $g\mathcal{O} = \alpha_1^{-1}\alpha_2^{-2}\alpha_3^4\mathcal{O}$ .

General strategy: For many  $\alpha\mathcal{O}$  factor into products of powers of some primes and  $g\mathcal{O}$ .

Solve system of equations to find generator for  $g\mathcal{O}$  as product of powers of the

## Exploiting factorization

Use LLL, BKZ, etc. to generate rather short  $\alpha \in g\mathcal{O}$ .

What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .  
Work much harder, find shorter  $\alpha$ .

Alternative: Gain information from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$

and  $\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$

and  $\alpha_3\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^2$  then

$P = \alpha_1\alpha_3^{-1}\mathcal{O}$  and  $Q = \alpha_2\alpha_3^{-1}\mathcal{O}$

and  $g\mathcal{O} = \alpha_1^{-1}\alpha_2^{-2}\alpha_3^4\mathcal{O}$ .

General strategy: For many  $\alpha$ 's, factor  $\alpha\mathcal{O}$  into products of powers of some primes and  $g\mathcal{O}$ .

Solve system of equations to find generator for  $g\mathcal{O}$  as product of powers of the  $\alpha$ 's.

## Exploiting factorization

Use LLL, BKZ, etc. to generate rather short  $\alpha \in g\mathcal{O}$ .

What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .  
Work much harder, find shorter  $\alpha$ .

Alternative: Gain information from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$

and  $\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$

and  $\alpha_3\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^2$  then

$P = \alpha_1\alpha_3^{-1}\mathcal{O}$  and  $Q = \alpha_2\alpha_3^{-1}\mathcal{O}$

and  $g\mathcal{O} = \alpha_1^{-1}\alpha_2^{-2}\alpha_3^4\mathcal{O}$ .

General strategy: For many  $\alpha$ 's, factor  $\alpha\mathcal{O}$  into products of powers of some primes and  $g\mathcal{O}$ .

Solve system of equations to find generator for  $g\mathcal{O}$  as product of powers of the  $\alpha$ 's.

“Can the system be solved?”

— Becomes increasingly reasonable to expect as the number of equations approaches and passes the number of primes.

## Exploiting factorization

Use LLL, BKZ, etc. to generate rather short  $\alpha \in g\mathcal{O}$ .

What happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

Pure lattice approach: Discard  $\alpha$ .  
Work much harder, find shorter  $\alpha$ .

Alternative: Gain information from factorization of ideals.

e.g. If  $\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$   
and  $\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$   
and  $\alpha_3\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^2$  then  
 $P = \alpha_1\alpha_3^{-1}\mathcal{O}$  and  $Q = \alpha_2\alpha_3^{-1}\mathcal{O}$   
and  $g\mathcal{O} = \alpha_1^{-1}\alpha_2^{-2}\alpha_3^4\mathcal{O}$ .

General strategy: For many  $\alpha$ 's, factor  $\alpha\mathcal{O}$  into products of powers of some primes and  $g\mathcal{O}$ .

Solve system of equations to find generator for  $g\mathcal{O}$  as product of powers of the  $\alpha$ 's.

“Can the system be solved?”

— Becomes increasingly reasonable to expect as the number of equations approaches and passes the number of primes.

“But {primes} is infinite!”

## Factorization

, BKZ, etc. to

rather short  $\alpha \in g\mathcal{O}$ .

happens if  $\alpha\mathcal{O} \neq g\mathcal{O}$ ?

naïve approach: Discard  $\alpha$ .

Much harder, find shorter  $\alpha$ .

Alternative: Gain information

Factorization of ideals.

$$\alpha_1\mathcal{O} = g\mathcal{O} \cdot P^2 \cdot Q^2$$

$$\alpha_2\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^3$$

$$\alpha_3\mathcal{O} = g\mathcal{O} \cdot P \cdot Q^2 \text{ then}$$

$$\alpha_3^{-1}\mathcal{O} \text{ and } Q = \alpha_2\alpha_3^{-1}\mathcal{O}$$

$$= \alpha_1^{-1}\alpha_2^{-2}\alpha_3^4\mathcal{O}.$$

General strategy: For many  $\alpha$ 's,  
factor  $\alpha\mathcal{O}$  into products of powers  
of some primes and  $g\mathcal{O}$ .

Solve system of equations  
to find generator for  $g\mathcal{O}$   
as product of powers of the  $\alpha$ 's.

“Can the system be solved?”

— Becomes increasingly  
reasonable to expect as the  
number of equations approaches  
and passes the number of primes.

“But {primes} is infinite!”

— Restr

e.g., all

ation

c. to

ort  $\alpha \in g\mathcal{O}$ .

$\alpha\mathcal{O} \neq g\mathcal{O}$ ?

ach: Discard  $\alpha$ .

r, find shorter  $\alpha$ .

information

of ideals.

$\cdot P^2 \cdot Q^2$

$\supset \cdot Q^3$

$\supset \cdot Q^2$  then

$Q = \alpha_2 \alpha_3^{-1} \mathcal{O}$

$^2 \alpha_3^4 \mathcal{O}$ .

General strategy: For many  $\alpha$ 's,  
factor  $\alpha\mathcal{O}$  into products of powers  
of some primes and  $g\mathcal{O}$ .

Solve system of equations  
to find generator for  $g\mathcal{O}$   
as product of powers of the  $\alpha$ 's.

“Can the system be solved?”

— Becomes increasingly  
reasonable to expect as the  
number of equations approaches  
and passes the number of primes.

“But {primes} is infinite!”

— Restrict to a “f”  
e.g., all primes of

General strategy: For many  $\alpha$ 's,  
factor  $\alpha\mathcal{O}$  into products of powers  
of some primes and  $g\mathcal{O}$ .

Solve system of equations  
to find generator for  $g\mathcal{O}$   
as product of powers of the  $\alpha$ 's.

“Can the system be solved?”

— Becomes increasingly  
reasonable to expect as the  
number of equations approaches  
and passes the number of primes.

“But {primes} is infinite!”

— Restrict to a “factor base”  
e.g., all primes of norm  $\leq y$ .

General strategy: For many  $\alpha$ 's,  
factor  $\alpha\mathcal{O}$  into products of powers  
of some primes and  $g\mathcal{O}$ .

Solve system of equations  
to find generator for  $g\mathcal{O}$   
as product of powers of the  $\alpha$ 's.

“Can the system be solved?”

— Becomes increasingly  
reasonable to expect as the  
number of equations approaches  
and passes the number of primes.

“But {primes} is infinite!”

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

General strategy: For many  $\alpha$ 's,  
factor  $\alpha \in \mathcal{O}$  into products of powers  
of some primes and  $g \in \mathcal{O}$ .

Solve system of equations  
to find generator for  $g \in \mathcal{O}$   
as product of powers of the  $\alpha$ 's.

“Can the system be solved?”

— Becomes increasingly  
reasonable to expect as the  
number of equations approaches  
and passes the number of primes.

“But {primes} is infinite!”

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha \in \mathcal{O}$  doesn't  
factor into those primes?”

General strategy: For many  $\alpha$ 's,  
factor  $\alpha\mathcal{O}$  into products of powers  
of some primes and  $g\mathcal{O}$ .

Solve system of equations  
to find generator for  $g\mathcal{O}$   
as product of powers of the  $\alpha$ 's.

“Can the system be solved?”

— Becomes increasingly  
reasonable to expect as the  
number of equations approaches  
and passes the number of primes.

“But {primes} is infinite!”

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha\mathcal{O}$  doesn't  
factor into those primes?”

— Then throw it away.  
But often it *does* factor.

General strategy: For many  $\alpha$ 's,  
factor  $\alpha\mathcal{O}$  into products of powers  
of some primes and  $g\mathcal{O}$ .

Solve system of equations  
to find generator for  $g\mathcal{O}$   
as product of powers of the  $\alpha$ 's.

“Can the system be solved?”

— Becomes increasingly  
reasonable to expect as the  
number of equations approaches  
and passes the number of primes.

“But {primes} is infinite!”

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha\mathcal{O}$  doesn't  
factor into those primes?”

— Then throw it away.  
But often it *does* factor.

Familiar issue from

“index calculus” DL methods,  
CFRAC, LS, QS, NFS, etc.

Model the norm of  $(\alpha/g)\mathcal{O}$

as “random” integer in  $[1, x]$ ;

$y$ -smoothness chance  $\approx 1/y$

if  $\log y \approx \sqrt{(1/2) \log x \log \log x}$ .

strategy: For many  $\alpha$ 's,  
 $\mathcal{O}$  into products of powers  
primes and  $g\mathcal{O}$ .

system of equations

generator for  $g\mathcal{O}$

product of powers of the  $\alpha$ 's.

the system be solved?"

times increasingly

able to expect as the

of equations approaches

uses the number of primes.

primes} is infinite!"

— Restrict to a “factor base” :  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha\mathcal{O}$  doesn't  
factor into those primes?”

— Then throw it away.

But often it *does* factor.

Familiar issue from

“index calculus” DL methods,  
CFRAC, LS, QS, NFS, etc.

Model the norm of  $(\alpha/g)\mathcal{O}$

as “random” integer in  $[1, x]$ ;

$y$ -smoothness chance  $\approx 1/y$

if  $\log y \approx \sqrt{(1/2) \log x \log \log x}$ .

Variation

Generate

factor  $\alpha$

After en

solve sys

obtain  $g$

For many  $\alpha$ 's,  
products of powers  
and  $g\mathcal{O}$ .

equations

for  $g\mathcal{O}$

in terms of the  $\alpha$ 's.

Can be solved?"

Increasingly

as the

number of approaches

number of primes.

infinite!"

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha\mathcal{O}$  doesn't  
factor into those primes?”

— Then throw it away.

But often it *does* factor.

