A subfield-logarithm attack
against ideal lattices,
part 1: the number-field sieve

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

Sieving small integers $i > 0$
using primes $2, 3, 5, 7$:

1	
2	2
3	3
4	2 2
5	5
6	2 3
7	7
8	2 2 2
9	3 3
10	2 5
11	
12	2 2 3
13	
14	2 7
15	3 5
16	2 2 2 2
17	
18	2 3 3
19	
20	2 2 5

etc.

A subfield-logarithm attack
against ideal lattices,
part 1: the number-field sieve

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

Sieving i and $611 + i$ for small i
using primes $2, 3, 5, 7$:

1	
2	2
3	3
4	2 2
5	5
6	2 3
7	7
8	2 2 2
9	3 3
10	2 5
11	
12	2 2 3
13	
14	2 7
15	3 5
16	2 2 2 2
17	
18	2 3 3
19	
20	2 2 5

612	2 2 3 3
613	
614	2
615	3 5
616	2 2 2 7
617	
618	2 3
619	
620	2 2 5
621	3 3 3
622	2
623	7
624	2 2 2 2 3
625	5 5 5 5
626	2
627	3
628	2 2
629	
630	2 3 3 5 7
631	

etc.

ld-logarithm attack
ideal lattices,
the number-field sieve

ernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven

Sieving i and $611 + i$ for small i using primes $2, 3, 5, 7$:

1	
2	2
3	3
4	2 2
5	5
6	2 3
7	7
8	2 2 2
9	3 3
10	2 5
11	
12	2 2 3
13	
14	2 7
15	3 5
16	2 2 2 2
17	
18	2 3 3
19	
20	2 2 5

612	2 2 3 3
613	
614	2
615	3 5
616	2 2 2 7
617	
618	2 3
619	
620	2 2 5
621	3 3 3
622	2
623	7
624	2 2 2 2 3
625	5 5 5 5
626	2
627	3
628	2 2
629	
630	2 3 3 5 7
631	

etc.

Have co
the "con
for some

$14 \cdot 625$
$64 \cdot 675$
$75 \cdot 686$

$14 \cdot 64 \cdot$
$= 2^8 3^4 5$

$\gcd\{611$
$= 47.$

$611 = 4$

m attack
ces,
er-field sieve

is at Chicago &
siteit Eindhoven

Sieving i and $611 + i$ for small i using primes $2, 3, 5, 7$:

1	
2	2
3	3
4	2 2
5	5
6	2 3
7	7
8	2 2 2
9	3 3
10	2 5
11	
12	2 2 3
13	
14	2 7
15	3 5
16	2 2 2 2
17	
18	2 3 3
19	
20	2 2 5

612	2 2 3 3
613	
614	2
615	3 5
616	2 2 2 7
617	
618	2 3
619	
620	2 2 5
621	3 3 3
622	2
623	7
624	2 2 2 2 3
625	5 5 5 5
626	2
627	3
628	2 2
629	
630	2 3 3 5 7
631	

etc.

Have complete fac
the "congruences"
for some i's.

$14 \cdot 625 = 2^1 3^0 5^4$
$64 \cdot 675 = 2^6 3^3 5^2$
$75 \cdot 686 = 2^1 3^1 5^2$

$14 \cdot 64 \cdot 75 \cdot 625 \cdot$
$= 2^8 3^4 5^8 7^4 = (2^4$

$\gcd\{611, 14 \cdot 64 \cdot$
$= 47.$

$611 = 47 \cdot 13.$

ve

ago &

hoven

Sieving i and $611 + i$ for small i using primes $2, 3, 5, 7$:

1	
2	2
3	3
4	2 2
5	5
6	2 3
7	7
8	2 2 2
9	3 3
10	2 5
11	
12	2 2 3
13	
14	2 7
15	3 5
16	2 2 2 2
17	
18	2 3 3
19	
20	2 2 5

612	2 2 3 3
613	
614	2
615	3 5
616	2 2 2 7
617	
618	2 3
619	
620	2 2 5
621	3 3 3
622	2
623	7
624	2 2 2 2 3
625	5 5 5 5
626	2
627	3
628	2 2
629	
630	2 3 3 5 7
631	

etc.

Have complete factorization
the "congruences" $i(611 + i$
for some i's.

$$14 \cdot 625 = 2^1 3^0 5^4 7^1.$$
$$64 \cdot 675 = 2^6 3^3 5^2 7^0.$$
$$75 \cdot 686 = 2^1 3^1 5^2 7^3.$$

$$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$$
$$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2.$$

$$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5$$
$$= 47.$$

$$611 = 47 \cdot 13.$$

Sieving i and $611 + i$ for small i using primes $2, 3, 5, 7$:

1				
2	2			
3		3		
4	2	2		
5			5	
6	2	3		
7				7
8	2	2	2	
9		3	3	
10	2		5	
11				
12	2	2	3	
13				
14	2			7
15		3	5	
16	2	2	2	2
17				
18	2	3	3	
19				
20	2	2	5	

612	2	2		3	3			
613								
614	2							
615				3		5		
616	2	2	2					7
617								
618	2			3				
619								
620	2	2				5		
621				3	3	3		
622	2							
623								7
624	2	2	2	2	3			
625						5	5	5 5
626	2							
627				3				
628	2	2						
629								
630	2			3	3	5		7
631								

etc.

Have complete factorization of the "congruences" $i(611 + i)$ for some i's.

$$14 \cdot 625 = 2^1 3^0 5^4 7^1.$$
$$64 \cdot 675 = 2^6 3^3 5^2 7^0.$$
$$75 \cdot 686 = 2^1 3^1 5^2 7^3.$$

$$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$$
$$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2.$$

$$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$$
$$= 47.$$

$$611 = 47 \cdot 13.$$

i and $611 + i$ for small i

imes 2, 3, 5, 7:

	5	
		7
3		
	5	
		7
	5	
3		
	5	

612	2	2			3	3						
613												
614	2											
615					3			5				
616	2	2	2									7
617												
618	2				3							
619												
620	2	2						5				
621					3	3	3					
622	2											
623												7
624	2	2	2	2	3							
625								5	5	5	5	
626	2											
627					3							
628	2	2										
629												
630	2				3	3		5				7
631												

Have complete factorization of the "congruences" $i(611 + i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

Why did

Was it ju

gcd{611

$+ i$ for small i

$5, 7$:

2		3	3				
		3		5			
2	2						7
		3					
2				5			
		3	3	3			
							7
2	2	2	3				
				5	5	5	5
		3					
2							
		3	3	5			7

Have complete factorization of the "congruences" $i(611 + i)$ for some i's.

$$14 \cdot 625 = 2^1 3^0 5^4 7^1.$$
$$64 \cdot 675 = 2^6 3^3 5^2 7^0.$$
$$75 \cdot 686 = 2^1 3^1 5^2 7^3.$$

$$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$$
$$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2.$$

$$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$$
$$= 47.$$

$$611 = 47 \cdot 13.$$

Why did this find
Was it just blind l
$\gcd\{611, \text{random}\}$

hall i

7

7

5 5 5

7

Have complete factorization of the "congruences" $i(611+i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

Why did this find a factor o
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

Have complete factorization of the "congruences" $i(611+i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

Have complete factorization of the "congruences" $i(611+i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime >7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

mplete factorization of
ngruences" $i(611+i)$
e i's.

$= 2^1 3^0 5^4 7^1$.
$= 2^6 3^3 5^2 7^0$.
$= 2^1 3^1 5^2 7^3$.

$75 \cdot 625 \cdot 675 \cdot 686$
$^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$

$7 \cdot 13$.

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime >7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did
complete
have squ
Was it ju

ctorization of
$i(611+i)$

7^1.
7^0.
7^3.

$675 \cdot 686$
$3^2 5^4 7^2)^2$.

$75 - 2^4 3^2 5^4 7^2\}$

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime >7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first
completely factore
have square produ
Was it just blind l

of
$\tilde{c}$)

$5^4 7^2\}$

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime >7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first three
completely factored congrue
have square product?
Was it just blind luck?

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime >7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime >7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1, 0, 4, 1), (6, 3, 2, 0), (1, 1, 2, 3)$
happened to have sum 0 mod 2.

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime >7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1, 0, 4, 1), (6, 3, 2, 0), (1, 1, 2, 3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
quickly find
nonempty subsequence
with sum 0 mod 2.

l this find a factor of 611?
ust blind luck:
, random$\} = 47$?

truction 611 divides $s^2 - t^2$
$= 14 \cdot 64 \cdot 75$
$2^4 3^2 5^4 7^2$.
prime >7 dividing 611
either $s - t$ or $s + t$.

ibly surprising
guaranteed in advance!)
prime divided $s - t$
other divided $s + t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1, 0, 4, 1), (6, 3, 2, 0), (1, 1, 2, 3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
quickly find
nonempty subsequence
with sum 0 mod 2.

This is l
Guarant
if numbe
exceeds

e.g. for
$1(n +$
$4(n +$
$15(n +$
$49(n +$
$64(n +$

a factor of 611?

uck:

$= 47$?

11 divides s^2-t^2

$\cdot 75$

dividing 611

t or $s+t$.

sing

ed in advance!)

vided $s-t$

ded $s+t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1,0,4,1),(6,3,2,0),(1,1,2,3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
quickly find
nonempty subsequence
with sum 0 mod 2.

This is linear algeb
Guaranteed to find
if number of vecto
exceeds length of

e.g. for $n = 671$:

$1(n+1) = 2^5 3$

$4(n+4) = 2^2 3$

$15(n+15) = 2^1 3$

$49(n+49) = 2^4 3$

$64(n+64) = 2^6 3$

f 611?

s^2-t^2

611

nce!)

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1,0,4,1),(6,3,2,0),(1,1,2,3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
quickly find
nonempty subsequence
with sum 0 mod 2.

This is linear algebra over **F**
Guaranteed to find subseque
if number of vectors
exceeds length of each vecto

e.g. for $n = 671$:
$1(n+1) = 2^5 3^1 5^0 7^1$;
$4(n+4) = 2^2 3^3 5^2 7^0$;
$15(n+15) = 2^1 3^1 5^1 7^3$;
$49(n+49) = 2^4 3^2 5^1 7^2$;
$64(n+64) = 2^6 3^1 5^1 7^2$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1,0,4,1), (6,3,2,0), (1,1,2,3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
quickly find
nonempty subsequence
with sum 0 mod 2.

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence
if number of vectors
exceeds length of each vector.

e.g. for $n = 671$:

$1(n + 1) = 2^5 3^1 5^0 7^1$;

$4(n + 4) = 2^2 3^3 5^2 7^0$;

$15(n + 15) = 2^1 3^1 5^1 7^3$;

$49(n + 49) = 2^4 3^2 5^1 7^2$;

$64(n + 64) = 2^6 3^1 5^1 7^2$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1,0,4,1), (6,3,2,0), (1,1,2,3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
quickly find
nonempty subsequence
with sum 0 mod 2.

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence
if number of vectors
exceeds length of each vector.

e.g. for $n = 671$:

$1(n+1) = 2^5 3^1 5^0 7^1$;

$4(n+4) = 2^2 3^3 5^2 7^0$;

$15(n+15) = 2^1 3^1 5^1 7^3$;

$49(n+49) = 2^4 3^2 5^1 7^2$;

$64(n+64) = 2^6 3^1 5^1 7^2$.

$\mathbf{F}_2$-kernel of exponent matrix is
gen by (0 1 0 1 1) and (1 0 1 1 0);
e.g., $1(n+1)15(n+15)49(n+49)$
is a square.

l the first three
ely factored congruences
uare product?
ust blind luck?

e exponent vectors
1), (6, 3, 2, 0), (1, 1, 2, 3)
d to have sum 0 mod 2.

didn't need this luck!
ng sequence of vectors,
find
ty subsequence
n 0 mod 2.

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence
if number of vectors
exceeds length of each vector.

e.g. for $n = 671$:
$1(n + 1) = 2^5 3^1 5^0 7^1$;
$4(n + 4) = 2^2 3^3 5^2 7^0$;
$15(n + 15) = 2^1 3^1 5^1 7^3$;
$49(n + 49) = 2^4 3^2 5^1 7^2$;
$64(n + 64) = 2^6 3^1 5^1 7^2$.

$\mathbf{F}_2$-kernel of exponent matrix is
gen by (0 1 0 1 1) and (1 0 1 1 0);
e.g., $1(n+1)15(n+15)49(n+49)$
is a square.

Plausible
separate
of any n

Given n

1. Try t
into proc
for $i \in \{$

2. Look
with $i(n$
and with

3. Comp
$s = \prod_i i$

three
d congruences
ct?
uck?

t vectors
0), (1, 1, 2, 3)
sum 0 mod 2.

d this luck!
ce of vectors,

uence
2.

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence
if number of vectors
exceeds length of each vector.

e.g. for $n = 671$:
$1(n + 1) = 2^5 3^1 5^0 7^1$;
$4(n + 4) = 2^2 3^3 5^2 7^0$;
$15(n + 15) = 2^1 3^1 5^1 7^3$;
$49(n + 49) = 2^4 3^2 5^1 7^2$;
$64(n + 64) = 2^6 3^1 5^1 7^2$.

$\mathbf{F}_2$-kernel of exponent matrix is
gen by (0 1 0 1 1) and (1 0 1 1 0);
e.g., $1(n+1)15(n+15)49(n+49)$
is a square.

Plausible conjectu
separate the odd p
of any n, not just

Given n and paran

1. Try to fully fac
into products of p
for $i \in \{1, 2, 3, \ldots$

2. Look for nonem
with $i(n + i)$ com
and with $\prod_i i(n +$

3. Compute gcd{
$s = \prod_i i$ and $t =$

nces

2, 3)

od 2.

k!

ors,

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence
if number of vectors
exceeds length of each vector.

e.g. for $n = 671$:
$1(n + 1) = 2^5 3^1 5^0 7^1$;
$4(n + 4) = 2^2 3^3 5^2 7^0$;
$15(n + 15) = 2^1 3^1 5^1 7^3$;
$49(n + 49) = 2^4 3^2 5^1 7^2$;
$64(n + 64) = 2^6 3^1 5^1 7^2$.

$\mathbf{F}_2$-kernel of exponent matrix is
gen by (0 1 0 1 1) and (1 0 1 1 0);
e.g., $1(n+1)15(n+15)49(n+49)$
is a square.

Plausible conjecture: **Q** sieve
separate the odd prime divis
of any n, not just 611.

Given n and parameter y:

1. Try to fully factor $i(n +$
into products of primes $\leq y$
for $i \in \{1, 2, 3, \ldots, y^2\}$.

2. Look for nonempty set of
with $i(n + i)$ completely fac
and with $\prod_i i(n + i)$ square.

3. Compute $\gcd\{n, s - t\}$ w
$s = \prod_i i$ and $t = \sqrt{\prod_i i(n +}$

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence
if number of vectors
exceeds length of each vector.

e.g. for $n = 671$:

$1(n + 1) = 2^5 3^1 5^0 7^1$;

$4(n + 4) = 2^2 3^3 5^2 7^0$;

$15(n + 15) = 2^1 3^1 5^1 7^3$;

$49(n + 49) = 2^4 3^2 5^1 7^2$;

$64(n + 64) = 2^6 3^1 5^1 7^2$.

$\mathbf{F}_2$-kernel of exponent matrix is
gen by (0 1 0 1 1) and (1 0 1 1 0);
e.g., $1(n+1)15(n+15)49(n+49)$
is a square.

Plausible conjecture: **Q** sieve can
separate the odd prime divisors
of any n, not just 611.

Given n and parameter y:

1. Try to fully factor $i(n + i)$
into products of primes $\leq y$
for $i \in \{1, 2, 3, \ldots, y^2\}$.

2. Look for nonempty set of i's
with $i(n + i)$ completely factored
and with $\prod_i i(n + i)$ square.

3. Compute $\gcd\{n, s - t\}$ where
$s = \prod_i i$ and $t = \sqrt{\prod_i i(n + i)}$.

inear algebra over $\mathbf{F}_2$.
eed to find subsequence
er of vectors
length of each vector.

$n = 671$:
$1) = 2^5 3^1 5^0 7^1$;
$4) = 2^2 3^3 5^2 7^0$;
$15) = 2^1 3^1 5^1 7^3$;
$49) = 2^4 3^2 5^1 7^2$;
$64) = 2^6 3^1 5^1 7^2$.

el of exponent matrix is
0 1 0 1 1) and (1 0 1 1 0);
$+1)15(n+15)49(n+49)$
are.