Familiar issue from

“index calculus” DL methods,  
CFRAC, LS, QS, NFS, etc.

Model the norm of  $(\alpha/g)\mathcal{O}$

as “random” integer in  $[1, x]$ ;

$y$ -smoothness chance  $\approx 1/y$

if  $\log y \approx \sqrt{(1/2) \log x \log \log x}$ .

Variation: Ignore  $g$

Generate rather than

factor  $\alpha\mathcal{O}$  into small

After enough  $\alpha$ 's,

solve system of eq

obtain generator for

$\alpha$ 's,  
powers

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha\mathcal{O}$  doesn't  
factor into those primes?”

— Then throw it away.  
But often it *does* factor.

Familiar issue from  
“index calculus” DL methods,  
CFRAC, LS, QS, NFS, etc.

Model the norm of  $(\alpha/g)\mathcal{O}$   
as “random” integer in  $[1, x]$ ;  
 $y$ -smoothness chance  $\approx 1/y$   
if  $\log y \approx \sqrt{(1/2) \log x \log \log x}$ .

$\alpha$ 's.

,

ches  
primes.

Variation: Ignore  $g\mathcal{O}$ .

Generate rather short  $\alpha \in \mathcal{C}$   
factor  $\alpha\mathcal{O}$  into small primes  
After enough  $\alpha$ 's,  
solve system of equations;  
obtain generator for each pr

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha\mathcal{O}$  doesn't  
factor into those primes?”

— Then throw it away.  
But often it *does* factor.

Familiar issue from

“index calculus” DL methods,  
CFRAC, LS, QS, NFS, etc.

Model the norm of  $(\alpha/g)\mathcal{O}$

as “random” integer in  $[1, x]$ ;

$y$ -smoothness chance  $\approx 1/y$

if  $\log y \approx \sqrt{(1/2) \log x \log \log x}$ .

Variation: Ignore  $g\mathcal{O}$ .

Generate rather short  $\alpha \in \mathcal{O}$ ,  
factor  $\alpha\mathcal{O}$  into small primes.

After enough  $\alpha$ 's,

solve system of equations;

obtain generator for each prime.

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha\mathcal{O}$  doesn't  
factor into those primes?”

— Then throw it away.  
But often it *does* factor.

Familiar issue from

“index calculus” DL methods,  
CFRAC, LS, QS, NFS, etc.

Model the norm of  $(\alpha/g)\mathcal{O}$

as “random” integer in  $[1, x]$ ;

$y$ -smoothness chance  $\approx 1/y$

if  $\log y \approx \sqrt{(1/2) \log x \log \log x}$ .

Variation: Ignore  $g\mathcal{O}$ .

Generate rather short  $\alpha \in \mathcal{O}$ ,  
factor  $\alpha\mathcal{O}$  into small primes.

After enough  $\alpha$ 's,

solve system of equations;

obtain generator for each prime.

After this precomputation,

factor *one*  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;

obtain generator for  $g\mathcal{O}$ .

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha\mathcal{O}$  doesn't  
factor into those primes?”

— Then throw it away.  
But often it *does* factor.

Familiar issue from

“index calculus” DL methods,  
CFRAC, LS, QS, NFS, etc.

Model the norm of  $(\alpha/g)\mathcal{O}$

as “random” integer in  $[1, x]$ ;

$y$ -smoothness chance  $\approx 1/y$

if  $\log y \approx \sqrt{(1/2) \log x \log \log x}$ .

Variation: Ignore  $g\mathcal{O}$ .

Generate rather short  $\alpha \in \mathcal{O}$ ,  
factor  $\alpha\mathcal{O}$  into small primes.

After enough  $\alpha$ 's,

solve system of equations;

obtain generator for each prime.

After this precomputation,

factor *one*  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;

obtain generator for  $g\mathcal{O}$ .

“Do all primes have generators?”

— Restrict to a “factor base”:  
e.g., all primes of norm  $\leq y$ .

“But what if  $\alpha\mathcal{O}$  doesn't  
factor into those primes?”

— Then throw it away.  
But often it *does* factor.

Familiar issue from

“index calculus” DL methods,  
CFRAC, LS, QS, NFS, etc.

Model the norm of  $(\alpha/g)\mathcal{O}$   
as “random” integer in  $[1, x]$ ;  
 $y$ -smoothness chance  $\approx 1/y$   
if  $\log y \approx \sqrt{(1/2) \log x \log \log x}$ .

Variation: Ignore  $g\mathcal{O}$ .

Generate rather short  $\alpha \in \mathcal{O}$ ,  
factor  $\alpha\mathcal{O}$  into small primes.

After enough  $\alpha$ 's,  
solve system of equations;  
obtain generator for each prime.  
After this precomputation,  
factor *one*  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;  
obtain generator for  $g\mathcal{O}$ .

“Do all primes have generators?”

— Standard heuristics:

For many (most?) number fields,  
yes; but for big cyclotomics, no!  
Modulo a few small primes, yes.

restrict to a “factor base”:

primes of norm  $\leq y$ .

What if  $\alpha\mathcal{O}$  doesn't

factor into those primes?”

Just throw it away.

When it *does* factor.

Issue from

“lattice reduction” DL methods,

LS, QS, NFS, etc.

The norm of  $(\alpha/g)\mathcal{O}$

is a “smooth” integer in  $[1, x]$ ;

Success chance  $\approx 1/y$

$\approx \sqrt{(1/2) \log x \log \log x}$ .

Variation: Ignore  $g\mathcal{O}$ .

Generate rather short  $\alpha \in \mathcal{O}$ ,

factor  $\alpha\mathcal{O}$  into small primes.

After enough  $\alpha$ 's,

solve system of equations;

obtain generator for each prime.

After this precomputation,

factor *one*  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;

obtain generator for  $g\mathcal{O}$ .

“Do all primes have generators?”

— Standard heuristics:

For many (most?) number fields,

yes; but for big cyclotomics, no!

Modulo a few small primes, yes.

{principal

kernel of

{nonzero

$C$  is a fin

the “clas

Fundam

in algebr

factor base”:

norm  $\leq y$ .

doesn't

primes?”

away.

factor.

n

DL methods,

NFS, etc.

f  $(\alpha/g)\mathcal{O}$

ger in  $[1, x]$ ;

nce  $\approx 1/y$

$\log x \log \log x$ .

Variation: Ignore  $g\mathcal{O}$ .

Generate rather short  $\alpha \in \mathcal{O}$ ,  
factor  $\alpha\mathcal{O}$  into small primes.

After enough  $\alpha$ 's,  
solve system of equations;  
obtain generator for each prime.  
After this precomputation,  
factor *one*  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;  
obtain generator for  $g\mathcal{O}$ .

“Do all primes have generators?”

— Standard heuristics:

For many (most?) number fields,  
yes; but for big cyclotomics, no!  
Modulo a few small primes, yes.

{principal nonzero

kernel of a semigro

{nonzero ideals} -

$C$  is a finite abelian

the “class group o

Fundamental objec

in algebraic number

Variation: Ignore  $g\mathcal{O}$ .  
Generate rather short  $\alpha \in \mathcal{O}$ ,  
factor  $\alpha\mathcal{O}$  into small primes.  
After enough  $\alpha$ 's,  
solve system of equations;  
obtain generator for each prime.  
After this precomputation,  
factor *one*  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;  
obtain generator for  $g\mathcal{O}$ .

“Do all primes have generators?”

— Standard heuristics:  
For many (most?) number fields,  
yes; but for big cyclotomics, no!  
Modulo a few small primes, yes.

{principal nonzero ideals} is  
kernel of a semigroup map  
{nonzero ideals}  $\rightarrow C$  where  
 $C$  is a finite abelian group,  
the “class group of  $K$ ”.

Fundamental object of study  
in algebraic number theory.

Variation: Ignore  $g\mathcal{O}$ .

Generate rather short  $\alpha \in \mathcal{O}$ ,  
factor  $\alpha\mathcal{O}$  into small primes.

After enough  $\alpha$ 's,  
solve system of equations;  
obtain generator for each prime.  
After this precomputation,  
factor *one*  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;  
obtain generator for  $g\mathcal{O}$ .

“Do all primes have generators?”

— Standard heuristics:

For many (most?) number fields,  
yes; but for big cyclotomics, no!  
Modulo a few small primes, yes.

{principal nonzero ideals} is  
kernel of a semigroup map  
{nonzero ideals}  $\twoheadrightarrow C$  where  
 $C$  is a finite abelian group,  
the “class group of  $K$ ”.

Fundamental object of study  
in algebraic number theory.

Variation: Ignore  $g\mathcal{O}$ .  
Generate rather short  $\alpha \in \mathcal{O}$ ,  
factor  $\alpha\mathcal{O}$  into small primes.  
After enough  $\alpha$ 's,  
solve system of equations;  
obtain generator for each prime.  
After this precomputation,  
factor *one*  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;  
obtain generator for  $g\mathcal{O}$ .

“Do all primes have generators?”

— Standard heuristics:

For many (most?) number fields,  
yes; but for big cyclotomics, no!  
Modulo a few small primes, yes.

{principal nonzero ideals} is  
kernel of a semigroup map  
{nonzero ideals}  $\twoheadrightarrow C$  where  
 $C$  is a finite abelian group,  
the “class group of  $K$ ”.

Fundamental object of study  
in algebraic number theory.

Factoring many small  $\alpha\mathcal{O}$   
is a standard textbook method  
of computing class group  
and generators of ideals.

Variation: Ignore  $g\mathcal{O}$ .  
Generate rather short  $\alpha \in \mathcal{O}$ ,  
factor  $\alpha\mathcal{O}$  into small primes.  
After enough  $\alpha$ 's,  
solve system of equations;  
obtain generator for each prime.  
After this precomputation,  
factor *one*  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;  
obtain generator for  $g\mathcal{O}$ .

“Do all primes have generators?”

— Standard heuristics:

For many (most?) number fields,  
yes; but for big cyclotomics, no!  
Modulo a few small primes, yes.

{principal nonzero ideals} is  
kernel of a semigroup map  
{nonzero ideals}  $\twoheadrightarrow C$  where  
 $C$  is a finite abelian group,  
the “class group of  $K$ ”.

Fundamental object of study  
in algebraic number theory.

Factoring many small  $\alpha\mathcal{O}$   
is a standard textbook method  
of computing class group  
and generators of ideals.

Also compute unit group  $\mathcal{O}^*$   
via ratios of generators.

n: Ignore  $g\mathcal{O}$ .

e rather short  $\alpha \in \mathcal{O}$ ,

$\mathcal{O}$  into small primes.

ough  $\alpha$ 's,

stem of equations;

enerator for each prime.

is precomputation,

ne  $\alpha\mathcal{O} \subseteq g\mathcal{O}$ ;

enerator for  $g\mathcal{O}$ .

primes have generators?"

andard heuristics:

y (most?) number fields,

for big cyclotomics, no!

a few small primes, yes.

{principal nonzero ideals} is

kernel of a semigroup map

{nonzero ideals}  $\rightarrow C$  where

$C$  is a finite abelian group,

the "class group of  $K$ ".

Fundamental object of study

in algebraic number theory.

Factoring many small  $\alpha\mathcal{O}$

is a standard textbook method

of computing class group

and generators of ideals.

Also compute unit group  $\mathcal{O}^*$

via ratios of generators.

Big gene

Smart-V

this met

a genera

with larg

large, th

generato

$\theta$  may ta

Indeed, g

product

Must be

but extre

$g\mathcal{O}$ .  
 For  $\alpha \in \mathcal{O}$ ,  
 all primes.  
 Equations;  
 for each prime.  
 computation,  
 $g\mathcal{O}$ ;  
 for  $g\mathcal{O}$ .  
 "ve generators?"  
 stics:  
 number fields,  
 clonics, no!  
 all primes, yes.

{principal nonzero ideals} is  
 kernel of a semigroup map  
 {nonzero ideals}  $\rightarrow C$  where  
 $C$  is a finite abelian group,  
 the "class group of  $K$ ".

Fundamental object of study  
 in algebraic number theory.

Factoring many small  $\alpha\mathcal{O}$   
 is a standard textbook method  
 of computing class group  
 and generators of ideals.

Also compute unit group  $\mathcal{O}^*$   
 via ratios of generators.

## Big generator

Smart–Vercauteren  
 this method is like  
 a generator of large  
 with large coefficients  
 large, that writing  
 generator down as  
 $\theta$  may take exponential

Indeed, generator  
 product of powers  
 Must be  $gu$  for some  
 but extremely unlikely

$\{\text{principal nonzero ideals}\}$  is  
kernel of a semigroup map  
 $\{\text{nonzero ideals}\} \rightarrow C$  where  
 $C$  is a finite abelian group,  
the “class group of  $K$ ”.

Fundamental object of study  
in algebraic number theory.

Factoring many small  $\alpha \mathcal{O}$   
is a standard textbook method  
of computing class group  
and generators of ideals.

Also compute unit group  $\mathcal{O}^*$   
via ratios of generators.

## Big generator

Smart–Vercauteren: “However,  
this method is likely to produce  
a generator of large height,  
with large coefficients. Indeed,  
large, that writing the obtained  
generator down as a polynomial  
 $\theta$  may take exponential time.”

Indeed, generator found for  
product of powers of various  
Must be  $gu$  for some  $u \in \mathcal{O}$   
but extremely unlikely to be

$\{\text{principal nonzero ideals}\}$  is kernel of a semigroup map  $\{\text{nonzero ideals}\} \twoheadrightarrow C$  where  $C$  is a finite abelian group, the “class group of  $K$ ”.

Fundamental object of study in algebraic number theory.

Factoring many small  $\alpha \mathcal{O}$  is a standard textbook method of computing class group and generators of ideals.

Also compute unit group  $\mathcal{O}^*$  via ratios of generators.

## Big generator

Smart–Vercauteren: “However this method is likely to produce a generator of large height, i.e., with large coefficients. Indeed so large, that writing the obtained generator down as a polynomial in  $\theta$  may take exponential time.”

Indeed, generator found for  $g\mathcal{O}$  is product of powers of various  $\alpha$ 's. Must be  $gu$  for some  $u \in \mathcal{O}^*$ , but extremely unlikely to be  $g$ .

$\{\text{principal nonzero ideals}\}$  is kernel of a semigroup map  $\{\text{nonzero ideals}\} \rightarrow C$  where  $C$  is a finite abelian group, the “class group of  $K$ ”.

Fundamental object of study in algebraic number theory.

Factoring many small  $\alpha \mathcal{O}$  is a standard textbook method of computing class group and generators of ideals.

Also compute unit group  $\mathcal{O}^*$  via ratios of generators.

## Big generator

Smart–Vercauteren: “However this method is likely to produce a generator of large height, i.e., with large coefficients. Indeed so large, that writing the obtained generator down as a polynomial in  $\theta$  may take exponential time.”

Indeed, generator found for  $g\mathcal{O}$  is product of powers of various  $\alpha$ 's. Must be  $gu$  for some  $u \in \mathcal{O}^*$ , but extremely unlikely to be  $g$ .

How do we find  $g$  from  $gu$ ?

al nonzero ideals} is  
f a semigroup map  
o ideals}  $\rightarrow C$  where  
nite abelian group,  
ss group of  $K$ ".

ental object of study  
raic number theory.

g many small  $\alpha \mathcal{O}$   
dard textbook method  
uting class group  
erators of ideals.

ompute unit group  $\mathcal{O}^*$   
s of generators.

## Big generator

Smart–Vercauteren: “However  
this method is likely to produce  
a generator of large height, i.e.,  
with large coefficients. Indeed so  
large, that writing the obtained  
generator down as a polynomial in  
 $\theta$  may take exponential time.”

Indeed, generator found for  $g\mathcal{O}$  is  
product of powers of various  $\alpha$ 's.  
Must be  $gu$  for some  $u \in \mathcal{O}^*$ ,  
but extremely unlikely to be  $g$ .

How do we find  $g$  from  $gu$ ?

There are  
ring maps

{ideals} is

group map

$\Rightarrow C$  where

n group,

f  $K$ ".

ct of study

er theory.

small  $\alpha\mathcal{O}$

book method

s group

ideals.

t group  $\mathcal{O}^*$

ators.

## Big generator

Smart–Vercauteren: “However this method is likely to produce a generator of large height, i.e., with large coefficients. Indeed so large, that writing the obtained generator down as a polynomial in  $\theta$  may take exponential time.”

Indeed, generator found for  $g\mathcal{O}$  is product of powers of various  $\alpha$ 's. Must be  $gu$  for some  $u \in \mathcal{O}^*$ , but extremely unlikely to be  $g$ .

How do we find  $g$  from  $gu$ ?

There are exactly  
ring maps  $\varphi_1, \dots,$

## Big generator

Smart–Vercauteren: “However this method is likely to produce a generator of large height, i.e., with large coefficients. Indeed so large, that writing the obtained generator down as a polynomial in  $\theta$  may take exponential time.”

Indeed, generator found for  $g\mathcal{O}$  is product of powers of various  $\alpha$ 's. Must be  $gu$  for some  $u \in \mathcal{O}^*$ , but extremely unlikely to be  $g$ .

How do we find  $g$  from  $gu$ ?

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow$

## Big generator

Smart–Vercauteren: “However this method is likely to produce a generator of large height, i.e., with large coefficients. Indeed so large, that writing the obtained generator down as a polynomial in  $\theta$  may take exponential time.”

Indeed, generator found for  $g\mathcal{O}$  is product of powers of various  $\alpha$ 's. Must be  $gu$  for some  $u \in \mathcal{O}^*$ , but extremely unlikely to be  $g$ .

How do we find  $g$  from  $gu$ ?

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

## Big generator

Smart–Vercauteren: “However this method is likely to produce a generator of large height, i.e., with large coefficients. Indeed so large, that writing the obtained generator down as a polynomial in  $\theta$  may take exponential time.”

Indeed, generator found for  $g\mathcal{O}$  is product of powers of various  $\alpha$ 's. Must be  $gu$  for some  $u \in \mathcal{O}^*$ , but extremely unlikely to be  $g$ .

How do we find  $g$  from  $gu$ ?

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|)$ .

## Big generator

Smart–Vercauteren: “However this method is likely to produce a generator of large height, i.e., with large coefficients. Indeed so large, that writing the obtained generator down as a polynomial in  $\theta$  may take exponential time.”

Indeed, generator found for  $g\mathcal{O}$  is product of powers of various  $\alpha$ 's. Must be  $gu$  for some  $u \in \mathcal{O}^*$ , but extremely unlikely to be  $g$ .

How do we find  $g$  from  $gu$ ?

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|).$$

$\text{Log } \mathcal{O}^*$  is a lattice

of rank  $r_1 + r_2 - 1$  where

$$\begin{aligned} r_1 &= \#\{i : \varphi_i(K) \subseteq \mathbf{R}\}, \\ 2r_2 &= \#\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}. \end{aligned}$$

## Big generator

Smart–Vercauteren: “However this method is likely to produce a generator of large height, i.e., with large coefficients. Indeed so large, that writing the obtained generator down as a polynomial in  $\theta$  may take exponential time.”

Indeed, generator found for  $g\mathcal{O}$  is product of powers of various  $\alpha$ 's. Must be  $gu$  for some  $u \in \mathcal{O}^*$ , but extremely unlikely to be  $g$ .