Plausible conjecture: **Q** sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

1. Try to fully factor $i(n+i)$ into products of primes $\leq y$ for $i \in \{1, 2, 3, \ldots, y^2\}$.

2. Look for nonempty set of i's with $i(n+i)$ completely factored and with $\prod_i i(n+i)$ square.

3. Compute $\gcd\{n, s-t\}$ where $s = \prod_i i$ and $t = \sqrt{\prod_i i(n+i)}$.

How larg
for this t

bra over $\mathbf{F}_2$.
d subsequence
ors
each vector.

$^1 5^0 7^1$;
$^3 5^2 7^0$;
$^1 5^1 7^3$;
$^2 5^1 7^2$;
$^1 5^1 7^2$.

nent matrix is

and (1 0 1 1 0);

$+15)49(n+49)$

Plausible conjecture: **Q** sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

1. Try to fully factor $i(n+i)$ into products of primes $\leq y$ for $i \in \{1, 2, 3, \ldots, y^2\}$.

2. Look for nonempty set of i's with $i(n+i)$ completely factored and with $\prod_i i(n+i)$ square.

3. Compute $\gcd\{n, s-t\}$ where $s = \prod_i i$ and $t = \sqrt{\prod_i i(n+i)}$.

How large does y
for this to find a s

2.

ence

or.

x is

1 1 0);

$n+49$)

Plausible conjecture: **Q** sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

1. Try to fully factor $i(n+i)$ into products of primes $\leq y$ for $i \in \{1, 2, 3, \ldots, y^2\}$.

2. Look for nonempty set of i's with $i(n+i)$ completely factored and with $\prod_i i(n+i)$ square.

3. Compute $\gcd\{n, s-t\}$ where $s = \prod_i i$ and $t = \sqrt{\prod_i i(n+i)}$.

How large does y have to be for this to find a square?

Plausible conjecture: **Q** sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

1. Try to fully factor $i(n+i)$ into products of primes $\leq y$ for $i \in \{1, 2, 3, \ldots, y^2\}$.

2. Look for nonempty set of i's with $i(n+i)$ completely factored and with $\prod_i i(n+i)$ square.

3. Compute $\gcd\{n, s-t\}$ where $s = \prod_i i$ and $t = \sqrt{\prod_i i(n+i)}$.

How large does y have to be for this to find a square?

Plausible conjecture: **Q** sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

1. Try to fully factor $i(n+i)$ into products of primes $\leq y$ for $i \in \{1, 2, 3, \ldots, y^2\}$.

2. Look for nonempty set of i's with $i(n+i)$ completely factored and with $\prod_i i(n+i)$ square.

3. Compute $\gcd\{n, s-t\}$ where $s = \prod_i i$ and $t = \sqrt{\prod_i i(n+i)}$.

How large does y have to be for this to find a square?

Let's aim for number of completely factored congruences to exceed length of each vector, guaranteeing a square.
(This is somewhat pessimistic; smaller numbers usually work.)

Vector length $\approx y/\log y$.
Will there be $> y/\log y$ completely factored congruences out of y^2 congruences?

e conjecture: **Q** sieve can
the odd prime divisors
, not just 611.

and parameter y:

o fully factor $i(n+i)$
ducts of primes $\leq y$
$\{1, 2, 3, \ldots, y^2\}$.

for nonempty set of i's
$+ i)$ completely factored
n $\prod_i i(n+i)$ square.

pute $\gcd\{n, s-t\}$ where
and $t = \sqrt{\prod_i i(n+i)}$.

How large does y have to be
for this to find a square?

Let's aim for number of
completely factored congruences
to exceed length of each vector,
guaranteeing a square.
(This is somewhat pessimistic;
smaller numbers usually work.)

Vector length $\approx y/\log y$.
Will there be $> y/\log y$
completely factored congruences
out of y^2 congruences?

What's
being y-
factored

re: **Q** sieve can
prime divisors
611.

meter y:

tor $i(n+i)$
rimes $\leq y$
$, y^2\}$.

npty set of i's
pletely factored
$i)$ square.

$n, s-t\}$ where
$\sqrt{\prod_i i(n+i)}$.

How large does y have to be for this to find a square?

Let's aim for number of completely factored congruences to exceed length of each vector, guaranteeing a square.
(This is somewhat pessimistic; smaller numbers usually work.)

Vector length $\approx y/\log y$.
Will there be $> y/\log y$ completely factored congruences out of y^2 congruences?

What's chance of being y-**smooth**, factored into prim

e can
sors

i)

f i's
ctored

where
$\overline{}$
$- i$).

How large does y have to be
for this to find a square?

Let's aim for number of
completely factored congruences
to exceed length of each vector,
guaranteeing a square.
(This is somewhat pessimistic;
smaller numbers usually work.)

Vector length $\approx y/\log y$.
Will there be $> y/\log y$
completely factored congruences
out of y^2 congruences?

What's chance of random i(
being y-**smooth**, i.e., compl
factored into primes $\leq y$?

How large does y have to be for this to find a square?

Let's aim for number of completely factored congruences to exceed length of each vector, guaranteeing a square.
(This is somewhat pessimistic; smaller numbers usually work.)

Vector length $\approx y/\log y$.
Will there be $> y/\log y$ completely factored congruences out of y^2 congruences?

What's chance of random $i(n+i)$ being y-**smooth**, i.e., completely factored into primes $\leq y$?

How large does y have to be for this to find a square?

Let's aim for number of completely factored congruences to exceed length of each vector, guaranteeing a square.
(This is somewhat pessimistic; smaller numbers usually work.)

Vector length $\approx y/\log y$.
Will there be $> y/\log y$ completely factored congruences out of y^2 congruences?

What's chance of random $i(n+i)$ being y-**smooth**, i.e., completely factored into primes $\leq y$?

Consider, e.g., $y = \lfloor n^{1/10} \rfloor$.
Uniform random integer in $[1, y^2]$ has y-smoothness chance $\approx$0.306; uniform random integer in $[1, n]$ has chance $\approx 2.77 \cdot 10^{-11}$.
Plausible conjecture:
y-smoothness chance of $i(n+i)$ is $\approx 8.5 \cdot 10^{-12}$.
Find $\approx 8.5 \cdot 10^{-12} y^2$ fully factored congruences.

ge does y have to be
to find a square?

n for number of
ely factored congruences
d length of each vector,
eeing a square.
somewhat pessimistic;
numbers usually work.)

ength $\approx y/\log y$.
re be $> y/\log y$
ely factored congruences
^{2} congruences?

What's chance of random $i(n+i)$ being y-**smooth**, i.e., completely factored into primes $\leq y$?

Consider, e.g., $y = \lfloor n^{1/10} \rfloor$.
Uniform random integer in $[1, y^2]$ has y-smoothness chance $\approx$0.306;
uniform random integer in $[1, n]$ has chance $\approx 2.77 \cdot 10^{-11}$.
Plausible conjecture:
y-smoothness chance of $i(n+i)$ is $\approx 8.5 \cdot 10^{-12}$.
Find $\approx 8.5 \cdot 10^{-12} y^2$ fully factored congruences.

If $n \geq 2$
$8.5 \cdot 10^{-}$
approxin
so conje
will find

Find ma
with neg
If gcd tu
try the n

Conjectu
splits od
prime-po

have to be
quare?

ber of
ed congruences
of each vector,
uare.
t pessimistic;
sually work.)

$/\log y$.
$/\log y$
ed congruences
nces?

What's chance of random $i(n+i)$ being y-**smooth**, i.e., completely factored into primes $\leq y$?

Consider, e.g., $y = \lfloor n^{1/10} \rfloor$.
Uniform random integer in $[1, y^2]$ has y-smoothness chance $\approx$0.306; uniform random integer in $[1, n]$ has chance $\approx 2.77 \cdot 10^{-11}$.
Plausible conjecture:
y-smoothness chance of $i(n+i)$ is $\approx 8.5 \cdot 10^{-12}$.
Find $\approx 8.5 \cdot 10^{-12} y^2$ fully factored congruences.

If $n \geq 2^{340}$ and y
$8.5 \cdot 10^{-12} y^2 > 3y$
approximations see
so conjecturally th
will find a square.

Find many indepe
with negligible ext
If gcd turns out to
try the next squar

Conjecturally alwa
splits odd n into
prime-power facto

e

nces
ctor,

ic;
k.)

nces

What's chance of random $i(n+i)$ being y-**smooth**, i.e., completely factored into primes $\leq y$?

Consider, e.g., $y = \lfloor n^{1/10} \rfloor$.
Uniform random integer in $[1, y^2]$ has y-smoothness chance $\approx$0.306;
uniform random integer in $[1, n]$ has chance $\approx 2.77 \cdot 10^{-11}$.
Plausible conjecture:
y-smoothness chance of $i(n+i)$ is $\approx 8.5 \cdot 10^{-12}$.
Find $\approx 8.5 \cdot 10^{-12} y^2$ fully factored congruences.

If $n \geq 2^{340}$ and $y = \lfloor n^{1/10} \rfloor$
$8.5 \cdot 10^{-12} y^2 > 3y/\log y$, ar
approximations seem fairly c
so conjecturally the **Q** sieve
will find a square.

Find many independent squa
with negligible extra effort.
If gcd turns out to be 1,
try the next square.

Conjecturally always works:
splits odd n into
prime-power factors.

What's chance of random $i(n+i)$ being y-**smooth**, i.e., completely factored into primes $\leq y$?

Consider, e.g., $y = \lfloor n^{1/10} \rfloor$.
Uniform random integer in $[1, y^2]$ has y-smoothness chance $\approx$0.306; uniform random integer in $[1, n]$ has chance $\approx 2.77 \cdot 10^{-11}$.
Plausible conjecture:
y-smoothness chance of $i(n+i)$ is $\approx 8.5 \cdot 10^{-12}$.
Find $\approx 8.5 \cdot 10^{-12} y^2$ fully factored congruences.

If $n \geq 2^{340}$ and $y = \lfloor n^{1/10} \rfloor$ then $8.5 \cdot 10^{-12} y^2 > 3y/\log y$, and approximations seem fairly close, so conjecturally the **Q** sieve will find a square.

Find many independent squares with negligible extra effort.
If gcd turns out to be 1, try the next square.

Conjecturally always works: splits odd n into prime-power factors.

chance of random $i(n+i)$
-smooth, i.e., completely
into primes $\leq y$?

r, e.g., $y = \lfloor n^{1/10} \rfloor$.
random integer in $[1, y^2]$
noothness chance $\approx$0.306;
random integer in $[1, n]$
nce $\approx 2.77 \cdot 10^{-11}$.
e conjecture:
hness chance of $i(n+i)$
$\cdot 10^{-12}$.
$8.5 \cdot 10^{-12} y^2$
tored congruences.

If $n \geq 2^{340}$ and $y = \lfloor n^{1/10} \rfloor$ then $8.5 \cdot 10^{-12} y^2 > 3y/\log y$, and approximations seem fairly close, so conjecturally the **Q** sieve will find a square.

Find many independent squares with negligible extra effort.
If gcd turns out to be 1, try the next square.

Conjecturally always works: splits odd n into prime-power factors.

How abo
for large

Uniform
has $n^{1/u}$
roughly

Plausible
Q sieve
with $y =$
for all n
here $o(1$

random $i(n+i)$
i.e., completely
es $\le y$?

$= \lfloor n^{1/10} \rfloor$.
nteger in $[1, y^2]$
chance $\approx$0.306;
nteger in $[1, n]$
$\cdot 10^{-11}$.

re:
nce of $i(n+i)$

y^2
gruences.

If $n \ge 2^{340}$ and $y = \lfloor n^{1/10} \rfloor$ then
$8.5 \cdot 10^{-12} y^2 > 3y/\log y$, and
approximations seem fairly close,
so conjecturally the **Q** sieve
will find a square.

Find many independent squares
with negligible extra effort.
If gcd turns out to be 1,
try the next square.

Conjecturally always works:
splits odd n into
prime-power factors.

How about $y \approx n$
for larger u?

Uniform random i
has $n^{1/u}$-smoothn
roughly u^{-u}.

Plausible conjectu
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \ge u^{(1+o(1}$
here $o(1)$ is as u -

$(n+i)$

letely

$1, y^2]$

0.306;

$1, n]$

$+ i)$

If $n \geq 2^{340}$ and $y = \lfloor n^{1/10} \rfloor$ then $8.5 \cdot 10^{-12} y^2 > 3y/\log y$, and approximations seem fairly close, so conjecturally the **Q** sieve will find a square.

Find many independent squares with negligible extra effort.
If gcd turns out to be 1, try the next square.

Conjecturally always works: splits odd n into prime-power factors.

How about $y \approx n^{1/u}$ for larger u?

Uniform random integer in [
has $n^{1/u}$-smoothness chance
roughly u^{-u}.

Plausible conjecture:
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \geq u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

If $n \geq 2^{340}$ and $y = \lfloor n^{1/10} \rfloor$ then $8.5 \cdot 10^{-12} y^2 > 3y/\log y$, and approximations seem fairly close, so conjecturally the **Q** sieve will find a square.

Find many independent squares with negligible extra effort.
If gcd turns out to be 1, try the next square.

Conjecturally always works: splits odd n into prime-power factors.

How about $y \approx n^{1/u}$ for larger u?

Uniform random integer in $[1, n]$ has $n^{1/u}$-smoothness chance roughly u^{-u}.

Plausible conjecture:
Q sieve succeeds with $y = \lfloor n^{1/u} \rfloor$ for all $n \geq u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

^{340} and $y = \lfloor n^{1/10} \rfloor$ then
$^{-12}y^2 > 3y/\log y$, and
nations seem fairly close,
cturally the **Q** sieve
a square.

ny independent squares
gligible extra effort.
urns out to be 1,
next square.

urally always works:
d n into
ower factors.

How about $y \approx n^{1/u}$
for larger u?

Uniform random integer in $[1, n]$
has $n^{1/u}$-smoothness chance
roughly u^{-u}.

Plausible conjecture:
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \geq u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

How abo
letting u

Given n,
in geom
until **Q**
e.g., inc

Plausible
$\exp\sqrt{(\frac{1}{2}$
$u \in \sqrt{(2}$

Cost of
hence su

$= \lfloor n^{1/10} \rfloor$ then
$y/\log y$, and
em fairly close,
e **Q** sieve

ndent squares
ra effort.
be 1,
e.

ys works:

rs.

How about $y \approx n^{1/u}$
for larger u?

Uniform random integer in $[1, n]$
has $n^{1/u}$-smoothness chance
roughly u^{-u}.

Plausible conjecture:
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \geq u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

How about
letting u grow wit

Given n, try seque
in geometric progr
until **Q** sieve work
e.g., increasing po

Plausible conjectu
$\exp \sqrt{\left(\frac{1}{2} + o(1)\right) \log n \log \log n}$
$u \in \sqrt{(2 + o(1)) \log n / \log \log n}$

Cost of **Q** sieve is
hence subexponen

then
nd
close,

ares

How about $y \approx n^{1/u}$
for larger u?

Uniform random integer in $[1, n]$
has $n^{1/u}$-smoothness chance
roughly u^{-u}.

Plausible conjecture:
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \geq u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

How about
letting u grow with n?

Given n, try sequence of y's
in geometric progression
until **Q** sieve works;
e.g., increasing powers of 2.

Plausible conjecture: final y
$\exp \sqrt{\left(\frac{1}{2} + o(1)\right) \log n \log \log$
$u \in \sqrt{(2 + o(1)) \log n / \log \log$

Cost of **Q** sieve is a power o
hence subexponential in n.

How about $y \approx n^{1/u}$
for larger u?

Uniform random integer in $[1, n]$
has $n^{1/u}$-smoothness chance
roughly u^{-u}.

Plausible conjecture:
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \geq u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

How about
letting u grow with n?

Given n, try sequence of y's
in geometric progression
until **Q** sieve works;
e.g., increasing powers of 2.

Plausible conjecture: final $y \in$
$\exp \sqrt{\left(\frac{1}{2} + o(1)\right) \log n \log \log n}$,
$u \in \sqrt{(2 + o(1)) \log n / \log \log n}$.