How do we find  $g$  from  $gu$ ?

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|).$$

$\text{Log } \mathcal{O}^*$  is a lattice

of rank  $r_1 + r_2 - 1$  where

$$\begin{aligned} r_1 &= \#\{i : \varphi_i(K) \subseteq \mathbf{R}\}, \\ 2r_2 &= \#\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}. \end{aligned}$$

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$ :

images of  $\zeta$  under ring maps

are  $\zeta, \zeta^3, \zeta^5, \dots, \zeta^{511}$ .

$$r_1 = 0; r_2 = 128; \text{rank } 127.$$

erator

Vercauteren: “However  
method is likely to produce  
factor of large height, i.e.,  
large coefficients. Indeed so  
that writing the obtained  
factor down as a polynomial in  
takes exponential time.”

generator found for  $g\mathcal{O}$  is  
sum of powers of various  $\alpha$ 's.

$gu$  for some  $u \in \mathcal{O}^*$ ,  
extremely unlikely to be  $g$ .

how do we find  $g$  from  $gu$ ?

There are exactly  $n$  distinct  
ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|).$$

$\text{Log } \mathcal{O}^*$  is a lattice

of rank  $r_1 + r_2 - 1$  where

$$r_1 = \#\{i : \varphi_i(K) \subseteq \mathbf{R}\},$$

$$2r_2 = \#\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}.$$

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$ :

images of  $\zeta$  under ring maps

are  $\zeta, \zeta^3, \zeta^5, \dots, \zeta^{511}$ .

$$r_1 = 0; r_2 = 128; \text{rank } 127.$$

Comput

as sum of

for the c

n: “However  
 ly to produce  
 ge height, i.e.,  
 ents. Indeed so  
 the obtained  
 a polynomial in  
 ential time.”

found for  $g\mathcal{O}$  is  
 of various  $\alpha$ 's.  
 me  $u \in \mathcal{O}^*$ ,  
 kely to be  $g$ .

from  $gu$ ?

There are exactly  $n$  distinct  
 ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|).$$

$\text{Log } \mathcal{O}^*$  is a lattice

of rank  $r_1 + r_2 - 1$  where

$$r_1 = \#\{i : \varphi_i(K) \subseteq \mathbf{R}\},$$

$$2r_2 = \#\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}.$$

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$ :

images of  $\zeta$  under ring maps

are  $\zeta, \zeta^3, \zeta^5, \dots, \zeta^{511}$ .

$$r_1 = 0; r_2 = 128; \text{rank } 127.$$

Compute  $\text{Log } gu$   
 as sum of multiples  
 for the original  $\alpha$ 's

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|).$$

$\text{Log } \mathcal{O}^*$  is a lattice

of rank  $r_1 + r_2 - 1$  where

$$r_1 = \#\{i : \varphi_i(K) \subseteq \mathbf{R}\},$$

$$2r_2 = \#\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}.$$

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$ :

images of  $\zeta$  under ring maps

are  $\zeta, \zeta^3, \zeta^5, \dots, \zeta^{511}$ .

$$r_1 = 0; r_2 = 128; \text{rank } 127.$$

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$

for the original  $\alpha$ 's.

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|).$$

$\text{Log } \mathcal{O}^*$  is a lattice

of rank  $r_1 + r_2 - 1$  where

$$r_1 = \#\{i : \varphi_i(K) \subseteq \mathbf{R}\},$$

$$2r_2 = \#\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}.$$

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$ :

images of  $\zeta$  under ring maps

are  $\zeta, \zeta^3, \zeta^5, \dots, \zeta^{511}$ .

$r_1 = 0$ ;  $r_2 = 128$ ; rank 127.

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$

for the original  $\alpha$ 's.

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|).$$

$\text{Log } \mathcal{O}^*$  is a lattice

of rank  $r_1 + r_2 - 1$  where

$$r_1 = \#\{i : \varphi_i(K) \subseteq \mathbf{R}\},$$

$$2r_2 = \#\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}.$$

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$ :

images of  $\zeta$  under ring maps

are  $\zeta, \zeta^3, \zeta^5, \dots, \zeta^{511}$ .

$$r_1 = 0; r_2 = 128; \text{rank } 127.$$

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$

for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$

close to  $\text{Log } gu$ .

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|).$$

$\text{Log } \mathcal{O}^*$  is a lattice

of rank  $r_1 + r_2 - 1$  where

$$r_1 = \#\{i : \varphi_i(K) \subseteq \mathbf{R}\},$$
$$2r_2 = \#\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}.$$

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$ :

images of  $\zeta$  under ring maps

are  $\zeta, \zeta^3, \zeta^5, \dots, \zeta^{511}$ .

$r_1 = 0$ ;  $r_2 = 128$ ; rank 127.

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$

for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$

close to  $\text{Log } gu$ .

This is a close-vector problem

(“bounded-distance decoding”).

“Embedding” heuristic:

CVP as fast as SVP.

There are exactly  $n$  distinct ring maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

Define  $\text{Log} : K^* \rightarrow \mathbf{R}^n$  by

$$\text{Log} = (\log |\varphi_1|, \dots, \log |\varphi_n|).$$

$\text{Log } \mathcal{O}^*$  is a lattice

of rank  $r_1 + r_2 - 1$  where

$$r_1 = \#\{i : \varphi_i(K) \subseteq \mathbf{R}\},$$
$$2r_2 = \#\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}.$$

e.g.  $\zeta = \exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$ :

images of  $\zeta$  under ring maps

are  $\zeta, \zeta^3, \zeta^5, \dots, \zeta^{511}$ .

$r_1 = 0$ ;  $r_2 = 128$ ; rank 127.

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$  for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$  close to  $\text{Log } gu$ .

This is a close-vector problem (“bounded-distance decoding”).

“Embedding” heuristic:

CVP as fast as SVP.

This finds  $\text{Log } u$ .

Easily reconstruct  $g$

up to a root of unity.

$\#\{\text{roots of unity}\}$  is small.

are exactly  $n$  distinct  
maps  $\varphi_1, \dots, \varphi_n : K \rightarrow \mathbf{C}$ .

$\log : K^* \rightarrow \mathbf{R}^n$  by  
 $(\log |\varphi_1|, \dots, \log |\varphi_n|)$ .

is a lattice

$r_1 + r_2 - 1$  where

$\{i : \varphi_i(K) \subseteq \mathbf{R}\}$ ,

$\{i : \varphi_i(K) \not\subseteq \mathbf{R}\}$ .

$\exp(\pi i/256)$ ,  $K = \mathbf{Q}(\zeta)$ :

of  $\zeta$  under ring maps

$\zeta, \zeta^5, \dots, \zeta^{511}$ .

$r_2 = 128$ ; rank 127.

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$   
for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$   
close to  $\text{Log } gu$ .

This is a close-vector problem  
("bounded-distance decoding").

"Embedding" heuristic:

CVP as fast as SVP.

This finds  $\text{Log } u$ .

Easily reconstruct  $g$

up to a root of unity.

$\#\{\text{roots of unity}\}$  is small.

A subfield

(2014.02)

Say we have

for a product

$n$  distinct

$\varphi_n : K \rightarrow \mathbf{C}$ .

$\rightarrow \mathbf{R}^n$  by

$(\cdot, \log |\varphi_n|)$ .

L where

$\subseteq \mathbf{R}$ ,

$\not\subseteq \mathbf{R}$ .

(56),  $K = \mathbf{Q}(\zeta)$ :

ring maps

511.

rank 127.

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$   
for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$   
close to  $\text{Log } gu$ .

This is a close-vector problem  
("bounded-distance decoding").

"Embedding" heuristic:

CVP as fast as SVP.

This finds  $\text{Log } u$ .

Easily reconstruct  $g$

up to a root of unity.

$\#\{\text{roots of unity}\}$  is small.

A subfield-logarithm

(2014.02 Bernstein)

Say we know  $\text{Log } m$   
for a proper subfield

C. Compute  $\text{Log } gu$   
as sum of multiples of  $\text{Log } \alpha$   
for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$   
close to  $\text{Log } gu$ .

This is a close-vector problem  
(“bounded-distance decoding”).

“Embedding” heuristic:  
CVP as fast as SVP.

This finds  $\text{Log } u$ .

Easily reconstruct  $g$   
up to a root of unity.

$\#\{\text{roots of unity}\}$  is small.

A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$   
for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$   
close to  $\text{Log } gu$ .

This is a close-vector problem  
(“bounded-distance decoding”).

“Embedding” heuristic:

CVP as fast as SVP.

This finds  $\text{Log } u$ .

Easily reconstruct  $g$

up to a root of unity.

$\#\{\text{roots of unity}\}$  is small.

A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$   
for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$   
close to  $\text{Log } gu$ .

This is a close-vector problem  
(“bounded-distance decoding”).

“Embedding” heuristic:

CVP as fast as SVP.

This finds  $\text{Log } u$ .

Easily reconstruct  $g$

up to a root of unity.

$\#\{\text{roots of unity}\}$  is small.

A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

We also know  $\text{Log norm}_{K:F} gu$ ,  
so we know  $\text{Log norm}_{K:F} u$ .

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$   
for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$   
close to  $\text{Log } gu$ .

This is a close-vector problem  
("bounded-distance decoding").

"Embedding" heuristic:

CVP as fast as SVP.

This finds  $\text{Log } u$ .

Easily reconstruct  $g$

up to a root of unity.

$\#\{\text{roots of unity}\}$  is small.

A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

We also know  $\text{Log norm}_{K:F} gu$ ,  
so we know  $\text{Log norm}_{K:F} u$ .

This linearly constrains  $\text{Log } u$   
to a shifted sublattice of  $\text{Log } \mathcal{O}^*$ .

Number of independent  
constraints: unit rank for  $F$ .

Compute  $\text{Log } gu$

as sum of multiples of  $\text{Log } \alpha$   
for the original  $\alpha$ 's.

Find elements of  $\text{Log } \mathcal{O}^*$   
close to  $\text{Log } gu$ .

This is a close-vector problem  
("bounded-distance decoding").

"Embedding" heuristic:

CVP as fast as SVP.

This finds  $\text{Log } u$ .

Easily reconstruct  $g$

up to a root of unity.

$\#\{\text{roots of unity}\}$  is small.

A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

We also know  $\text{Log norm}_{K:F} gu$ ,  
so we know  $\text{Log norm}_{K:F} u$ .

This linearly constrains  $\text{Log } u$   
to a shifted sublattice of  $\text{Log } \mathcal{O}^*$ .

Number of independent  
constraints: unit rank for  $F$ .

Find elements close to  $\text{Log } gu$ .

Lower-dimension lattice problem,  
if unit rank of  $F$  is positive.

the  $\text{Log } gu$

of multiples of  $\text{Log } \alpha$   
original  $\alpha$ 's.

elements of  $\text{Log } \mathcal{O}^*$

$\text{Log } gu$ .

a close-vector problem  
(“nearest-distance decoding”).

“nearest” heuristic:

as fast as SVP.

finds  $\text{Log } u$ .

reconstruct  $g$

root of unity.

{roots of unity} is small.

## A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

We also know  $\text{Log norm}_{K:F} gu$ ,  
so we know  $\text{Log norm}_{K:F} u$ .

This linearly constrains  $\text{Log } u$   
to a shifted sublattice of  $\text{Log } \mathcal{O}^*$ .

Number of independent  
constraints: unit rank for  $F$ .

Find elements close to  $\text{Log } gu$ .

Lower-dimension lattice problem,  
if unit rank of  $F$  is positive.

Start by

Log norm  
for each

Various  
dependin

## A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

We also know  $\text{Log norm}_{K:F} g u$ ,  
so we know  $\text{Log norm}_{K:F} u$ .

This linearly constrains  $\text{Log } u$   
to a shifted sublattice of  $\text{Log } \mathcal{O}^*$ .

Number of independent  
constraints: unit rank for  $F$ .

Find elements close to  $\text{Log } g u$ .

Lower-dimension lattice problem,  
if unit rank of  $F$  is positive.

Start by recursively

$\text{Log norm}_{K:F} g$  via  
for each  $F \subset K$ .

Various constraints  
depending on subf

## A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

We also know  $\text{Log norm}_{K:F} g u$ ,  
so we know  $\text{Log norm}_{K:F} u$ .

This linearly constrains  $\text{Log } u$   
to a shifted sublattice of  $\text{Log } \mathcal{O}^*$ .

Number of independent  
constraints: unit rank for  $F$ .

Find elements close to  $\text{Log } g u$ .

Lower-dimension lattice problem,  
if unit rank of  $F$  is positive.

Start by recursively computing

$\text{Log norm}_{K:F} g$  via norm of  $g$   
for each  $F \subset K$ .

Various constraints on  $\text{Log } u$   
depending on subfield structure.

## A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

We also know  $\text{Log norm}_{K:F} g u$ ,  
so we know  $\text{Log norm}_{K:F} u$ .

This linearly constrains  $\text{Log } u$   
to a shifted sublattice of  $\text{Log } \mathcal{O}^*$ .

Number of independent  
constraints: unit rank for  $F$ .

Find elements close to  $\text{Log } g u$ .

Lower-dimension lattice problem,  
if unit rank of  $F$  is positive.

Start by recursively computing  
 $\text{Log norm}_{K:F} g$  via norm of  $g \mathcal{O}$   
for each  $F \subset K$ .

Various constraints on  $\text{Log } u$ ,  
depending on subfield structure.

## A subfield-logarithm attack

(2014.02 Bernstein)

Say we know  $\text{Log norm}_{K:F} g$   
for a proper subfield  $F \subset K$ .

We also know  $\text{Log norm}_{K:F} g u$ ,  
so we know  $\text{Log norm}_{K:F} u$ .

This linearly constrains  $\text{Log } u$   
to a shifted sublattice of  $\text{Log } \mathcal{O}^*$ .  
Number of independent  
constraints: unit rank for  $F$ .

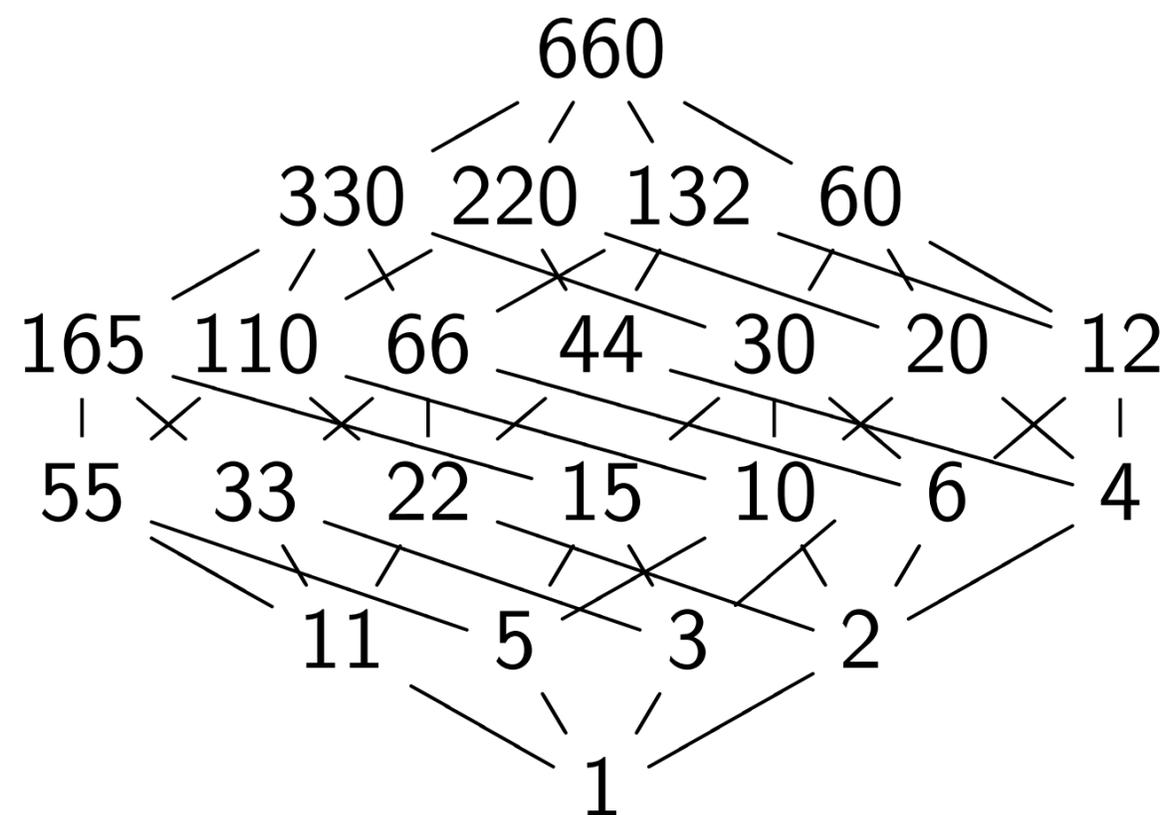
Find elements close to  $\text{Log } g u$ .  
Lower-dimension lattice problem,  
if unit rank of  $F$  is positive.

Start by recursively computing  
 $\text{Log norm}_{K:F} g$  via norm of  $g \mathcal{O}$   
for each  $F \subset K$ .

Various constraints on  $\text{Log } u$ ,  
depending on subfield structure.

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$ .

Degrees of subfields of  $K$ :



# Field-logarithm attack

(Bernstein)

know  $\text{Log norm}_{K:F} g$   
proper subfield  $F \subset K$ .

know  $\text{Log norm}_{K:F} g u$ ,  
know  $\text{Log norm}_{K:F} u$ .

early constrains  $\text{Log } u$

ated sublattice of  $\text{Log } \mathcal{O}^*$ .

of independent

nts: unit rank for  $F$ .

ments close to  $\text{Log } g u$ .