Cost of **Q** sieve is a power of y,
hence subexponential in n.

out $y \approx n^{1/u}$
r u?

random integer in $[1, n]$
^{u}-smoothness chance
u^{-u}.

e conjecture:
succeeds
$= \lfloor n^{1/u} \rfloor$
$\geq u^{(1+o(1))u^2}$;
) is as $u \to \infty$.

How about
letting u grow with n?

Given n, try sequence of y's
in geometric progression
until **Q** sieve works;
e.g., increasing powers of 2.

Plausible conjecture: final $y \in$
$\exp \sqrt{\left(\frac{1}{2} + o(1)\right) \log n \log \log n}$,
$u \in \sqrt{(2 + o(1)) \log n / \log \log n}$.

Cost of **Q** sieve is a power of y,
hence subexponential in n.

More ge
exp $\sqrt{(\frac{1}{2}}$
conjectu
is $1/y^{c+}$

Find enc
by chang
replace y
exp $\sqrt{($

Increasin
increases
reduces
So linear
when y

$1/u$

nteger in $[1, n]$
ess chance

re:

$1))u^2$;
$\to \infty$.

How about
letting u grow with n?

Given n, try sequence of y's
in geometric progression
until **Q** sieve works;
e.g., increasing powers of 2.

Plausible conjecture: final $y \in$
$\exp \sqrt{\left(\frac{1}{2} + o(1)\right) \log n \log \log n}$,
$u \in \sqrt{(2 + o(1)) \log n / \log \log n}$.

Cost of **Q** sieve is a power of y,
hence subexponential in n.

More generally, if
$\exp \sqrt{\left(\frac{1}{2c} + o(1)\right)}$
conjectured y-smo
is $1/y^{c+o(1)}$.

Find enough smoo
by changing the ra
replace y^2 with y^c
$\exp \sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right.}$

Increasing c past 1
increases number
reduces linear-alge
So linear algebra
when y is chosen

$1, n]$
e

How about
letting u grow with n?

Given n, try sequence of y's
in geometric progression
until **Q** sieve works;
e.g., increasing powers of 2.

Plausible conjecture: final $y \in$
$\exp \sqrt{\left(\frac{1}{2} + o(1)\right) \log n \log \log n}$,
$u \in \sqrt{(2 + o(1)) \log n / \log \log n}$.

Cost of **Q** sieve is a power of y,
hence subexponential in n.

More generally, if $y \in$
$\exp \sqrt{\left(\frac{1}{2c} + o(1)\right) \log n \log \log$
conjectured y-smoothness ch
is $1/y^{c+o(1)}$.

Find enough smooth congru
by changing the range of i's
replace y^2 with $y^{c+1+o(1)} =$
$\exp \sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right) \log n \log$

Increasing c past 1
increases number of i's but
reduces linear-algebra cost.
So linear algebra never domi
when y is chosen properly.

How about
letting u grow with n?

Given n, try sequence of y's
in geometric progression
until $\mathbf{Q}$ sieve works;
e.g., increasing powers of 2.

Plausible conjecture: final $y \in$
$\exp \sqrt{\left(\frac{1}{2} + o(1)\right) \log n \log \log n}$,
$u \in \sqrt{(2 + o(1)) \log n / \log \log n}$.

Cost of $\mathbf{Q}$ sieve is a power of y,
hence subexponential in n.

More generally, if $y \in$
$\exp \sqrt{\left(\frac{1}{2c} + o(1)\right) \log n \log \log n}$,
conjectured y-smoothness chance
is $1/y^{c+o(1)}$.

Find enough smooth congruences
by changing the range of i's:
replace y^2 with $y^{c+1+o(1)} =$
$\exp \sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right) \log n \log \log n}$.

Increasing c past 1
increases number of i's but
reduces linear-algebra cost.
So linear algebra never dominates
when y is chosen properly.

out

u grow with n?

, try sequence of y's

etric progression

sieve works;

reasing powers of 2.

e conjecture: final $y \in$

$\frac{1}{2} + o(1)\big)\log n \log\log n$,

$2 + o(1))\log n/\log\log n$.

Q sieve is a power of y,

ubexponential in n.

More generally, if $y \in$

$\exp\sqrt{\big(\frac{1}{2c} + o(1)\big)\log n \log\log n}$,

conjectured y-smoothness chance

is $1/y^{c+o(1)}$.

Find enough smooth congruences

by changing the range of i's:

replace y^2 with $y^{c+1+o(1)} =$

$\exp\sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right)\log n \log\log n}$.

Increasing c past 1

increases number of i's but

reduces linear-algebra cost.

So linear algebra never dominates

when y is chosen properly.

Improvin

Smoothn

degrades

Smaller

Crude a

$\approx yn$ if

$\approx y^2 n$ i

More ca

$n + i$ do

i is alwa

only 30%

Can we

to avoid

h n?

ence of y's
ression
s;
wers of 2.

re: final $y \in$
$\log n \log\log n$,
$\log n / \log\log n$.

a power of y,
tial in n.

More generally, if $y \in$
$\exp\sqrt{\left(\frac{1}{2c}+o(1)\right)\log n \log\log n}$,
conjectured y-smoothness chance
is $1/y^{c+o(1)}$.

Find enough smooth congruences
by changing the range of i's:
replace y^2 with $y^{c+1+o(1)} =$
$\exp\sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right)\log n \log\log n}$.

Increasing c past 1
increases number of i's but
reduces linear-algebra cost.
So linear algebra never dominates
when y is chosen properly.

Improving smooth

Smoothness chanc
degrades as i grow
Smaller for $i \approx y^2$

Crude analysis: $i($
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analy
$n + i$ doesn't degr
i is always smooth
only 30% chance f

Can we select con
to avoid this degra

s

$\in$

$\overline{}$

$g\, n,$

$\overline{}$

$\log n.$

of y,

More generally, if $y \in$

$\exp \sqrt{\left(\frac{1}{2c} + o(1)\right) \log n \log \log n}$,

conjectured y-smoothness chance

is $1/y^{c+o(1)}$.

Find enough smooth congruences

by changing the range of i's:

replace y^2 with $y^{c+1+o(1)} =$

$\exp \sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right) \log n \log \log n}$.

Increasing c past 1

increases number of i's but

reduces linear-algebra cost.

So linear algebra never dominates

when y is chosen properly.

Improving smoothness chanc

Smoothness chance of $i(n +$

degrades as i grows.

Smaller for $i \approx y^2$ than for

Crude analysis: $i(n+i)$ gro

$\approx yn$ if $i \approx y$;

$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:

$n + i$ doesn't degrade, but

i is always smooth for $i \leq y$

only 30% chance for $i \approx y^2$.

Can we select congruences

to avoid this degradation?

More generally, if $y \in$
$\exp \sqrt{\left(\frac{1}{2c} + o(1)\right) \log n \log \log n}$,
conjectured y-smoothness chance
is $1/y^{c+o(1)}$.

Find enough smooth congruences
by changing the range of i's:
replace y^2 with $y^{c+1+o(1)} =$
$\exp \sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right) \log n \log \log n}$.

Increasing c past 1
increases number of i's but
reduces linear-algebra cost.
So linear algebra never dominates
when y is chosen properly.

Improving smoothness chances

Smoothness chance of $i(n+i)$
degrades as i grows.
Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \leq y$,
only 30% chance for $i \approx y^2$.

Can we select congruences
to avoid this degradation?

nerally, if $y \in$

$\frac{1}{2c} + o(1)\big)\log n \log\log n$,

red y-smoothness chance

$o(1)}$.

ough smooth congruences

ging the range of i's:

y^2 with $y^{c+1+o(1)} =$

$\frac{(c+1)^2+o(1)}{2c}\Big)\log n \log\log n$.

ng c past 1

s number of i's but

linear-algebra cost.

r algebra never dominates

is chosen properly.

Improving smoothness chances

Smoothness chance of $i(n+i)$
degrades as i grows.
Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \le y$,
only 30% chance for $i \approx y^2$.

Can we select congruences
to avoid this degradation?

Choose

Choose

arithmet

where q

e.g. prog

$2q - (n$

etc.

Check sm

generaliz

for i's in

e.g. che

smooth

Try man

Rare for

$y \in$

$\log n \log\log n$,
oothness chance

oth congruences
ange of i's:
$+1+o(1)) =$

$\left(\frac{}{}\right) \log n \log\log n.$

1

of i's but
ebra cost.
never dominates
properly.

Improving smoothness chances

Smoothness chance of $i(n+i)$
degrades as i grows.
Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \leq y$,
only 30% chance for $i \approx y^2$.

Can we select congruences
to avoid this degradation?

Choose q, square
Choose a "q-subla
arithmetic progres
where q divides ea
e.g. progression q
$2q - (n \bmod q)$, 3
etc.

Check smoothness
generalized congru
for i's in this subla
e.g. check whethe
smooth for $i = q$ -

Try many large q's
Rare for i's to ove

$\log n$,
hance

ences
:

$\log \log n$.

inates

Improving smoothness chances

Smoothness chance of $i(n+i)$
degrades as i grows.
Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \leq y$,
only 30% chance for $i \approx y^2$.

Can we select congruences
to avoid this degradation?

Choose q, square of large pr
Choose a "q-sublattice" of i
arithmetic progression of i's
where q divides each $i(n+$
e.g. progression $q - (n \bmod$
$2q - (n \bmod q)$, $3q - (n$ mo
etc.

Check smoothness of
generalized congruence $i(n$
for i's in this sublattice.
e.g. check whether $i, (n+i)$
smooth for $i = q - (n \bmod$

Try many large q's.
Rare for i's to overlap.

Improving smoothness chances

Smoothness chance of $i(n+i)$
degrades as i grows.
Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \leq y$,
only 30% chance for $i \approx y^2$.

Can we select congruences
to avoid this degradation?

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n+i)$.
e.g. progression $q - (n \bmod q)$,
$2q - (n \bmod q)$, $3q - (n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n+i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are
smooth for $i = q - (n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

ng smoothness chances

ness chance of $i(n+i)$
s as i grows.
for $i \approx y^2$ than for $i \approx y$.

nalysis: $i(n+i)$ grows.
$i \approx y$;
f $i \approx y^2$.

reful analysis:
oesn't degrade, but
ys smooth for $i \leq y$,
% chance for $i \approx y^2$.

select congruences
this degradation?

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n+i)$.
e.g. progression $q - (n \bmod q)$,
$2q - (n \bmod q)$, $3q - (n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n+i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are
smooth for $i = q - (n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

e.g. $n =$

Original

i	n
1	3
2	3
3	3

Use 997
$i \in 8024$

8024
17964
27904

ness chances

ce of $i(n+i)$
vs.
than for $i \approx y$.

$n+i)$ grows.

ysis:
rade, but
n for $i \leq y$,
for $i \approx y^2$.

gruences
adation?

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n+i)$.
e.g. progression $q - (n \bmod q)$,
$2q - (n \bmod q)$, $3q - (n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n+i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are
smooth for $i = q - (n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

e.g. $n = 3141592$

Original **Q** sieve:

i	$n+i$
1	3141592653
2	3141592653
3	3141592653

Use 997^2-sublattic

$i \in 802458 + 994$

i	$(n+$
802458	316
1796467	316
2790476	316

ces

$-i)$

$i \approx y.$

ows.

,

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n+i)$.
e.g. progression $q-(n \bmod q)$,
$2q-(n \bmod q)$, $3q-(n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n+i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are
smooth for $i = q-(n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

e.g. $n = 31415926535897$

Original **Q** sieve:

i	$n+i$
1	3141592653589732
2	3141592653589732
3	3141592653589732

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	3160527373
1796467	3160527373
2790476	3160527373

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n+i)$.
e.g. progression $q-(n \bmod q)$,
$2q-(n \bmod q)$, $3q-(n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n+i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are
smooth for $i = q-(n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

e.g. $n = 31415926535897932 3$:

Original $\mathbf{Q}$ sieve:

i	$n+i$
1	31415926535897932 4
2	31415926535897932 5
3	31415926535897932 6

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

q, square of large prime.
a "q-sublattice" of i's:
tic progression of i's
divides each $i(n+i)$.
gression $q-(n \bmod q)$,
$\bmod q)$, $3q-(n \bmod q)$,

moothness of
zed congruence $i(n+i)/q$
this sublattice.
ck whether $i, (n+i)/q$ are
for $i = q-(n \bmod q)$ etc.

y large q's.
i's to overlap.

e.g. $n = 31415926535897932 3$:

Original $\mathbf{Q}$ sieve:

i	$n+i$
1	31415926535897932 4
2	31415926535897932 5
3	31415926535897932 6

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

Crude ar
eliminat
Have pr
of gener
$(q-(n$ m
between

More ca
are even
For $q \approx$
$i \approx (n+$
so smoo
$(u/2)^{-u}$
2^u times

of large prime.
ttice" of i's:
sion of i's
ch $i(n+i)$.
$-(n \bmod q)$,
$q-(n \bmod q)$,

s of
uence $i(n+i)/q$
attice.
er i, $(n+i)/q$ are
$-(n \bmod q)$ etc.

s.
erlap.

e.g. $n = 31415926535897932 3$:

Original $\mathbf{Q}$ sieve:

i	$n+i$
1	31415926535897932 4
2	31415926535897932 5
3	31415926535897932 6

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

Crude analysis: Su
eliminate the grow
Have practically u
of generalized con
$(q-(n \bmod q))\frac{n+}{}$
between 0 and n.

More careful analy
are even better th
For $q \approx n^{1/2}$ have
$i \approx (n+i)/q \approx n$
so smoothness cha
$(u/2)^{-u/2}(u/2)^{-}$
2^u times larger th

ime.

's:

i).

q),

od q),

$+i)/q$

$)/q$ are

q) etc.

e.g. $n = 31415926535897932^3$:

Original $\mathbf{Q}$ sieve:

i	$n+i$
1	31415926535897932**4**
2	31415926535897932**5**
3	31415926535897932**6**

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

Crude analysis: Sublattices
eliminate the growth problem
Have practically unlimited su
of generalized congruences
$(q-(n \bmod q))\dfrac{n+q-(n \bmod$
q
between 0 and n.

More careful analysis: Subla
are even better than that!
For $q \approx n^{1/2}$ have
$i \approx (n+i)/q \approx n^{1/2} \approx y^{u/}$
so smoothness chance is rou
$(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/$
2^u times larger than before.

e.g. $n = 31415926535897932 3$:

Original $\mathbf{Q}$ sieve:

i	$n+i$
1	31415926535897932 4
2	31415926535897932 5
3	31415926535897932 6

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences $(q-(n \bmod q))\dfrac{n+q-(n \bmod q)}{q}$ between 0 and n.

More careful analysis: Sublattices are even better than that!
For $q \approx n^{1/2}$ have
$i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$
so smoothness chance is roughly
$(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$,
2^u times larger than before.

= 31415926535897932**3**:

Q sieve:

$n+i$

3141592653589793**24**

3141592653589793**25**

3141592653589793**26**

^{2}-sublattice,

$458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
458	316052737309
467	316052737310
476	316052737311

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences $(q-(n \bmod q))\frac{n+q-(n \bmod q)}{q}$ between 0 and n.

More careful analysis: Sublattices are even better than that! For $q \approx n^{1/2}$ have $i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$ so smoothness chance is roughly $(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$, 2^u times larger than before.

Even lar
from cha

"Quadra
$i^2 - n$ w
have i^2
much sm

"MPQS"
using su
But still

"Numbe
achieves

6535897932**3**:

3589793**24**

3589793**25**

3589793**26**

ce,

009**Z**:

$+ i)/997^2$

052737309

052737310

052737311

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences $(q-(n \bmod q))\dfrac{n+q-(n \bmod q)}{q}$ between 0 and n.

More careful analysis: Sublattices are even better than that! For $q \approx n^{1/2}$ have $i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$ so smoothness chance is roughly $(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$, 2^u times larger than before.

Even larger improv
from changing pol

"Quadratic sieve"
$i^2 - n$ with $i \approx \sqrt$
have $i^2 - n \approx n^{1/}$
much smaller than

"MPQS" improves
using sublattices:
But still $\approx n^{1/2}$.

"Number-field siev
achieves $n^{o(1)}$.

323:

4
5
6

9
0
1

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences $(q-(n \bmod q))\dfrac{n+q-(n \bmod q)}{q}$ between 0 and n.

More careful analysis: Sublattices are even better than that! For $q \approx n^{1/2}$ have $i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$ so smoothness chance is roughly $(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$, 2^u times larger than before.

Even larger improvements from changing polynomial $i($

"Quadratic sieve" (QS) uses $i^2 - n$ with $i \approx \sqrt{n}$; have $i^2 - n \approx n^{1/2+o(1)}$, much smaller than n.

"MPQS" improves $o(1)$ using sublattices: $(i^2 - n)/$ But still $\approx n^{1/2}$.

"Number-field sieve" (NFS) achieves $n^{o(1)}$.

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences $(q-(n \bmod q))\dfrac{n+q-(n \bmod q)}{q}$ between 0 and n.

More careful analysis: Sublattices are even better than that! For $q \approx n^{1/2}$ have $i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$ so smoothness chance is roughly $(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$, 2^u times larger than before.

Even larger improvements from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses $i^2 - n$ with $i \approx \sqrt{n}$; have $i^2 - n \approx n^{1/2+o(1)}$, much smaller than n.

"MPQS" improves $o(1)$ using sublattices: $(i^2 - n)/q$. But still $\approx n^{1/2}$.

"Number-field sieve" (NFS) achieves $n^{o(1)}$.

nalysis: Sublattices
e the growth problem.
actically unlimited supply
alized congruences
$\text{nod } q))\frac{n+q-(n \bmod q)}{q}$
0 and n.

reful analysis: Sublattices
better than that!
$n^{1/2}$ have
$-i)/q \approx n^{1/2} \approx y^{u/2}$
thness chance is roughly
$^{/2}(u/2)^{-u/2} = 2^u/u^u$,
s larger than before.

Even larger improvements
from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses
$i^2 - n$ with $i \approx \sqrt{n}$;
have $i^2 - n \approx n^{1/2+o(1)}$,
much smaller than n.

"MPQS" improves $o(1)$
using sublattices: $(i^2 - n)/q$.
But still $\approx n^{1/2}$.

"Number-field sieve" (NFS)
achieves $n^{o(1)}$.

Generali

The **Q** s
the num

Recall h
factors 6

Form a s
as produ
for sever
$14(625)$
$= 44100$

$\gcd\{611$
$= 47$.

ublattices
yth problem.
nlimited supply
gruences
$\frac{-q-(n \bmod q)}{q}$

ysis: Sublattices
an that!
e
$^{1/2} \approx y^{u/2}$
ance is roughly
$^{u/2} = 2^u/u^u$,
an before.

Even larger improvements
from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses
$i^2 - n$ with $i \approx \sqrt{n}$;
have $i^2 - n \approx n^{1/2+o(1)}$,
much smaller than n.

"MPQS" improves $o(1)$
using sublattices: $(i^2 - n)/q$.
But still $\approx n^{1/2}$.

"Number-field sieve" (NFS)
achieves $n^{o(1)}$.

Generalizing beyo

The **Q** sieve is a s
the number-field s

Recall how the **Q**
factors 611:

Form a square
as product of $i(i -$
for several pairs (i
$14(625) \cdot 64(675)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot$
$= 47$.

m.
upply

d q)

ttices

2

ghly
u^u,

Even larger improvements
from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses
$i^2 - n$ with $i \approx \sqrt{n}$;
have $i^2 - n \approx n^{1/2+o(1)}$,
much smaller than n.

"MPQS" improves $o(1)$
using sublattices: $(i^2 - n)/q$.
But still $\approx n^{1/2}$.

"Number-field sieve" (NFS)
achieves $n^{o(1)}$.

Generalizing beyond **Q**

The **Q** sieve is a special case
the number-field sieve.

Recall how the **Q** sieve
factors 611:

Form a square
as product of $i(i + 611j)$
for several pairs (i, j):
$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410$
$= 47$.

Even larger improvements
from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses
$i^2 - n$ with $i \approx \sqrt{n}$;
have $i^2 - n \approx n^{1/2+o(1)}$,
much smaller than n.

"MPQS" improves $o(1)$
using sublattices: $(i^2 - n)/q$.
But still $\approx n^{1/2}$.

"Number-field sieve" (NFS)
achieves $n^{o(1)}$.

Generalizing beyond **Q**

The **Q** sieve is a special case of
the number-field sieve.

Recall how the **Q** sieve
factors 611:

Form a square
as product of $i(i + 611j)$
for several pairs (i, j):
$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410000\}$
$= 47$.

ger improvements
anging polynomial $i(n+i)$.

tic sieve" (QS) uses
with $i \approx \sqrt{n}$;
$- n \approx n^{1/2+o(1)}$,
naller than n.

' improves $o(1)$
blattices: $(i^2 - n)/q$.
$\approx n^{1/2}$.

r-field sieve" (NFS)
$n^{o(1)}$.

Generalizing beyond **Q**

The **Q** sieve is a special case of the number-field sieve.

Recall how the **Q** sieve factors 611:

Form a square as product of $i(i + 611j)$ for several pairs (i, j):
$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410000\}$
$= 47$.

The $\mathbf{Q}(\sqrt$
factors 6

Form a s
as produ
for sever
$(-11 +$
$\cdot (3$
$= (112 -$

Compute
$s = (-1$
$t = 112$
$\gcd\{611$

vements

ynomial $i(n+i)$.

(QS) uses

$\sqrt{n}$;

$^{2+o(1)}$,

n.

s $o(1)$

$(i^2-n)/q$.

ve" (NFS)

Generalizing beyond $\mathbf{Q}$

The $\mathbf{Q}$ sieve is a special case of the number-field sieve.

Recall how the $\mathbf{Q}$ sieve factors 611:

Form a square as product of $i(i+611j)$ for several pairs (i,j):

$14(625)\cdot 64(675)\cdot 75(686)$

$= 4410000^2$.

$\gcd\{611, 14\cdot 64\cdot 75 - 4410000\}$

$= 47$.

The $\mathbf{Q}(\sqrt{14})$ sieve

factors 611 as follo

Form a square

as product of $(i+$

for several pairs $(i$

$(-11+3\cdot 25)(-1$

$\cdot(3+25)(3+$

$= (112-16\sqrt{14})^2$

Compute

$s = (-11+3\cdot 25)$

$t = 112-16\cdot 25,$

$\gcd\{611, s-t\} =$

$(n+i)$.

s

q.

Generalizing beyond $\mathbf{Q}$

The $\mathbf{Q}$ sieve is a special case of the number-field sieve.

Recall how the $\mathbf{Q}$ sieve factors 611:

Form a square as product of $i(i+611j)$ for several pairs (i,j):

$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410000\}$
$= 47$.

The $\mathbf{Q}(\sqrt{14})$ sieve factors 611 as follows:

Form a square as product of $(i+25j)(i+$ for several pairs (i,j):

$(-11+3\cdot 25)(-11+3\sqrt{14}$
$\cdot (3+25)(3+\sqrt{14})$
$= (112-16\sqrt{14})^2$.

Compute

$s = (-11+3\cdot 25)\cdot(3+25$

$t = 112 - 16\cdot 25$,

$\gcd\{611, s-t\} = 13$.

Generalizing beyond $\mathbf{Q}$

The $\mathbf{Q}$ sieve is a special case of the number-field sieve.

Recall how the $\mathbf{Q}$ sieve factors 611:

Form a square as product of $i(i + 611j)$ for several pairs (i, j):

$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410000\}$
$= 47$.

The $\mathbf{Q}(\sqrt{14})$ sieve factors 611 as follows:

Form a square as product of $(i + 25j)(i + \sqrt{14}j)$ for several pairs (i, j):

$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14})$
$\cdot (3 + 25)(3 + \sqrt{14})$
$= (112 - 16\sqrt{14})^2$.

Compute

$s = (-11 + 3 \cdot 25) \cdot (3 + 25)$,

$t = 112 - 16 \cdot 25$,

$\gcd\{611, s - t\} = 13$.

zing beyond **Q**

sieve is a special case of
ber-field sieve.

ow the **Q** sieve
611:

square
uct of $i(i+611j)$
ral pairs (i,j):
$\cdot 64(675)\cdot 75(686)$
000^2.

$, 14\cdot 64\cdot 75 - 4410000\}$

The $\mathbf{Q}(\sqrt{14})$ sieve factors 611 as follows:

Form a square
as product of $(i+25j)(i+\sqrt{14}j)$
for several pairs (i,j):

$$(-11+3\cdot 25)(-11+3\sqrt{14})$$
$$\cdot(3+25)(3+\sqrt{14})$$
$$=(112-16\sqrt{14})^2.$$

Compute
$s=(-11+3\cdot 25)\cdot(3+25)$,
$t=112-16\cdot 25$,
$\gcd\{611, s-t\}=13$.

Why do

Answer:
$\mathbf{Z}[\sqrt{14}]$
since 25

Apply ri
$(-11+$
$\cdot(3$
$=(112-$

i.e. $s^2=$

Unsurpri

nd **Q**

pecial case of
ieve.

sieve

$+ 611j)$
$, j)$:
$\cdot 75(686)$

$75 - 4410000\}$

The $\mathbf{Q}(\sqrt{14})$ sieve
factors 611 as follows:

Form a square
as product of $(i + 25j)(i + \sqrt{14}j)$
for several pairs (i, j):
$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14})$
$\cdot (3 + 25)(3 + \sqrt{14})$
$= (112 - 16\sqrt{14})^2.$

Compute
$s = (-11 + 3 \cdot 25) \cdot (3 + 25),$
$t = 112 - 16 \cdot 25,$
$\gcd\{611, s - t\} = 13.$

Why does this wo

Answer: Have ring
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611,$
since $25^2 = 14$ in

Apply ring morphi
$(-11 + 3 \cdot 25)(-1$
$\cdot (3 + 25)(3 +$
$= (112 - 16 \cdot 25)^2$

i.e. $s^2 = t^2$ in $\mathbf{Z}/6$

Unsurprising to fin

e of

000}

The $\mathbf{Q}(\sqrt{14})$ sieve
factors 611 as follows:

Form a square
as product of $(i + 25j)(i + \sqrt{14}j)$
for several pairs (i, j):
$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14})$
$\cdot (3 + 25)(3 + \sqrt{14})$
$= (112 - 16\sqrt{14})^2$.

Compute
$s = (-11 + 3 \cdot 25) \cdot (3 + 25)$,
$t = 112 - 16 \cdot 25$,
$\gcd\{611, s - t\} = 13$.

Why does this work?

Answer: Have ring morphism
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 2$
since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to squ
$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25)$
$\cdot (3 + 25)(3 + 25)$
$= (112 - 16 \cdot 25)^2$ in $\mathbf{Z}/611$

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

The $\mathbf{Q}(\sqrt{14})$ sieve
factors 611 as follows:

Form a square
as product of $(i + 25j)(i + \sqrt{14}j)$
for several pairs (i, j):
$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14})$
$\cdot (3 + 25)(3 + \sqrt{14})$
$= (112 - 16\sqrt{14})^2$.

Compute
$s = (-11 + 3 \cdot 25) \cdot (3 + 25)$,
$t = 112 - 16 \cdot 25$,
$\gcd\{611, s - t\} = 13$.

Why does this work?

Answer: Have ring morphism
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,
since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:
$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25)$
$\cdot (3 + 25)(3 + 25)$
$= (112 - 16 \cdot 25)^2$ in $\mathbf{Z}/611$.

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

$\sqrt{14}$) sieve
611 as follows:

square
uct of $(i + 25j)(i + \sqrt{14}j)$
ral pairs (i, j):
$3 \cdot 25)(-11 + 3\sqrt{14})$
$3 + 25)(3 + \sqrt{14})$
$- 16\sqrt{14})^2$.

e
$1 + 3 \cdot 25) \cdot (3 + 25)$,
$- 16 \cdot 25$,
$, s - t\} = 13$.

Why does this work?

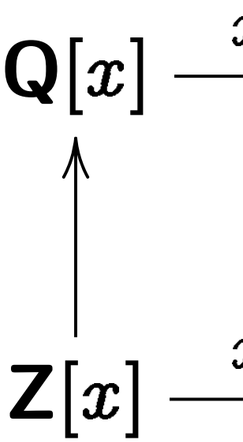
Answer: Have ring morphism
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,
since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:
$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25)$
$\cdot (3 + 25)(3 + 25)$
$= (112 - 16 \cdot 25)^2$ in $\mathbf{Z}/611$.

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

Diagram



$\mathbf{Z}[x]$ use
$\{i_0 x^0 +$
$\mathbf{Z}[\sqrt{14}]$
$\{i_0 + i_1$
$\mathbf{Z}/611$ u
on $\{0, 1,$

e

ows:

$25j)(i+\sqrt{14}j)$

$,j)$:

$1+3\sqrt{14})$

$+\sqrt{14})$

^{2}.

$)\cdot(3+25)$,

13.

Why does this work?

Answer: Have ring morphism
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,
since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:
$(-11+3\cdot 25)(-11+3\cdot 25)$
$\cdot(3+25)(3+25)$
$= (112-16\cdot 25)^2$ in $\mathbf{Z}/611$.

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

Diagram of ring m

$$\begin{array}{ccc} \mathbf{Q}[x] & \xrightarrow{x\mapsto\sqrt{14}} & \mathbf{Q} \\ \uparrow & & \\ \mathbf{Z}[x] & \xrightarrow{x\mapsto\sqrt{14}} & \mathbf{Z} \end{array}$$

$\mathbf{Z}$

$\mathbf{Z}[x]$ uses poly arit
$\{i_0x^0+i_1x^1+\cdots$
$\mathbf{Z}[\sqrt{14}]$ uses $\mathbf{R}$ ari
$\{i_0+i_1\sqrt{14} : i_0,$
$\mathbf{Z}/611$ uses arithm
on $\{0,1,\ldots,610\}$

$\sqrt{14}j)$

)

),

Why does this work?

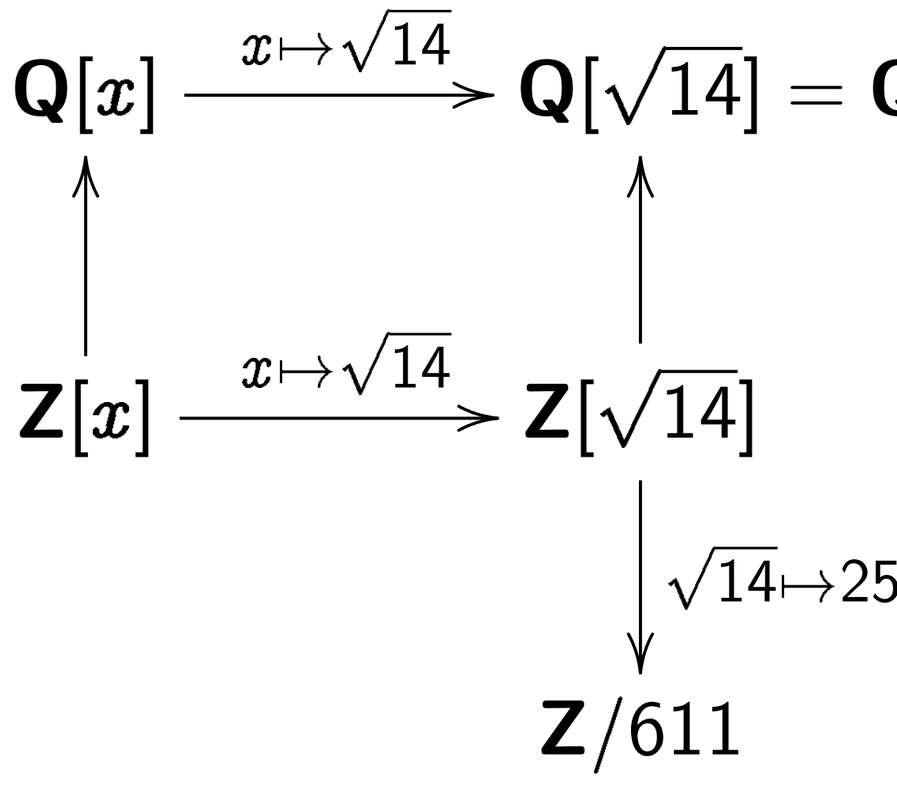
Answer: Have ring morphism
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,
since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:
$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25)$
$\cdot (3 + 25)(3 + 25)$
$= (112 - 16 \cdot 25)^2$ in $\mathbf{Z}/611$.