imension lattice problem,

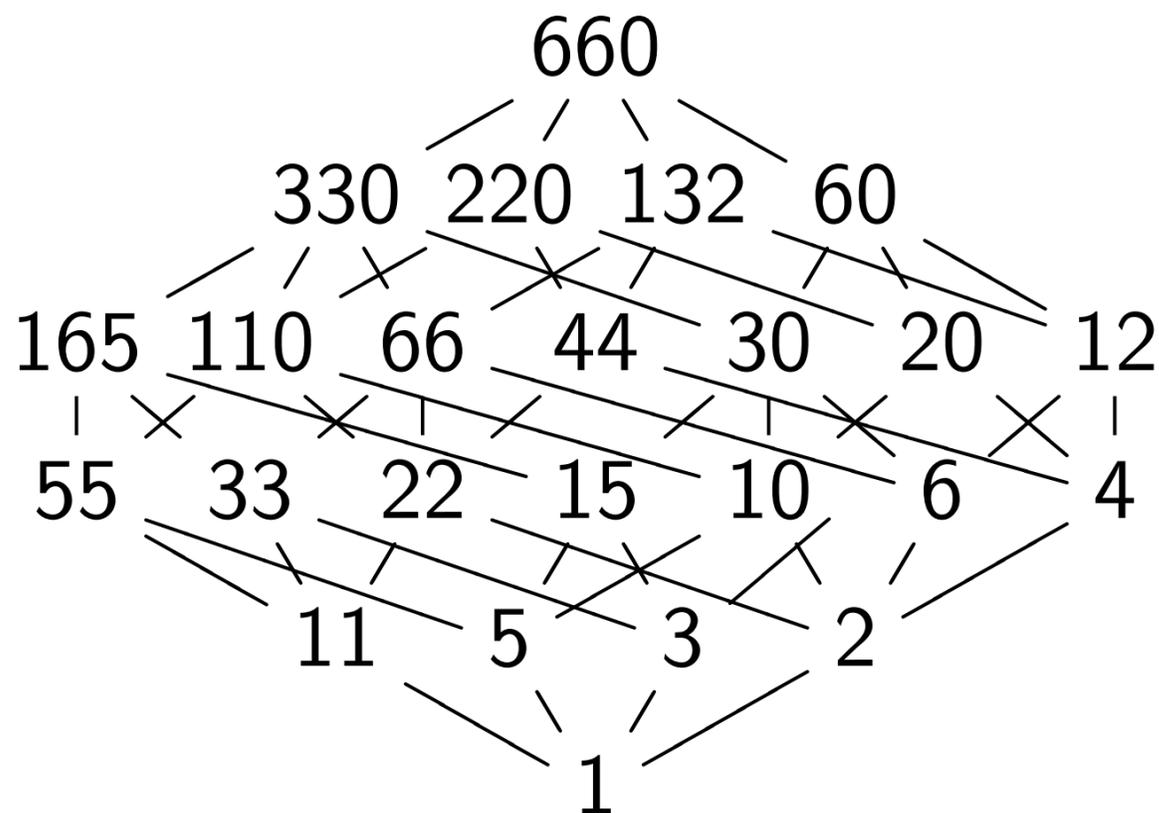
rank of  $F$  is positive.

Start by recursively computing  
 $\text{Log norm}_{K:F} g$  via norm of  $g \mathcal{O}$   
for each  $F \subset K$ .

Various constraints on  $\text{Log } u$ ,  
depending on subfield structure.

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$ .

Degrees of subfields of  $K$ :



Most ex

Compos

$K = \mathbf{Q}(\zeta)$

CVP bec

m attack

n)

$\text{norm}_{K:F} g$

field  $F \subset K$ .

$\text{norm}_{K:F} g u$ ,

$\text{norm}_{K:F} u$ .

constraints  $\text{Log } u$

lattice of  $\text{Log } \mathcal{O}^*$ .

independent

rank for  $F$ .

use to  $\text{Log } g u$ .

lattice problem,

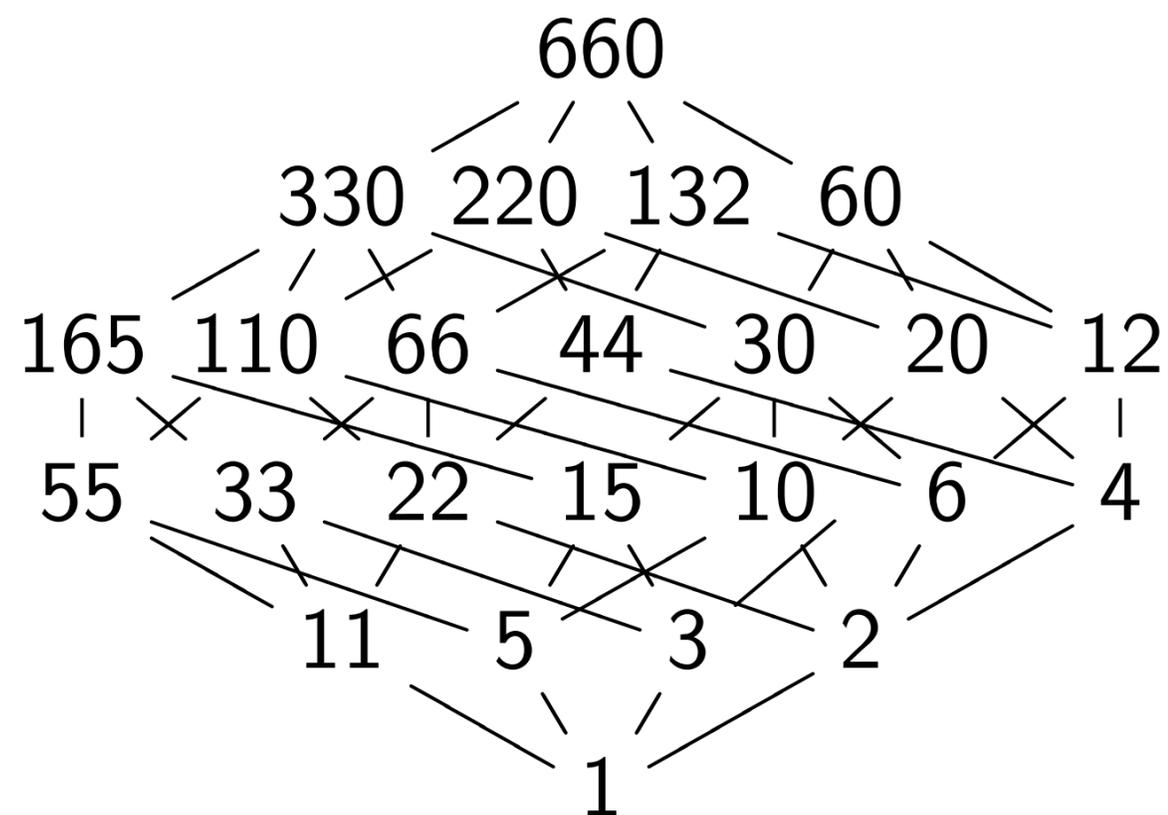
is positive.

Start by recursively computing  
 $\text{Log norm}_{K:F} g$  via norm of  $g \mathcal{O}$   
for each  $F \subset K$ .

Various constraints on  $\text{Log } u$ ,  
depending on subfield structure.

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$ .

Degrees of subfields of  $K$ :



Most extreme case

Composite of quad

$K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

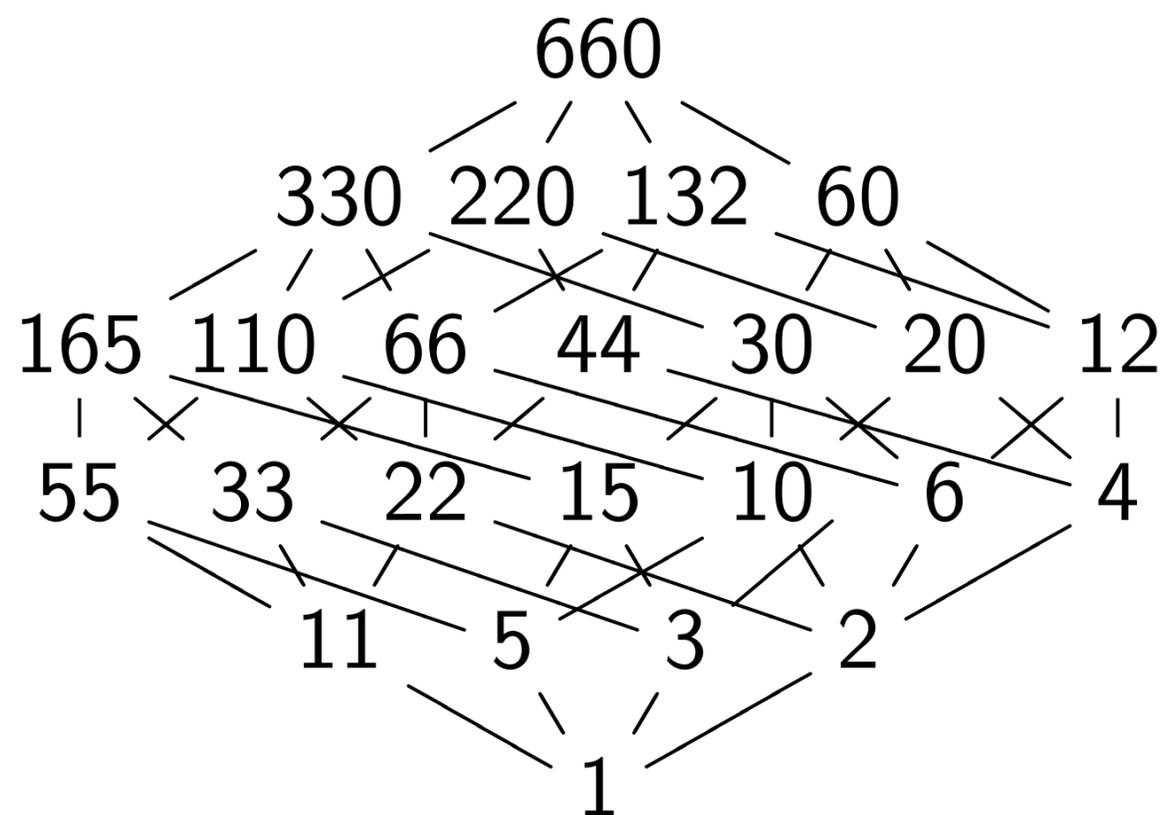
CVP becomes triv

Start by recursively computing  
 $\text{Log norm}_{K:F} g$  via norm of  $g \mathcal{O}$   
 for each  $F \subset K$ .

Various constraints on  $\text{Log } u$ ,  
 depending on subfield structure.

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$ .