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

Diagram of ring morphisms:



$\mathbf{Z}[x]$ uses poly arithmetic on
$\{i_0 x^0 + i_1 x^1 + \cdots : \text{all } i_m \in$
$\mathbf{Z}[\sqrt{14}]$ uses $\mathbf{R}$ arithmetic on
$\{i_0 + i_1\sqrt{14} : i_0, i_1 \in \mathbf{Z}\}$;
$\mathbf{Z}/611$ uses arithmetic mod
on $\{0, 1, \ldots, 610\}$.

Why does this work?

Answer: Have ring morphism
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,
since $25^2 = 14$ in $\mathbf{Z}/611$.

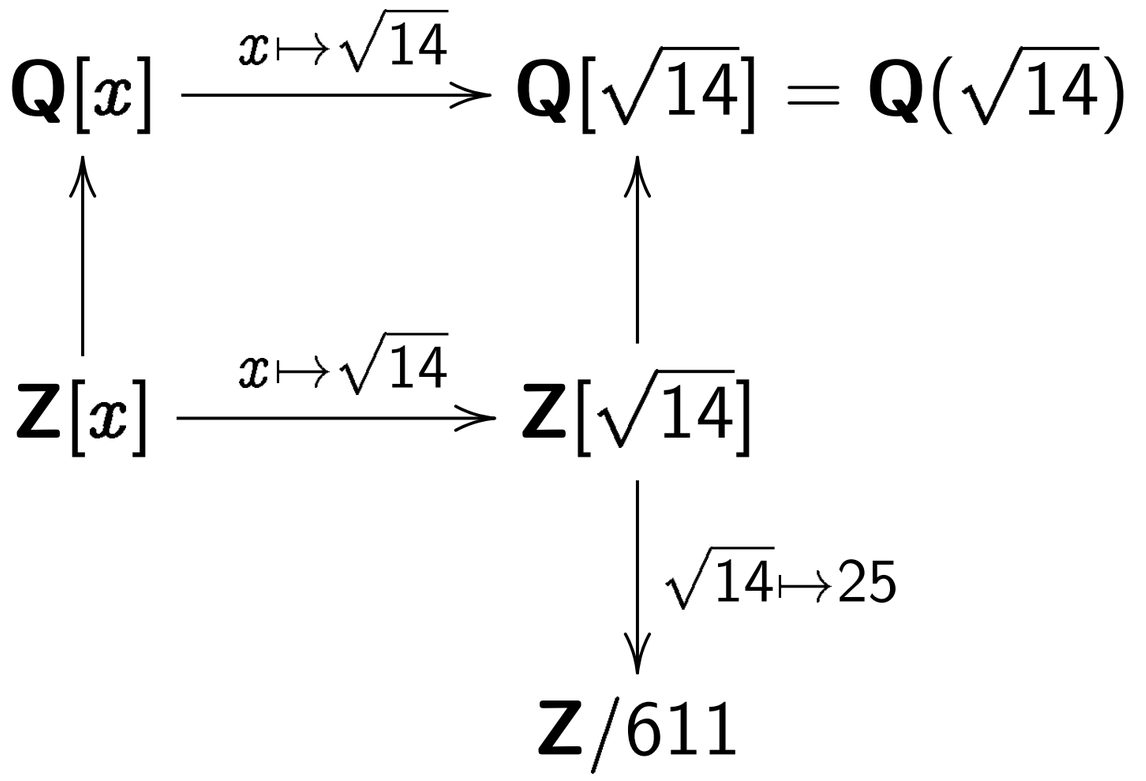
Apply ring morphism to square:

$$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25)$$
$$\cdot (3 + 25)(3 + 25)$$
$$= (112 - 16 \cdot 25)^2 \text{ in } \mathbf{Z}/611.$$

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

Diagram of ring morphisms:



$\mathbf{Z}[x]$ uses poly arithmetic on
$\{i_0 x^0 + i_1 x^1 + \cdots : \text{all } i_m \in \mathbf{Z}\}$;
$\mathbf{Z}[\sqrt{14}]$ uses $\mathbf{R}$ arithmetic on
$\{i_0 + i_1\sqrt{14} : i_0, i_1 \in \mathbf{Z}\}$;
$\mathbf{Z}/611$ uses arithmetic mod 611
on $\{0, 1, \ldots, 610\}$.

es this work?

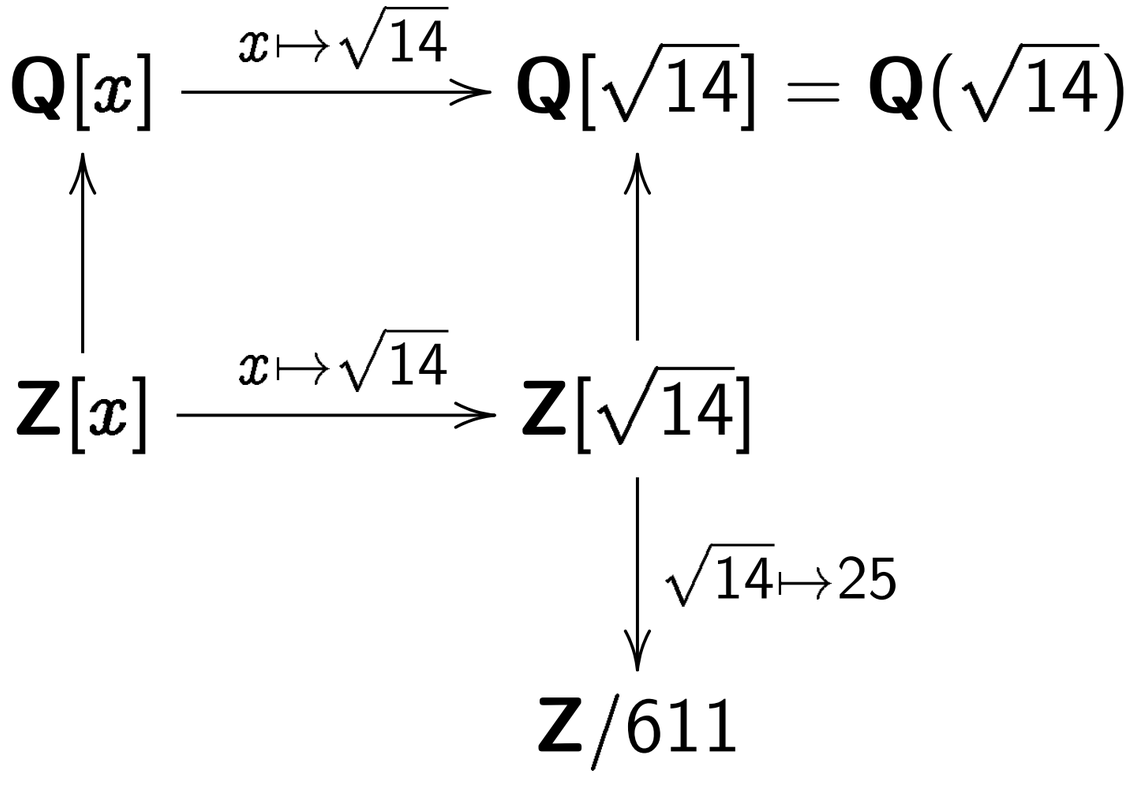
Have ring morphism
$\to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,
$^2 = 14$ in $\mathbf{Z}/611$.

ng morphism to square:
$3 \cdot 25)(-11 + 3 \cdot 25)$
$3 + 25)(3 + 25)$
$- 16 \cdot 25)^2$ in $\mathbf{Z}/611$.

$= t^2$ in $\mathbf{Z}/611$.

ising to find factor.

Diagram of ring morphisms:



$\mathbf{Z}[x]$ uses poly arithmetic on
$\{i_0 x^0 + i_1 x^1 + \cdots : \text{all } i_m \in \mathbf{Z}\}$;
$\mathbf{Z}[\sqrt{14}]$ uses $\mathbf{R}$ arithmetic on
$\{i_0 + i_1\sqrt{14} : i_0, i_1 \in \mathbf{Z}\}$;
$\mathbf{Z}/611$ uses arithmetic mod 611
on $\{0, 1, \ldots, 610\}$.

Generali
to $(f, m$
$m \in \mathbf{Z}$,

Write d
$f = f_d x$

Can take
but large
better p

Pick $\alpha \in$
Then f_d
monic g

rk?

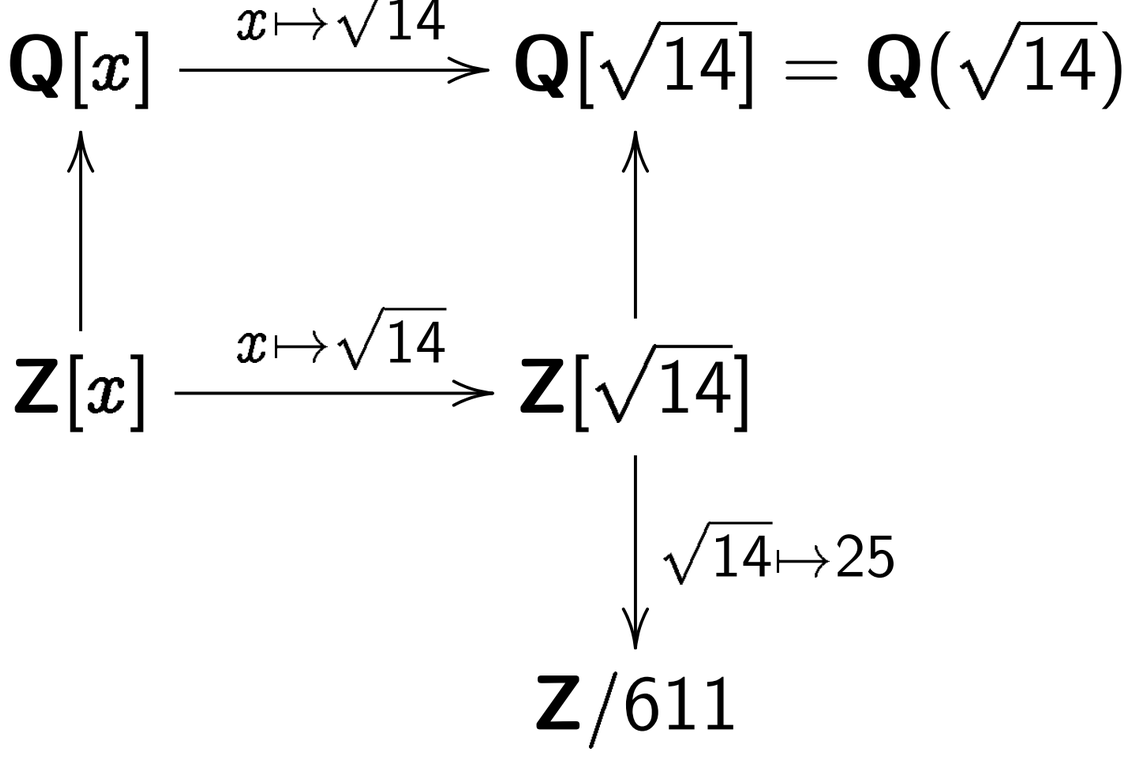
g morphism
$\sqrt{14} \mapsto 25$,
$\mathbf{Z}/611$.

sm to square:
$1 + 3 \cdot 25)$
$+ 25)$
^{2} in $\mathbf{Z}/611$.

611.

nd factor.

Diagram of ring morphisms:



$\mathbf{Z}[x]$ uses poly arithmetic on
$\{i_0 x^0 + i_1 x^1 + \cdots : \text{all } i_m \in \mathbf{Z}\}$;
$\mathbf{Z}[\sqrt{14}]$ uses $\mathbf{R}$ arithmetic on
$\{i_0 + i_1 \sqrt{14} : i_0, i_1 \in \mathbf{Z}\}$;
$\mathbf{Z}/611$ uses arithmetic mod 611
on $\{0, 1, \ldots, 610\}$.

Generalize from $(x$
to (f, m) with irre
$m \in \mathbf{Z}$, $f(m) \in n$

Write $d = \deg f$,
$f = f_d x^d + \cdots +$

Can take $f_d = 1$ f
but larger f_d allow
better parameter s

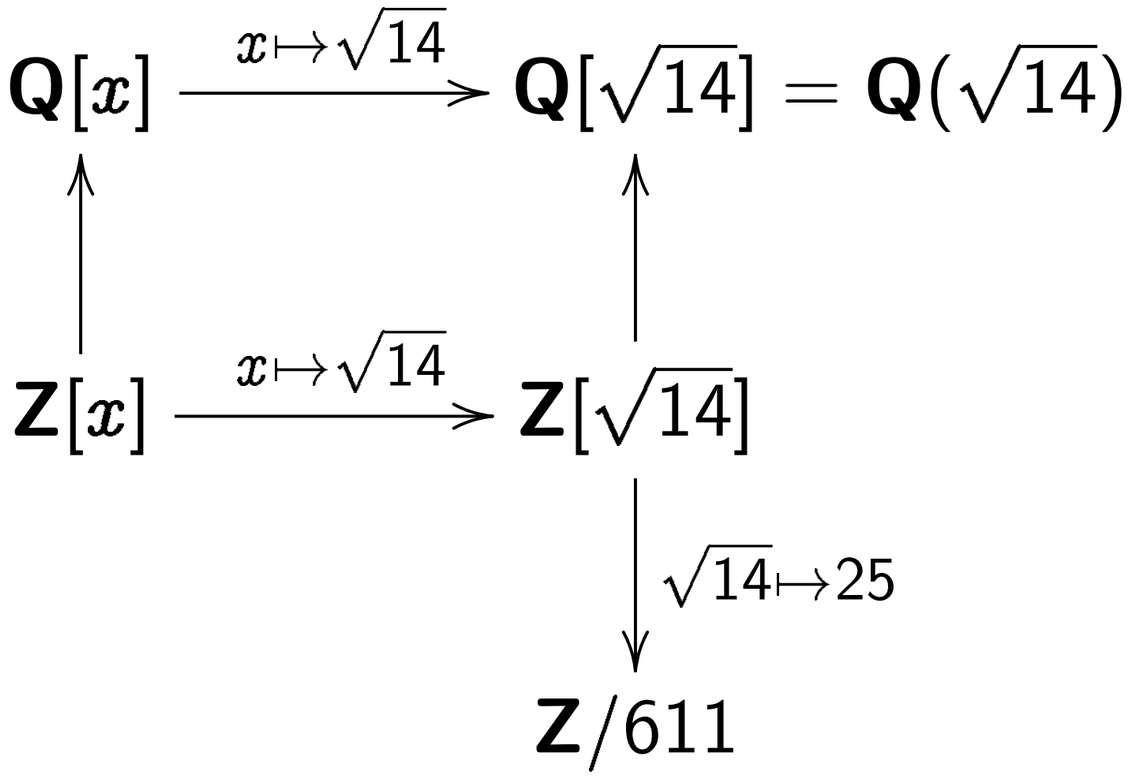
Pick $\alpha \in \mathbf{C}$, root
Then $f_d \alpha$ is a roo
monic $g = f_d^{d-1} f($

m
25,

are:
)

..

Diagram of ring morphisms:



$\mathbf{Z}[x]$ uses poly arithmetic on
$\{i_0 x^0 + i_1 x^1 + \cdots : \text{all } i_m \in \mathbf{Z}\}$;
$\mathbf{Z}[\sqrt{14}]$ uses $\mathbf{R}$ arithmetic on
$\{i_0 + i_1 \sqrt{14} : i_0, i_1 \in \mathbf{Z}\}$;
$\mathbf{Z}/611$ uses arithmetic mod 611
on $\{0, 1, \ldots, 610\}$.

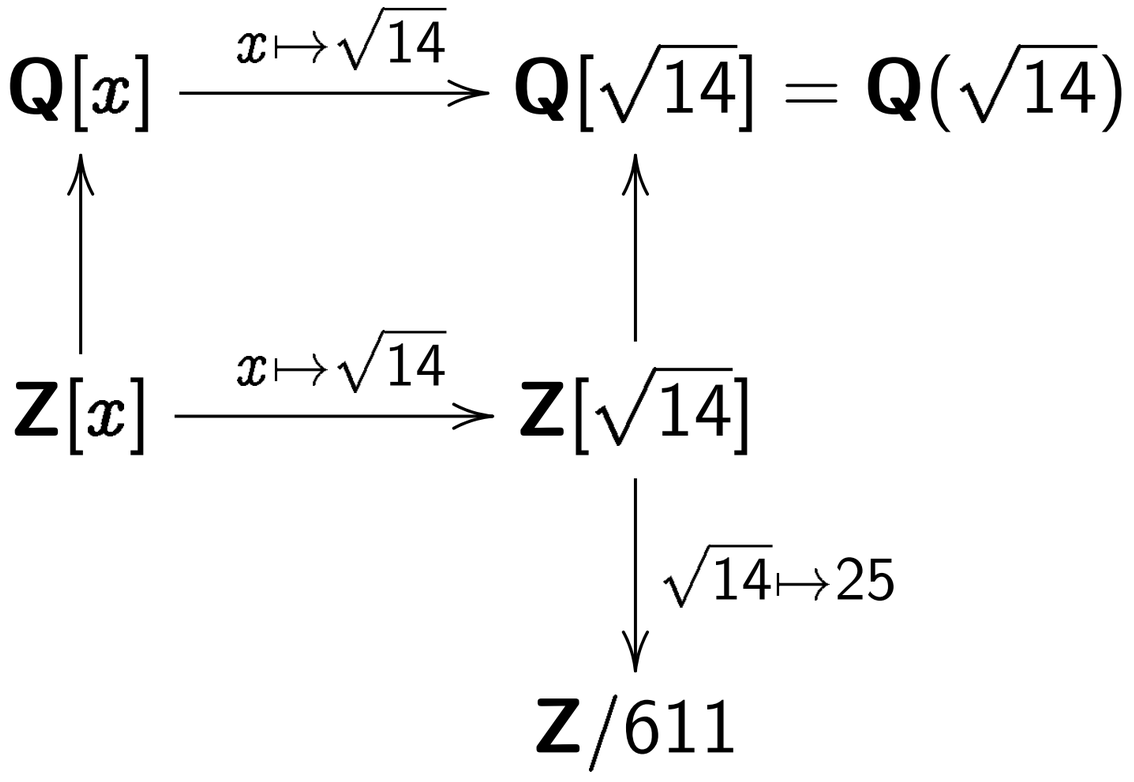
Generalize from $(x^2 - 14, 25$
to (f, m) with irred $f \in \mathbf{Z}[x$
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0$

Can take $f_d = 1$ for simplici
but larger f_d allows
better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d \alpha$ is a root of
monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}$

Diagram of ring morphisms:



$\mathbf{Z}[x]$ uses poly arithmetic on
$\{i_0x^0 + i_1x^1 + \cdots : \text{all } i_m \in \mathbf{Z}\}$;
$\mathbf{Z}[\sqrt{14}]$ uses $\mathbf{R}$ arithmetic on
$\{i_0 + i_1\sqrt{14} : i_0, i_1 \in \mathbf{Z}\}$;
$\mathbf{Z}/611$ uses arithmetic mod 611
on $\{0, 1, \ldots, 610\}$.

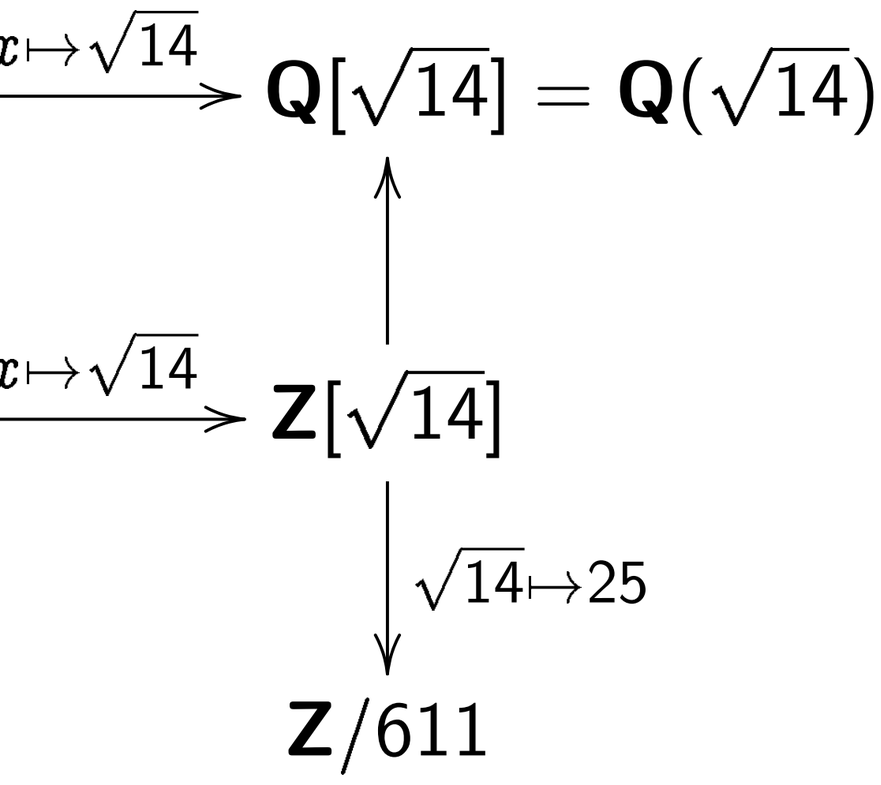
Generalize from $(x^2 - 14, 25)$
to (f, m) with irred $f \in \mathbf{Z}[x]$,
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_dx^d + \cdots + f_1x^1 + f_0x^0$.

Can take $f_d = 1$ for simplicity,
but larger f_d allows
better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d\alpha$ is a root of
monic $g = f_d^{d-1}f(x/f_d) \in \mathbf{Z}[x]$.

n of ring morphisms:



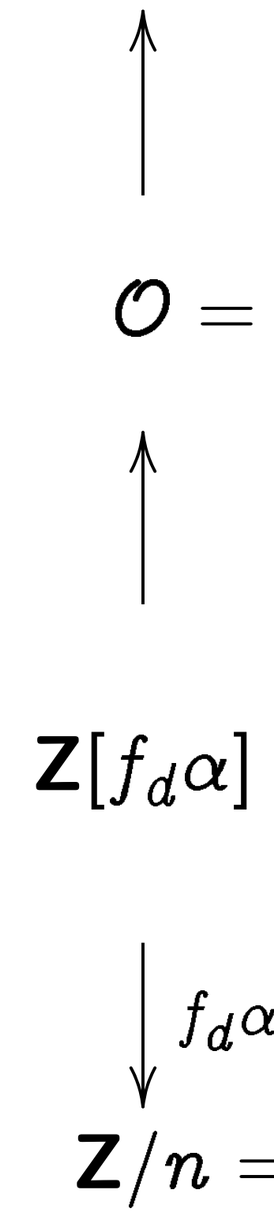
es poly arithmetic on
$i_1 x^1 + \cdots$: all $i_m \in \mathbf{Z}\}$;
uses $\mathbf{R}$ arithmetic on
$\sqrt{14} : i_0, i_1 \in \mathbf{Z}\}$;
ses arithmetic mod 611
$, \ldots, 610\}$.

Generalize from $(x^2 - 14, 25)$
to (f, m) with irred $f \in \mathbf{Z}[x]$,
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity,
but larger f_d allows
better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d \alpha$ is a root of
monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.



norphisms:

$[\sqrt{14}] = \mathbf{Q}(\sqrt{14})$

$\uparrow$

$[\sqrt{14}]$

$\downarrow \sqrt{14} \mapsto 25$

$\mathbf{Z}/611$

thmetic on

$\cdot$: all $i_m \in \mathbf{Z}\}$;

thmetic on

$i_1 \in \mathbf{Z}\}$;

netic mod 611

.

Generalize from $(x^2 - 14, 25)$
to (f, m) with irred $f \in \mathbf{Z}[x]$,
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity,
but larger f_d allows
better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d\alpha$ is a root of
monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$\mathbf{Q}(\alpha) = \{ r_0 + r$
$\cdots +$
$r_0, \ldots$

$\uparrow$

$\mathcal{O} = \{$ algebrai
in $\mathbf{Q}$

$\uparrow$

$\mathbf{Z}[f_d\alpha] = \{ i_0 +$
$\cdots +$
$i_0, \ldots$

$\downarrow f_d\alpha \mapsto f_d m$

$\mathbf{Z}/n = \{0, 1, \ldots$

$\mathbf{Q}(\sqrt{14})$

$\}$;

611

Generalize from $(x^2 - 14, 25)$
to (f, m) with irred $f \in \mathbf{Z}[x]$,
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity,
but larger f_d allows
better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d \alpha$ is a root of
monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) = \begin{cases} r_0 + r_1\alpha + r_2\alpha \\ \cdots + r_{d-1}\alpha^{d-1} \\ r_0, \ldots, r_{d-1} \in \mathbf{Q} \end{cases}$$

$\uparrow$

$$\mathcal{O} = \begin{cases} \text{algebraic integers} \\ \text{in } \mathbf{Q}(\alpha) \end{cases}$$

$\uparrow$

$$\mathbf{Z}[f_d\alpha] = \begin{cases} i_0 + i_1 f_d \alpha + \\ \cdots + i_{d-1} f_d^{d-1} \\ i_0, \ldots, i_{d-1} \in \mathbf{Z} \end{cases}$$

$\downarrow f_d\alpha \mapsto f_d m$

$$\mathbf{Z}/n = \{0, 1, \ldots, n-1\}$$

Generalize from $(x^2 - 14, 25)$
to (f, m) with irred $f \in \mathbf{Z}[x]$,
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity,
but larger f_d allows
better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d\alpha$ is a root of
monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) = \left\{ \begin{array}{l} r_0 + r_1\alpha + r_2\alpha^2 + \\ \cdots + r_{d-1}\alpha^{d-1}: \\ r_0, \ldots, r_{d-1} \in \mathbf{Q} \end{array} \right\}$$

$$\uparrow$$

$$\mathcal{O} = \left\{ \begin{array}{c} \text{algebraic integers} \\ \text{in } \mathbf{Q}(\alpha) \end{array} \right\}$$

$$\uparrow$$

$$\mathbf{Z}[f_d\alpha] = \left\{ \begin{array}{l} i_0 + i_1 f_d\alpha + \\ \cdots + i_{d-1} f_d^{d-1} \alpha^{d-1}: \\ i_0, \ldots, i_{d-1} \in \mathbf{Z} \end{array} \right\}$$

$$\downarrow f_d\alpha \mapsto f_d m$$

$$\mathbf{Z}/n = \{0, 1, \ldots, n-1\}$$

ze from $(x^2 - 14, 25)$
) with irred $f \in \mathbf{Z}[x]$,
$f(m) \in n\mathbf{Z}$.

$= \deg f$,
$^d + \cdots + f_1 x^1 + f_0 x^0$.

e $f_d = 1$ for simplicity,
er f_d allows
arameter selection.

$\in \mathbf{C}$, root of f.
α is a root of
$= f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) = \left\{ \begin{array}{l} r_0 + r_1\alpha + r_2\alpha^2 + \\ \cdots + r_{d-1}\alpha^{d-1} : \\ r_0, \ldots, r_{d-1} \in \mathbf{Q} \end{array} \right\}$$

$$\uparrow$$

$$\mathcal{O} = \left\{ \begin{array}{c} \text{algebraic integers} \\ \text{in } \mathbf{Q}(\alpha) \end{array} \right\}$$

$$\uparrow$$

$$\mathbf{Z}[f_d\alpha] = \left\{ \begin{array}{l} i_0 + i_1 f_d \alpha + \\ \cdots + i_{d-1} f_d^{d-1} \alpha^{d-1} : \\ i_0, \ldots, i_{d-1} \in \mathbf{Z} \end{array} \right\}$$

$$\downarrow f_d\alpha \mapsto f_d m$$

$$\mathbf{Z}/n = \{0, 1, \ldots, n-1\}$$

Build sq
congruen
with $i\mathbf{Z}$

Could re
higher-d
quadrati
for some
But let's

Say we h
$\prod_{(i,j)\in S}$
in $\mathbf{Q}(\alpha)$

$c^2 - 14, 25)$

ed $f \in \mathbf{Z}[x]$,

$\mathbf{Z}$.

$f_1 x^1 + f_0 x^0$.

or simplicity,

ys

selection.

of f.

t of

$(x/f_d) \in \mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) = \left\{ \begin{array}{l} r_0 + r_1\alpha + r_2\alpha^2 + \\ \cdots + r_{d-1}\alpha^{d-1} : \\ r_0, \ldots, r_{d-1} \in \mathbf{Q} \end{array} \right\}$$

$\uparrow$

$$\mathcal{O} = \left\{ \begin{array}{c} \text{algebraic integers} \\ \text{in } \mathbf{Q}(\alpha) \end{array} \right\}$$

$\uparrow$

$$\mathbf{Z}[f_d\alpha] = \left\{ \begin{array}{l} i_0 + i_1 f_d \alpha + \\ \cdots + i_{d-1} f_d^{d-1} \alpha^{d-1} : \\ i_0, \ldots, i_{d-1} \in \mathbf{Z} \end{array} \right\}$$

$\downarrow f_d\alpha \mapsto f_d m$

$$\mathbf{Z}/n = \{0, 1, \ldots, n-1\}$$

Build square in $\mathbf{Q}($

congruences $(i - j$

with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$

Could replace $i -$

higher-deg irred in

quadratics seem fa

for some number f

But let's not both

Say we have a squ

$\prod_{(i,j)\in S}(i - jm)($

in $\mathbf{Q}(\alpha)$; now wha

5)
c],

x^0.

ty,

$\mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) = \left\{ \begin{array}{l} r_0 + r_1\alpha + r_2\alpha^2 + \\ \cdots + r_{d-1}\alpha^{d-1} : \\ r_0, \ldots, r_{d-1} \in \mathbf{Q} \end{array} \right\}$$

$\uparrow$

$$\mathcal{O} = \left\{ \begin{array}{c} \text{algebraic integers} \\ \text{in } \mathbf{Q}(\alpha) \end{array} \right\}$$

$\uparrow$

$$\mathbf{Z}[f_d\alpha] = \left\{ \begin{array}{l} i_0 + i_1 f_d \alpha + \\ \cdots + i_{d-1} f_d^{d-1} \alpha^{d-1} : \\ i_0, \ldots, i_{d-1} \in \mathbf{Z} \end{array} \right\}$$

$\downarrow f_d\alpha \mapsto f_d m$

$$\mathbf{Z}/n = \{0, 1, \ldots, n-1\}$$

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j)\in S}(i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

$$\mathbf{Q}(\alpha) = \left\{ \begin{array}{l} r_0 + r_1\alpha + r_2\alpha^2 + \\ \cdots + r_{d-1}\alpha^{d-1}; \\ r_0, \ldots, r_{d-1} \in \mathbf{Q} \end{array} \right\}$$

$\uparrow$

$$\mathcal{O} = \left\{ \begin{array}{c} \text{algebraic integers} \\ \text{in } \mathbf{Q}(\alpha) \end{array} \right\}$$

$\uparrow$

$$\mathbf{Z}[f_d\alpha] = \left\{ \begin{array}{l} i_0 + i_1 f_d \alpha + \\ \cdots + i_{d-1} f_d^{d-1} \alpha^{d-1}; \\ i_0, \ldots, i_{d-1} \in \mathbf{Z} \end{array} \right\}$$

$\downarrow f_d\alpha \mapsto f_d m$

$$\mathbf{Z}/n = \{0, 1, \ldots, n-1\}$$

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j\alpha)$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j)\in S}(i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

$$= \left\{ \begin{array}{l} r_0 + r_1\alpha + r_2\alpha^2 + \\ \cdots + r_{d-1}\alpha^{d-1} : \\ r_0, \ldots, r_{d-1} \in \mathbf{Q} \end{array} \right\}$$

$$\left\{ \begin{array}{c} \text{algebraic integers} \\ \text{in } \mathbf{Q}(\alpha) \end{array} \right\}$$

$$= \left\{ \begin{array}{l} i_0 + i_1 f_d \alpha + \\ \cdots + i_{d-1} f_d^{d-1} \alpha^{d-1} : \\ i_0, \ldots, i_{d-1} \in \mathbf{Z} \end{array} \right\}$$

$\mapsto f_d m$

$= \{0, 1, \ldots, n-1\}$

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j\alpha)$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j)\in S}(i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

$\prod(i - j$ is a squa ring of i

Multiply putting compute $\prod(i - j$

Then ap $\varphi : \mathbf{Z}[f_d$ $f_d\alpha$ to $\varphi(r) - g$ In $\mathbf{Z}/n$ $g'(f_d m)$

$r_1\alpha + r_2\alpha^2 +$
$r_{d-1}\alpha^{d-1}$:
$, r_{d-1} \in \mathbf{Q}$

c integers
$\mathbf{Q}(\alpha)$

$i_1 f_d\alpha +$
$i_{d-1} f_d^{d-1}\alpha^{d-1}$:
$\ldots, i_{d-1} \in \mathbf{Z}$

$, n-1\}$

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j\alpha)$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j)\in S}(i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

$\prod(i - jm)(i - j\alpha)$ is a square in $\mathcal{O}$, ring of integers of

Multiply by $g'(f_d\alpha)^2$ putting square roo
compute r with r^2
$\prod(i - jm)(i - j\alpha)$

Then apply the rin
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$
$f_d\alpha$ to $f_d m$. Com
$\varphi(r) - g'(f_d m)\prod$
In $\mathbf{Z}/n$ have $\varphi(r)^2$
$g'(f_d m)^2 \prod(i - j$

$^2 +$
$\}$
$\mathbf{Q}$

$\}$

α^{d-1}:
$\mathbf{Z}$

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j\alpha)$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j)\in S}(i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

$\prod(i - jm)(i - j\alpha)f_d^2$ is a square in $\mathcal{O}$, ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$, putting square root into $\mathbf{Z}[f$ compute r with $r^2 = g'(f_d\alpha$ $\prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphis $\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking $f_d\alpha$ to f_dm. Compute gcd$\{$ $\varphi(r) - g'(f_dm)\prod(i - jm)$ In $\mathbf{Z}/n$ have $\varphi(r)^2 =$ $g'(f_dm)^2\prod(i - jm)^2 f_d^2$.