Degrees of subfields of  $K$ :



Most extreme case:

Composite of quadratics, such as

$$K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$$

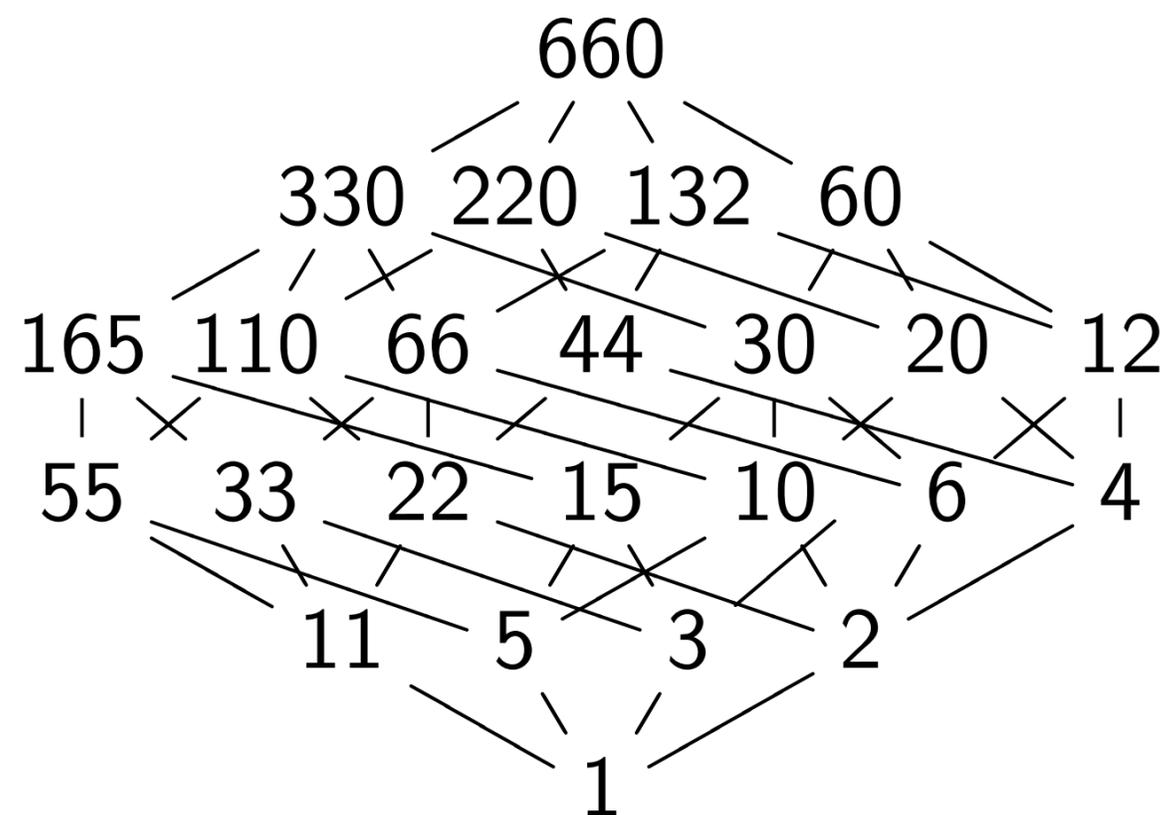
CVP becomes trivial!

Start by recursively computing  
 $\text{Log norm}_{K:F} g$  via norm of  $g\mathcal{O}$   
 for each  $F \subset K$ .

Various constraints on  $\text{Log } u$ ,  
 depending on subfield structure.

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$ .

Degrees of subfields of  $K$ :



Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

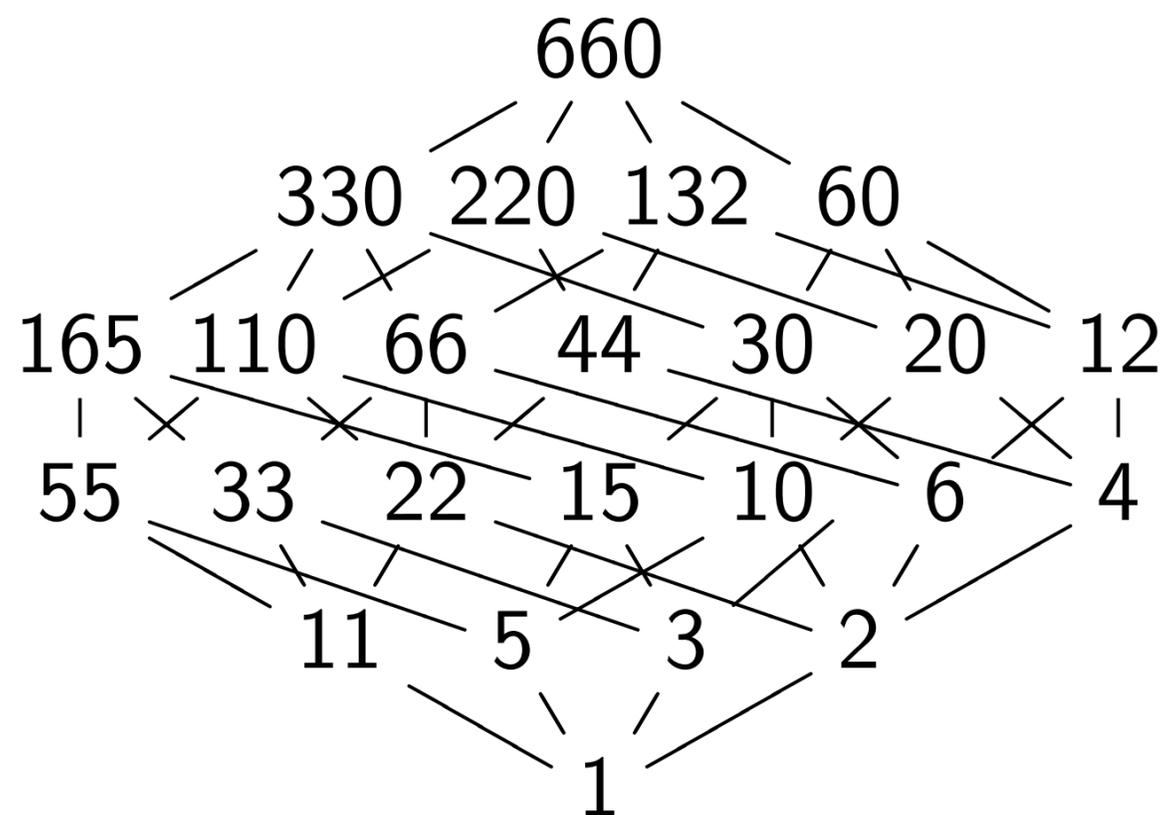
CVP becomes trivial!

Start by recursively computing  
 $\text{Log norm}_{K:F} g$  via norm of  $g\mathcal{O}$   
 for each  $F \subset K$ .

Various constraints on  $\text{Log } u$ ,  
 depending on subfield structure.

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$ .

Degrees of subfields of  $K$ :



Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

CVP becomes trivial!

Opposite extreme: prime degree;  
 the only proper subfield is  $\mathbf{Q}$ .

My recommendation: big Galois  
 group; e.g.,  $\mathbf{Q}[x]/(x^p - x - 1)$ .

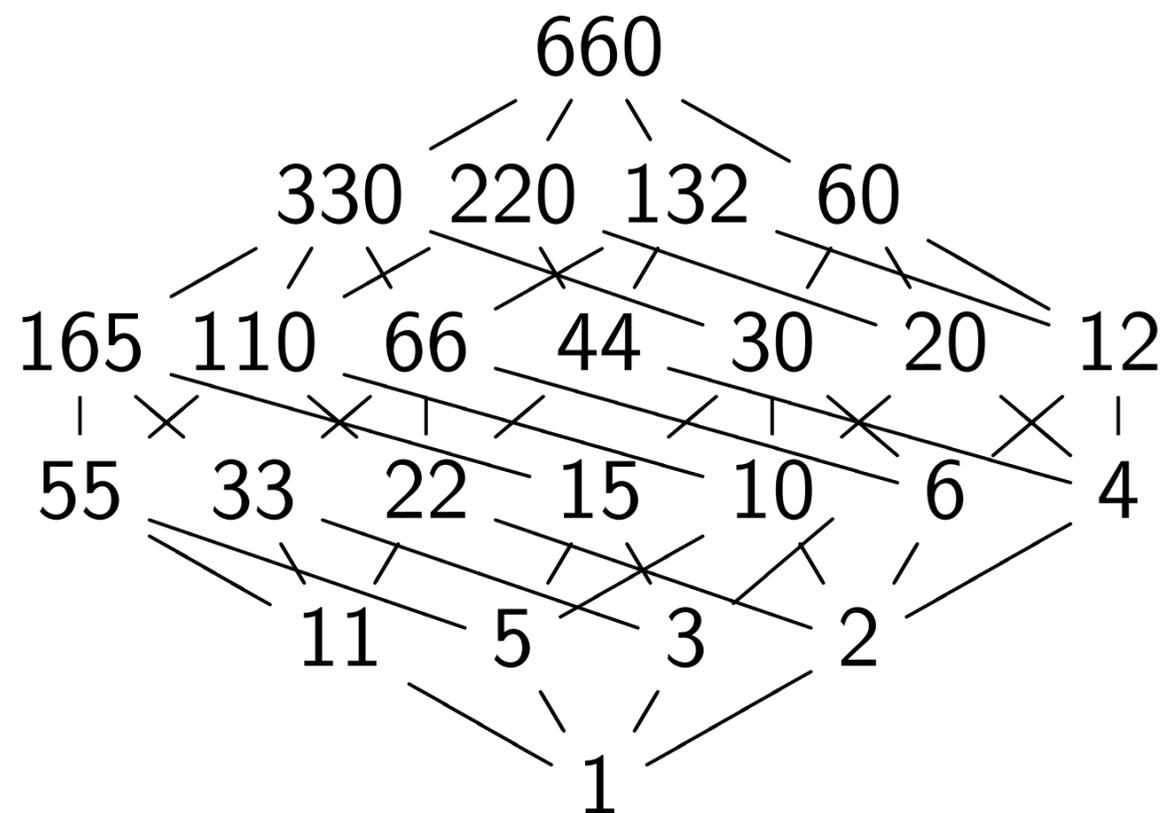
Many intermediate cases.