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j\alpha)$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j)\in S}(i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

$\prod(i - jm)(i - j\alpha)f_d^2$ is a square in $\mathcal{O}$, ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$, putting square root into $\mathbf{Z}[f_d\alpha]$: compute r with $r^2 = g'(f_d\alpha)^2 \cdot \prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphism $\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking $f_d\alpha$ to $f_d m$. Compute $\gcd\{n, \varphi(r) - g'(f_d m)\prod(i - jm)f_d\}$. In $\mathbf{Z}/n$ have $\varphi(r)^2 = g'(f_d m)^2 \prod(i - jm)^2 f_d^2$.

uare in $\mathbf{Q}(\alpha)$ from
nces $(i - jm)(i - j\alpha)$
$+ j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

eplace $i - jx$ by
eg irred in $\mathbf{Z}[x]$;
cs seem fairly small
e number fields.
s not bother.

have a square
$(i - jm)(i - j\alpha)$
; now what?

$\prod(i - jm)(i - j\alpha)f_d^2$
is a square in $\mathcal{O}$,
ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$,
putting square root into $\mathbf{Z}[f_d\alpha]$:
compute r with $r^2 = g'(f_d\alpha)^2 \cdot \prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking
$f_d\alpha$ to $f_d m$. Compute $\gcd\{n, \varphi(r) - g'(f_d m)\prod(i - jm)f_d\}$.
In $\mathbf{Z}/n$ have $\varphi(r)^2 = g'(f_d m)^2 \prod(i - jm)^2 f_d^2$.

How to
of congr

Start wi
e.g., y^2

Look for
y-smoot
y-smoot
$f_d i^d + \cdot$

Find enc
Perform
exponen

(α) from
$jm)(i - j\alpha)$
and $j > 0$.

jx by
$\mathbf{Z}[x]$;
airly small
fields.
er.

uare
$(i - j\alpha)$
t?

$\prod(i - jm)(i - j\alpha)f_d^2$
is a square in $\mathcal{O}$,
ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$,
putting square root into $\mathbf{Z}[f_d\alpha]$:
compute r with $r^2 = g'(f_d\alpha)^2 \cdot$
$\prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking
$f_d\alpha$ to $f_d m$. Compute $\gcd\{n,$
$\varphi(r) - g'(f_d m)\prod(i - jm)f_d\}$.
In $\mathbf{Z}/n$ have $\varphi(r)^2 =$
$g'(f_d m)^2 \prod(i - jm)^2 f_d^2$.

How to find squar
of congruences $(i$

Start with congrue
e.g., y^2 pairs $(i, j$

Look for y-smooth
y-smooth $i - jm$
y-smooth f_d norm
$f_d i^d + \cdots + f_0 j^d$

Find enough smoo
Perform linear alge
exponent vectors

$\alpha)$
0.

$\prod(i - jm)(i - j\alpha)f_d^2$
is a square in $\mathcal{O}$,
ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$,
putting square root into $\mathbf{Z}[f_d\alpha]$:
compute r with $r^2 = g'(f_d\alpha)^2 \cdot$
$\prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking
$f_d\alpha$ to $f_d m$. Compute $\gcd\{n,$
$\varphi(r) - g'(f_d m)\prod(i - jm)f_d\}$.
In $\mathbf{Z}/n$ have $\varphi(r)^2 =$
$g'(f_d m)^2 \prod(i - jm)^2 f_d^2$.

How to find square product
of congruences $(i - jm)(i -$

Start with congruences for,
e.g., y^2 pairs (i, j).

Look for y-smooth congruen
y-smooth $i - jm$ and
y-smooth f_d norm$(i - j\alpha) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j$

Find enough smooth congru
Perform linear algebra on
exponent vectors mod 2.

$\prod(i - jm)(i - j\alpha)f_d^2$
is a square in $\mathcal{O}$,
ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$,
putting square root into $\mathbf{Z}[f_d\alpha]$:
compute r with $r^2 = g'(f_d\alpha)^2$.
$\prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking
$f_d\alpha$ to $f_d m$. Compute $\gcd\{n,$
$\varphi(r) - g'(f_d m)\prod(i - jm)f_d\}$.
In $\mathbf{Z}/n$ have $\varphi(r)^2 =$
$g'(f_d m)^2\prod(i - jm)^2 f_d^2$.

How to find square product
of congruences $(i - jm)(i - j\alpha)$?

Start with congruences for,
e.g., y^2 pairs (i, j).

Look for y-smooth congruences:
y-smooth $i - jm$ and
y-smooth $f_d \operatorname{norm}(i - j\alpha) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$.

Find enough smooth congruences.
Perform linear algebra on
exponent vectors mod 2.

$m)(i - j\alpha)f_d^2$
are in $\mathcal{O}$,
ntegers of $\mathbf{Q}(\alpha)$.

by $g'(f_d\alpha)^2$,
square root into $\mathbf{Z}[f_d\alpha]$:
e r with $r^2 = g'(f_d\alpha)^2$.
$m)(i - j\alpha)f_d^2$.

pply the ring morphism
$\alpha] \to \mathbf{Z}/n$ taking
$f_d m$. Compute $\gcd\{n,$
$g'(f_d m)\prod(i - jm)f_d\}$.
have $\varphi(r)^2 =$
$^2\prod(i - jm)^2 f_d^2$.

How to find square product of congruences $(i - jm)(i - j\alpha)$?

Start with congruences for, e.g., y^2 pairs (i, j).

Look for y-smooth congruences: y-smooth $i - jm$ and y-smooth $f_d \operatorname{norm}(i - j\alpha) = f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$.

Find enough smooth congruences. Perform linear algebra on exponent vectors mod 2.

Exponen
many "r
many "a
a few "c

One rati
for each
Value or

One rati
Value 0
value 1 i

If $\prod(i -$
then vec
in ration

$\alpha)f_d^2$

$\mathbf{Q}(\alpha)$.

$\alpha)^2$,

ot into $\mathbf{Z}[f_d\alpha]$:

$^2 = g'(f_d\alpha)^2$.

$\alpha)f_d^2$.

ng morphism

taking

mpute $\gcd\{n,$

$\prod(i - jm)f_d\}$.

$^2 =$

$m)^2 f_d^2$.

How to find square product of congruences $(i - jm)(i - j\alpha)$?

Start with congruences for, e.g., y^2 pairs (i, j).

Look for y-smooth congruences:
y-smooth $i - jm$ and
y-smooth $f_d \operatorname{norm}(i - j\alpha) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$.

Find enough smooth congruences.
Perform linear algebra on exponent vectors mod 2.

Exponent vectors
many "rational" c
many "algebraic"
a few "character"

One rational comp
for each prime $p \leq$
Value $\operatorname{ord}_p(i - jm$

One rational comp
Value 0 if $i - jm$
value 1 if $i - jm$

If $\prod(i - jm)$ is a
then vectors add t
in rational compon

$f_d\alpha]$:
$\alpha)^2$.

sm

$n,$
$f_d\}$.

How to find square product
of congruences $(i - jm)(i - j\alpha)$?

Start with congruences for,
e.g., y^2 pairs (i, j).

Look for y-smooth congruences:
y-smooth $i - jm$ and
y-smooth $f_d \operatorname{norm}(i - j\alpha) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$.

Find enough smooth congruences.
Perform linear algebra on
exponent vectors mod 2.

Exponent vectors have
many "rational" component
many "algebraic" componen
a few "character" componen

One rational component
for each prime $p \leq y$.
Value $\operatorname{ord}_p(i - jm)$.

One rational component for
Value 0 if $i - jm > 0$,
value 1 if $i - jm < 0$.

If $\prod(i - jm)$ is a square
then vectors add to 0
in rational components.

How to find square product
of congruences $(i - jm)(i - j\alpha)$?

Start with congruences for,
e.g., y^2 pairs (i, j).

Look for y-smooth congruences:
y-smooth $i - jm$ and
y-smooth $f_d \operatorname{norm}(i - j\alpha) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$.

Find enough smooth congruences.
Perform linear algebra on
exponent vectors mod 2.

Exponent vectors have
many "rational" components,
many "algebraic" components,
a few "character" components.

One rational component
for each prime $p \leq y$.
Value $\operatorname{ord}_p(i - jm)$.

One rational component for -1.
Value 0 if $i - jm > 0$,
value 1 if $i - jm < 0$.

If $\prod(i - jm)$ is a square
then vectors add to 0
in rational components.

find square product
uences $(i - jm)(i - j\alpha)$?

th congruences for,
pairs (i, j).

y-smooth congruences:
h $i - jm$ and
h $f_d \operatorname{norm}(i - j\alpha) =$
$\cdots + f_0 j^d = j^d f(i/j)$.

ough smooth congruences.
linear algebra on
t vectors mod 2.

Exponent vectors have
many "rational" components,
many "algebraic" components,
a few "character" components.

One rational component
for each prime $p \leq y$.
Value $\operatorname{ord}_p(i - jm)$.

One rational component for -1.
Value 0 if $i - jm > 0$,
value 1 if $i - jm < 0$.

If $\prod(i - jm)$ is a square
then vectors add to 0
in rational components.

One alge
for each
p is a pr
$f_d \notin p\mathbf{Z}$
$r \in \mathbf{F}_p$;

Value 0
otherwis

This is t
the valu
at the p
Recall th
so no hig

e product
$-jm)(i-j\alpha)$?

ences for,
).

n congruences:
and
$(i-j\alpha) =$
$= j^d f(i/j)$.

oth congruences.
ebra on
mod 2.

Exponent vectors have
many "rational" components,
many "algebraic" components,
a few "character" components.

One rational component
for each prime $p \le y$.
Value $\mathrm{ord}_p(i-jm)$.

One rational component for -1.
Value 0 if $i-jm > 0$,
value 1 if $i-jm < 0$.

If $\prod(i-jm)$ is a square
then vectors add to 0
in rational components.

One algebraic com
for each pair (p, r)
p is a prime $\le y$;
$f_d \notin p\mathbf{Z}$; disc $f \notin$
$r \in \mathbf{F}_p$; $f(r) = 0$ i

Value 0 if $i - jr \notin$
otherwise $\mathrm{ord}_p(j^d$

This is the same a
the valuation of i
at the prime $p\mathcal{O} +$
Recall that $i\mathbf{Z} + j$
so no higher-degre

$- j\alpha)$?

nces:

$=$

$i)$.

ences.

Exponent vectors have
many "rational" components,
many "algebraic" components,
a few "character" components.

One rational component
for each prime $p \leq y$.
Value $\text{ord}_p(i - jm)$.

One rational component for -1.
Value 0 if $i - jm > 0$,
value 1 if $i - jm < 0$.

If $\prod(i - jm)$ is a square
then vectors add to 0
in rational components.

One algebraic component
for each pair (p, r) such tha
p is a prime $\leq y$;
$f_d \notin p\mathbf{Z}$; disc $f \notin p\mathbf{Z}$;
$r \in \mathbf{F}_p$; $f(r) = 0$ in $\mathbf{F}_p$.

Value 0 if $i - jr \notin p\mathbf{Z}$;
otherwise $\text{ord}_p(j^d f(i/j))$.

This is the same as
the valuation of $i - j\alpha$
at the prime $p\mathcal{O} + (f_d\alpha - f$
Recall that $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$,
so no higher-degree primes.

Exponent vectors have
many "rational" components,
many "algebraic" components,
a few "character" components.

One rational component
for each prime $p \le y$.
Value $\operatorname{ord}_p(i - jm)$.

One rational component for -1.
Value 0 if $i - jm > 0$,
value 1 if $i - jm < 0$.

If $\prod(i - jm)$ is a square
then vectors add to 0
in rational components.

One algebraic component
for each pair (p, r) such that
p is a prime $\le y$;
$f_d \notin p\mathbf{Z}$; disc $f \notin p\mathbf{Z}$;
$r \in \mathbf{F}_p$; $f(r) = 0$ in $\mathbf{F}_p$.

Value 0 if $i - jr \notin p\mathbf{Z}$;
otherwise $\operatorname{ord}_p(j^d f(i/j))$.

This is the same as
the valuation of $i - j\alpha$
at the prime $p\mathcal{O} + (f_d\alpha - f_d r)\mathcal{O}$.
Recall that $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$,
so no higher-degree primes.

nt vectors have
ational" components,
lgebraic" components,
character" components.

onal component
prime $p \leq y$.
$\mathrm{ord}_p(i - jm)$.

onal component for -1.
if $i - jm > 0$,
if $i - jm < 0$.

$- jm)$ is a square
ctors add to 0
al components.

One algebraic component
for each pair (p, r) such that
p is a prime $\leq y$;
$f_d \notin p\mathbf{Z}$; disc $f \notin p\mathbf{Z}$;
$r \in \mathbf{F}_p$; $f(r) = 0$ in $\mathbf{F}_p$.

Value 0 if $i - jr \notin p\mathbf{Z}$;
otherwise $\mathrm{ord}_p(j^d f(i/j))$.

This is the same as
the valuation of $i - j\alpha$
at the prime $p\mathcal{O} + (f_d\alpha - f_d r)\mathcal{O}$.
Recall that $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$,
so no higher-degree primes.

One cha
for each
p in a sh

Value 0
square in

If $\prod(i -$
then vec
in algebr
and char

have
omponents,
components,
components.

ponent
$\leq y$.
a).

ponent for -1.
> 0,
< 0.

square
o 0
nents.

One algebraic component
for each pair (p, r) such that
p is a prime $\leq y$;
$f_d \notin p\mathbf{Z}$; disc $f \notin p\mathbf{Z}$;
$r \in \mathbf{F}_p$; $f(r) = 0$ in $\mathbf{F}_p$.

Value 0 if $i - jr \notin p\mathbf{Z}$;
otherwise $\mathrm{ord}_p(j^d f(i/j))$.

This is the same as
the valuation of $i - j\alpha$
at the prime $p\mathcal{O} + (f_d\alpha - f_d r)\mathcal{O}$.
Recall that $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$,
so no higher-degree primes.

One character com
for each pair (p, r)
p in a short range

Value 0 if $i - jr$ i
square in $\mathbf{F}_p$, else

If $\prod(i - j\alpha)$ is a s
then vectors add t
in algebraic compo
and character com

s,
ts,
nts.

−1.

One algebraic component
for each pair (p, r) such that
p is a prime $\leq y$;
$f_d \notin p\mathbf{Z}$; disc $f \notin p\mathbf{Z}$;
$r \in \mathbf{F}_p$; $f(r) = 0$ in $\mathbf{F}_p$.

Value 0 if $i - jr \notin p\mathbf{Z}$;
otherwise $\mathrm{ord}_p(j^d f(i/j))$.

This is the same as
the valuation of $i - j\alpha$
at the prime $p\mathcal{O} + (f_d\alpha - f_d r)\mathcal{O}$.
Recall that $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$,
so no higher-degree primes.

One character component
for each pair (p, r) with
p in a short range above y.

Value 0 if $i - jr$ is a
square in $\mathbf{F}_p$, else 1.

If $\prod(i - j\alpha)$ is a square
then vectors add to 0
in algebraic components
and character components.

One algebraic component
for each pair (p, r) such that
p is a prime $\leq y$;
$f_d \notin p\mathbf{Z}$; disc $f \notin p\mathbf{Z}$;
$r \in \mathbf{F}_p$; $f(r) = 0$ in $\mathbf{F}_p$.

Value 0 if $i - jr \notin p\mathbf{Z}$;
otherwise $\mathrm{ord}_p(j^d f(i/j))$.

This is the same as
the valuation of $i - j\alpha$
at the prime $p\mathcal{O} + (f_d\alpha - f_d r)\mathcal{O}$.
Recall that $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$,
so no higher-degree primes.

One character component
for each pair (p, r) with
p in a short range above y.

Value 0 if $i - jr$ is a
square in $\mathbf{F}_p$, else 1.

If $\prod(i - j\alpha)$ is a square
then vectors add to 0
in algebraic components
and character components.

ebraic component
pair (p, r) such that
rime $\leq y$;
; disc $f \notin p\mathbf{Z}$;
$f(r) = 0$ in $\mathbf{F}_p$.

if $i - jr \notin p\mathbf{Z}$;
e $\mathrm{ord}_p(j^d f(i/j))$.

he same as
ation of $i - j\alpha$
rime $p\mathcal{O} + (f_d\alpha - f_d r)\mathcal{O}$.
hat $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$,
gher-degree primes.

One character component
for each pair (p, r) with
p in a short range above y.

Value 0 if $i - jr$ is a
square in $\mathbf{F}_p$, else 1.

If $\prod(i - j\alpha)$ is a square
then vectors add to 0
in algebraic components
and character components.

Converse
adding t

$\prod(i - j$

Is $\prod(i -$
Ideal $\prod($
square o
What ab
Even if i
is square
Even if i
by squar
does squ

nponent
) such that

$p\mathbf{Z}$;
in $\mathbf{F}_p$.

$\not\equiv p\mathbf{Z}$;
$f(i/j)$).

s
$- j\alpha$
$- (f_d\alpha - f_d r)\mathcal{O}$.
$\mathbf{Z} = \mathbf{Z}$,
ee primes.

One character component
for each pair (p, r) with
p in a short range above y.

Value 0 if $i - jr$ is a
square in $\mathbf{F}_p$, else 1.

If $\prod(i - j\alpha)$ is a square
then vectors add to 0
in algebraic components
and character components.

Conversely, consid
adding to 0 in all

$\prod(i - jm)$ must

Is $\prod(i - j\alpha)$ a sq
Ideal $\prod(i - j\alpha)\mathcal{O}$
square outside f_d
What about prime
Even if ideal is squ
is square root prin
Even if ideal is ge
by square of eleme
does square equal

t

$f_d r)\mathcal{O}$.

One character component
for each pair (p, r) with
p in a short range above y.

Value 0 if $i - jr$ is a
square in $\mathbf{F}_p$, else 1.

If $\prod(i - j\alpha)$ is a square
then vectors add to 0
in algebraic components
and character components.

Conversely, consider vectors
adding to 0 in all componen

$\prod(i - jm)$ must be a squar

Is $\prod(i - j\alpha)$ a square?
Ideal $\prod(i - j\alpha)\mathcal{O}$ must be
square outside f_d disc f.
What about primes in f_d dis
Even if ideal is square,
is square root principal?
Even if ideal is generated
by square of element,
does square equal $\prod(i - j\alpha$

One character component
for each pair (p, r) with
p in a short range above y.

Value 0 if $i - jr$ is a
square in $\mathbf{F}_p$, else 1.

If $\prod(i - j\alpha)$ is a square
then vectors add to 0
in algebraic components
and character components.

Conversely, consider vectors
adding to 0 in all components.

$\prod(i - jm)$ must be a square.

Is $\prod(i - j\alpha)$ a square?
Ideal $\prod(i - j\alpha)\mathcal{O}$ must be
square outside f_d disc f.
What about primes in f_d disc f?
Even if ideal is square,
is square root principal?
Even if ideal is generated
by square of element,
does square equal $\prod(i - j\alpha)$?

racter component
pair (p, r) with
hort range above y.

if $i - jr$ is a
n $\mathbf{F}_p$, else 1.

$- j\alpha)$ is a square
ctors add to 0
raic components
racter components.

Conversely, consider vectors
adding to 0 in all components.

$\prod(i - jm)$ must be a square.

Is $\prod(i - j\alpha)$ a square?
Ideal $\prod(i - j\alpha)\mathcal{O}$ must be
square outside f_d disc f.
What about primes in f_d disc f?
Even if ideal is square,
is square root principal?
Even if ideal is generated
by square of element,
does square equal $\prod(i - j\alpha)$?

Obstruct
conjectu
"(f_d disc

A few ch
suffice t
forcing $\prod$
to be a s

Can be e
easy to
with mo
non-squa

nponent
) with
above y.

s a
1.

square
o 0
onents
nponents.

Conversely, consider vectors
adding to 0 in all components.

$\prod(i - jm)$ must be a square.

Is $\prod(i - j\alpha)$ a square?
Ideal $\prod(i - j\alpha)\mathcal{O}$ must be
square outside $f_d \operatorname{disc} f$.
What about primes in $f_d \operatorname{disc} f$?
Even if ideal is square,
is square root principal?
Even if ideal is generated
by square of element,
does square equal $\prod(i - j\alpha)$?

Obstruction group
conjecturally very
"($f_d \operatorname{disc} f$)-Selme

A few characters
suffice to generate
forcing $\prod(i - j\alpha)$
to be a square.

Can be quite slopp
easy to redo linear
with more charact
non-square is enco

Conversely, consider vectors adding to 0 in all components.

$\prod(i - jm)$ must be a square.

Is $\prod(i - j\alpha)$ a square?
Ideal $\prod(i - j\alpha)\mathcal{O}$ must be square outside $f_d \operatorname{disc} f$.
What about primes in $f_d \operatorname{disc} f$?
Even if ideal is square, is square root principal?
Even if ideal is generated by square of element, does square equal $\prod(i - j\alpha)$?

Obstruction group is small, conjecturally very small.
"$(f_d \operatorname{disc} f)$-Selmer group."

A few characters suffice to generate dual, forcing $\prod(i - j\alpha)$ to be a square.

Can be quite sloppy here; easy to redo linear algebra with more characters if non-square is encountered.

Conversely, consider vectors
adding to 0 in all components.

$\prod(i - jm)$ must be a square.

Is $\prod(i - j\alpha)$ a square?
Ideal $\prod(i - j\alpha)\mathcal{O}$ must be
square outside $f_d \operatorname{disc} f$.
What about primes in $f_d \operatorname{disc} f$?
Even if ideal is square,
is square root principal?
Even if ideal is generated
by square of element,
does square equal $\prod(i - j\alpha)$?

Obstruction group is small,
conjecturally very small.
"$(f_d \operatorname{disc} f)$-Selmer group."

A few characters
suffice to generate dual,
forcing $\prod(i - j\alpha)$
to be a square.

Can be quite sloppy here;
easy to redo linear algebra
with more characters if
non-square is encountered.

ely, consider vectors
o 0 in all components.

m) must be a square.

$- j\alpha$) a square?
$(i - j\alpha)\mathcal{O}$ must be
utside $f_d \operatorname{disc} f$.
bout primes in $f_d \operatorname{disc} f$?
deal is square,
e root principal?
deal is generated
re of element,
uare equal $\prod(i - j\alpha)$?

Obstruction group is small,
conjecturally very small.
"($f_d \operatorname{disc} f$)-Selmer group."

A few characters
suffice to generate dual,
forcing $\prod(i - j\alpha)$
to be a square.

Can be quite sloppy here;
easy to redo linear algebra
with more characters if
non-square is encountered.

Sublatti

Consider
of pairs
q divides

Assume
$(i - jm$
expands
before d

Number
within a
on $(i -$
is propo

er vectors
components.

be a square.

uare?
must be
disc f.
es in $f_d \operatorname{disc} f$?
uare,
cipal?
nerated
ent,
$\prod(i - j\alpha)$?

Obstruction group is small,
conjecturally very small.
"$(f_d \operatorname{disc} f)$-Selmer group."

A few characters
suffice to generate dual,
forcing $\prod(i - j\alpha)$
to be a square.

Can be quite sloppy here;
easy to redo linear algebra
with more characters if
non-square is encountered.

Sublattices

Consider a sublatt
of pairs (i, j) whe
q divides $j^d f(i/j)$

Assume squarish la
$(i - jm)j^d f(i/j)$
expands by factor
before division by

Number of sublatt
within any particu
on $(i - jm)j^d f(i$
is proportional to

ts.

re.

c f?

)?

Obstruction group is small,
conjecturally very small.
"(f_d disc f)-Selmer group."

A few characters
suffice to generate dual,
forcing $\prod(i - j\alpha)$
to be a square.

Can be quite sloppy here;
easy to redo linear algebra
with more characters if
non-square is encountered.

Sublattices

Consider a sublattice
of pairs (i, j) where
q divides $j^d f(i/j)$.

Assume squarish lattice.
$(i - jm)j^d f(i/j)$
expands by factor $q^{(d+1)/2}$
before division by q.

Number of sublattice elemen
within any particular bound
on $(i - jm)j^d f(i/j)$
is proportional to $q^{-(d-1)/(d}$

Obstruction group is small,
conjecturally very small.
"(f_d disc f)-Selmer group."

A few characters
suffice to generate dual,
forcing $\prod(i - j\alpha)$
to be a square.

Can be quite sloppy here;
easy to redo linear algebra
with more characters if
non-square is encountered.

Sublattices

Consider a sublattice
of pairs (i, j) where
q divides $j^d f(i/j)$.

Assume squarish lattice.
$(i - jm)j^d f(i/j)$
expands by factor $q^{(d+1)/2}$
before division by q.

Number of sublattice elements
within any particular bound
on $(i - jm)j^d f(i/j)$
is proportional to $q^{-(d-1)/(d+1)}$.

tion group is small,
rally very small.
c f)-Selmer group."

haracters
o generate dual,
$\prod(i - j\alpha)$
square.

quite sloppy here;
redo linear algebra
re characters if
are is encountered.

Sublattices

Consider a sublattice
of pairs (i, j) where
q divides $j^d f(i/j)$.

Assume squarish lattice.
$(i - jm)j^d f(i/j)$
expands by factor $q^{(d+1)/2}$
before division by q.

Number of sublattice elements
within any particular bound
on $(i - jm)j^d f(i/j)$
is proportional to $q^{-(d-1)/(d+1)}$.

Compare
conjectu
times as
by using
all y-sm

Separate
$i - jm$ a
for more

Limit co
increasin

is small,
small.
r group."

dual,

by here;
algebra
ers if
ountered.

Sublattices

Consider a sublattice
of pairs (i, j) where
q divides $j^d f(i/j)$.

Assume squarish lattice.
$(i - jm)j^d f(i/j)$
expands by factor $q^{(d+1)/2}$
before division by q.

Number of sublattice elements
within any particular bound
on $(i - jm)j^d f(i/j)$
is proportional to $q^{-(d-1)/(d+1)}$.

Compared to just
conjecturally obtai
times as many con
by using sublattice
all y-smooth integ

Separately conside
$i - jm$ and $j^d f(i$
for more precise a

Limit congruences
increasing smooth

Sublattices

Consider a sublattice
of pairs (i, j) where
q divides $j^d f(i/j)$.

Assume squarish lattice.
$(i - jm)j^d f(i/j)$
expands by factor $q^{(d+1)/2}$
before division by q.

Number of sublattice elements
within any particular bound
on $(i - jm)j^d f(i/j)$
is proportional to $q^{-(d-1)/(d+1)}$.

Compared to just using $q =$
conjecturally obtain $y^{4/(d+1)}$
times as many congruences
by using sublattices for
all y-smooth integers $q \leq y^2$

Separately consider
$i - jm$ and $j^d f(i/j)/q$
for more precise analysis.

Limit congruences according
increasing smoothness chanc

Sublattices

Consider a sublattice
of pairs (i, j) where
q divides $j^d f(i/j)$.

Assume squarish lattice.
$(i - jm)j^d f(i/j)$
expands by factor $q^{(d+1)/2}$
before division by q.

Number of sublattice elements
within any particular bound
on $(i - jm)j^d f(i/j)$
is proportional to $q^{-(d-1)/(d+1)}$.

Compared to just using $q = 1$,
conjecturally obtain $y^{4/(d+1)+o(1)}$
times as many congruences
by using sublattices for
all y-smooth integers $q \leq y^2$.

Separately consider
$i - jm$ and $j^d f(i/j)/q$
for more precise analysis.

Limit congruences accordingly,
increasing smoothness chances.

ces

r a sublattice
(i, j) where
s $j^d f(i/j)$.

squarish lattice.
$)j^d f(i/j)$
by factor $q^{(d+1)/2}$
ivision by q.

of sublattice elements
ny particular bound
$jm)j^d f(i/j)$
rtional to $q^{-(d-1)/(d+1)}$.

Compared to just using $q = 1$,
conjecturally obtain $y^{4/(d+1)+o(1)}$
times as many congruences
by using sublattices for
all y-smooth integers $q \leq y^2$.

Separately consider
$i - jm$ and $j^d f(i/j)/q$
for more precise analysis.

Limit congruences accordingly,
increasing smoothness chances.

Multiple

Assume
is also ir

Pick $\beta \in$
Two con
$(i - jm)$
Expand
handle b

Merge s
by testin
abortin

Can use
$f + 2(x$

ice
re
.
attice.

$q^{(d+1)/2}$
q.

tice elements
lar bound
$/j)$
$q^{-(d-1)/(d+1)}$.

Compared to just using $q = 1$,
conjecturally obtain $y^{4/(d+1)+o(1)}$
times as many congruences
by using sublattices for
all y-smooth integers $q \leq y^2$.

Separately consider
$i - jm$ and $j^d f(i/j)/q$
for more precise analysis.

Limit congruences accordingly,
increasing smoothness chances.

Multiple number f

Assume that $f +$
is also irred.

Pick $\beta \in \mathbf{C}$, root
Two congruences
$(i - jm)(i - j\alpha)$; (
Expand exponent
handle both $\mathbf{Q}(\alpha)$

Merge smoothness
by testing $i - jm$
aborting if $i - jm$

Can use many nu
$f + 2(x - m)$ etc.

Compared to just using $q = 1$,
conjecturally obtain $y^{4/(d+1)+o(1)}$
times as many congruences
by using sublattices for
all y-smooth integers $q \leq y^2$.

Separately consider
$i - jm$ and $j^d f(i/j)/q$
for more precise analysis.

Limit congruences accordingly,
increasing smoothness chances.

nts

$+1)}$.

Multiple number fields

Assume that $f + x - m \in \mathbf{Z}$
is also irred.

Pick $\beta \in \mathbf{C}$, root of $f + x -$
Two congruences for (i, j):
$(i - jm)(i - j\alpha)$; $(i - jm)(i$
Expand exponent vectors to
handle both $\mathbf{Q}(\alpha)$ and $\mathbf{Q}(\beta$

Merge smoothness tests
by testing $i - jm$ first,
aborting if $i - jm$ not smoo

Can use many number fields
$f + 2(x - m)$ etc.

Compared to just using $q = 1$,
conjecturally obtain $y^{4/(d+1)+o(1)}$
times as many congruences
by using sublattices for
all y-smooth integers $q \leq y^2$.

Separately consider
$i - jm$ and $j^d f(i/j)/q$
for more precise analysis.

Limit congruences accordingly,
increasing smoothness chances.

Multiple number fields

Assume that $f + x - m \in \mathbf{Z}[x]$
is also irred.

Pick $\beta \in \mathbf{C}$, root of $f + x - m$.
Two congruences for (i, j):
$(i - jm)(i - j\alpha)$; $(i - jm)(i - j\beta)$.
Expand exponent vectors to
handle both $\mathbf{Q}(\alpha)$ and $\mathbf{Q}(\beta)$.

Merge smoothness tests
by testing $i - jm$ first,
aborting if $i - jm$ not smooth.

Can use many number fields:
$f + 2(x - m)$ etc.