Start by recursively computing  
 $\text{Log norm}_{K:F} g$  via norm of  $g\mathcal{O}$   
 for each  $F \subset K$ .

Various constraints on  $\text{Log } u$ ,  
 depending on subfield structure.

e.g.  $\zeta = \exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$ .

Degrees of subfields of  $K$ :



Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

CVP becomes trivial!

Opposite extreme: prime degree;  
 the only proper subfield is  $\mathbf{Q}$ .

My recommendation: big Galois  
 group; e.g.,  $\mathbf{Q}[x]/(x^p - x - 1)$ .

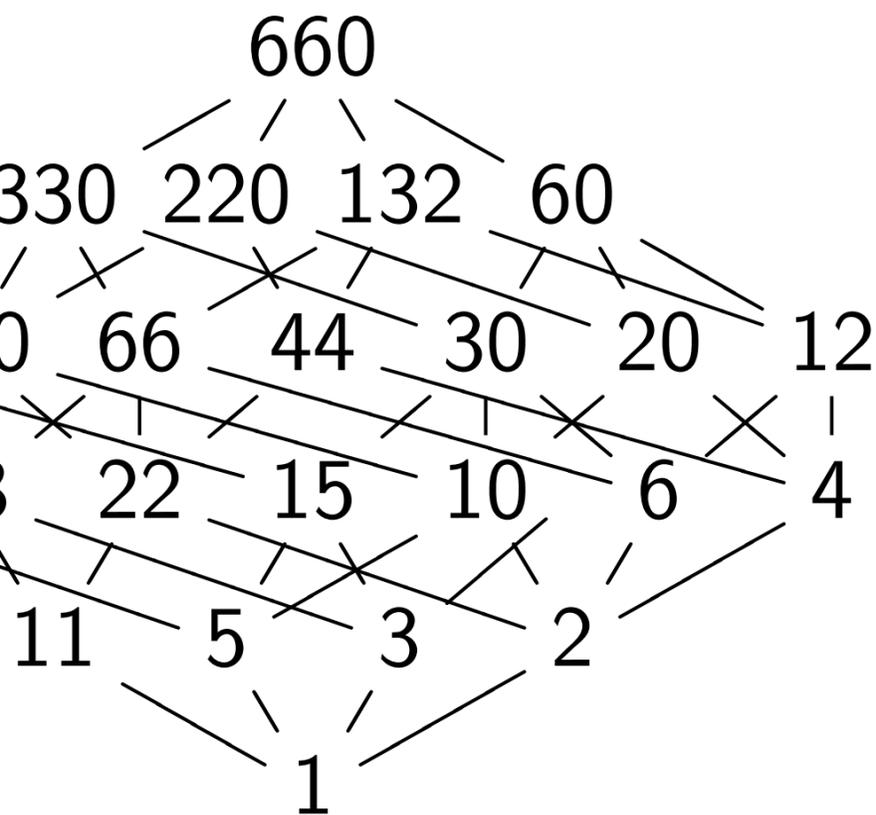
Many intermediate cases.

Confused summary by Cramer–  
 Ducas–Peikert–Regev: method  
 “may yield slightly subexponential  
 runtimes in *cyclotomic* rings of  
*highly smooth* index”.

recursively computing  
 $n_{K:F} g$  via norm of  $g \in \mathcal{O}_K$   
 $F \subset K$ .

constraints on  $\text{Log } u$ ,  
 on subfield structure.

$\exp(2\pi i/661)$ ,  $K = \mathbf{Q}(\zeta)$ .  
 of subfields of  $K$ :



Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

CVP becomes trivial!

Opposite extreme: prime degree;  
 the only proper subfield is  $\mathbf{Q}$ .

My recommendation: big Galois  
 group; e.g.,  $\mathbf{Q}[x]/(x^p - x - 1)$ .

Many intermediate cases.

Confused summary by Cramer–  
 Ducas–Peikert–Regev: method  
 “may yield slightly subexponential  
 runtimes in *cyclotomic* rings of  
*highly smooth* index”.

Further

① 2014

Shepher

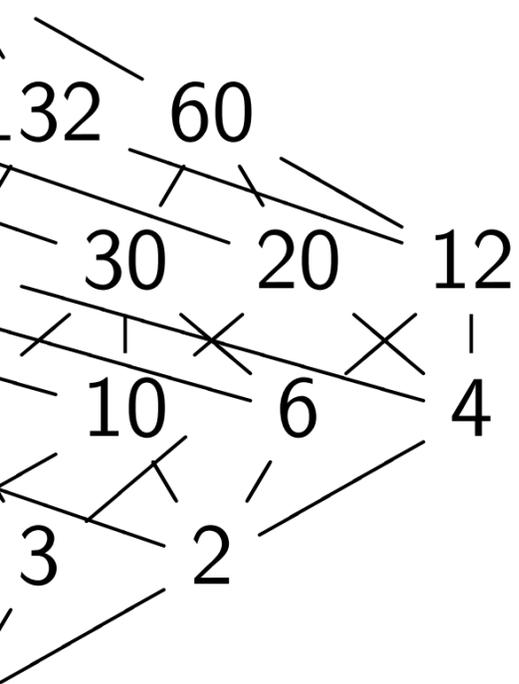
for **cyclo**

(good) b

by computing  
norm of  $g\mathcal{O}$

s on  $\text{Log } u$ ,  
field structure.

661),  $K = \mathbf{Q}(\zeta)$ .  
ds of  $K$ :



Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

CVP becomes trivial!

Opposite extreme: prime degree;  
the only proper subfield is  $\mathbf{Q}$ .

My recommendation: big Galois  
group; e.g.,  $\mathbf{Q}[x]/(x^p - x - 1)$ .

Many intermediate cases.

Confused summary by Cramer–  
Ducas–Peikert–Regev: method  
“may yield slightly subexponential  
runtimes in *cyclotomic* rings of  
*highly smooth* index” .

Further improvements

① 2014.10 Camp  
Shepherd: Quickly  
for **cyclotomics** u  
(good) basis for cy

ng

gO

,

ure.

$\mathbf{Q}(\zeta)$ .

12  
4

Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

CVP becomes trivial!

Opposite extreme: prime degree;  
the only proper subfield is  $\mathbf{Q}$ .

My recommendation: big Galois  
group; e.g.,  $\mathbf{Q}[x]/(x^p - x - 1)$ .

Many intermediate cases.

Confused summary by Cramer–  
Ducas–Peikert–Regev: method  
“may yield slightly subexponential  
runtimes in *cyclotomic* rings of  
*highly smooth* index”.

Further improvements: ①,

① 2014.10 Campbell–Grover  
Shepherd: Quickly solve CV  
for **cyclotomics** using know  
(good) basis for cyclotomic

Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

CVP becomes trivial!

Opposite extreme: prime degree;  
the only proper subfield is  $\mathbf{Q}$ .

My recommendation: big Galois  
group; e.g.,  $\mathbf{Q}[x]/(x^p - x - 1)$ .

Many intermediate cases.

Confused summary by Cramer–  
Ducas–Peikert–Regev: method  
“may yield slightly subexponential  
runtimes in *cyclotomic* rings of  
*highly smooth* index”.

Further improvements: ①, ②

① 2014.10 Campbell–Groves–  
Shepherd: Quickly solve CVP  
for **cyclotomics** using known  
(good) basis for cyclotomic units.

Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

CVP becomes trivial!

Opposite extreme: prime degree;  
the only proper subfield is  $\mathbf{Q}$ .

My recommendation: big Galois  
group; e.g.,  $\mathbf{Q}[x]/(x^p - x - 1)$ .

Many intermediate cases.

Confused summary by Cramer–  
Ducas–Peikert–Regev: method  
“may yield slightly subexponential  
runtimes in *cyclotomic* rings of  
*highly smooth* index”.

Further improvements: ①, ②

① 2014.10 Campbell–Groves–  
Shepherd: Quickly solve CVP  
for **cyclotomics** using known  
(good) basis for cyclotomic units.

Analysis in paper is bogus,  
but algorithm is very fast.

Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

CVP becomes trivial!

Opposite extreme: prime degree;  
the only proper subfield is  $\mathbf{Q}$ .

My recommendation: big Galois  
group; e.g.,  $\mathbf{Q}[x]/(x^p - x - 1)$ .

Many intermediate cases.

Confused summary by Cramer–  
Ducas–Peikert–Regev: method  
“may yield slightly subexponential  
runtimes in *cyclotomic* rings of  
*highly smooth* index”.

Further improvements: ①, ②

① 2014.10 Campbell–Groves–  
Shepherd: Quickly solve CVP  
for **cyclotomics** using known  
(good) basis for cyclotomic units.

Analysis in paper is bogus,  
but algorithm is very fast.

Plagiarized and properly analyzed  
by Cramer–Ducas–Peikert–Regev.

Most extreme case:

Composite of quadratics, such as  
 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{29})$ .

CVP becomes trivial!

Opposite extreme: prime degree;  
the only proper subfield is  $\mathbf{Q}$ .

My recommendation: big Galois  
group; e.g.,  $\mathbf{Q}[x]/(x^p - x - 1)$ .

Many intermediate cases.

Confused summary by Cramer–  
Ducas–Peikert–Regev: method  
“may yield slightly subexponential  
runtimes in *cyclotomic* rings of  
*highly smooth* index”.

Further improvements: ①, ②

① 2014.10 Campbell–Groves–  
Shepherd: Quickly solve CVP  
for **cyclotomics** using known  
(good) basis for cyclotomic units.

Analysis in paper is bogus,  
but algorithm is very fast.

Plagiarized and properly analyzed  
by Cramer–Ducas–Peikert–Regev.

② 2015.01 Song announcement:  
Fast **quantum** algorithm for  $gu$ .  
“PIP ... solved [BiasseSong'14]” .  
But paper not available yet.