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.

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.

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

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

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

$611 = 47 \cdot 13$.

Why did this find a factor of 611?

Was it just blind luck:

$\mathrm{gcd}\{611, \mathrm{random}\} = 47$?

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 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 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 $n = 671$:

$$\begin{aligned}
1(n+\ \ 1) &= 2^5 3^1 5^0 7^1;\\
4(n+\ \ 4) &= 2^2 3^3 5^2 7^0;\\
15(n+15) &= 2^1 3^1 5^1 7^3;\\
49(n+49) &= 2^4 3^2 5^1 7^2;\\
64(n+64) &= 2^6 3^1 5^1 7^2.
\end{aligned}$$

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

e.g. for $n = 671$:

$$
\begin{aligned}
1(n+\ \ 1) &= 2^5 3^1 5^0 7^1;\\
4(n+\ \ 4) &= 2^2 3^3 5^2 7^0;\\
15(n+15) &= 2^1 3^1 5^1 7^3;\\
49(n+49) &= 2^4 3^2 5^1 7^2;\\
64(n+64) &= 2^6 3^1 5^1 7^2.
\end{aligned}
$$

$\mathbf{F}_2$-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: $\mathbf{Q}$ 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?

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 $\le y$?

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

Consider, e.g., $y = \lfloor n^{1/10} \rfloor$.
Uniform random integer in $[1, y^2]$ has y-smoothness chance ≈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 $\mathbf{Q}$ 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:
$\mathbf{Q}$ 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 $\mathbf{Q}$ 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.

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 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. $n = 314159265358979323$:

Original $\mathbf{Q}$ sieve:

i	$n+i$
1	314159265358979324
2	314159265358979325
3	314159265358979326

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

$$(q-(n \bmod q))\frac{n+q-(n \bmod q)}{q}$$

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 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 $\mathbf{Q}$

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

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:

$$\begin{tikzcd}
\mathbf{Q}[x] \arrow[r, "x \mapsto \sqrt{14}"] & \mathbf{Q}[\sqrt{14}] = \mathbf{Q}(\sqrt{14}) \\
\mathbf{Z}[x] \arrow[u] \arrow[r, "x \mapsto \sqrt{14}"] & \mathbf{Z}[\sqrt{14}] \arrow[u] \arrow[d, "\sqrt{14} \mapsto 25"] \\
& \mathbf{Z}/611
\end{tikzcd}$$

$\mathbf{Z}[x]$ 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 $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

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 $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$$
\begin{tikzcd}
\mathbf{Q}(\alpha) = \left\{ \begin{array}{l} r_0 + r_1\alpha + r_2\alpha^2 + \\ \cdots + r_{d-1}\alpha^{d-1} : \\ r_0, \ldots, r_{d-1} \in \mathbf{Q} \end{array} \right\} \\
\mathcal{O} = \left\{ \begin{array}{c} \text{algebraic integers} \\ \text{in } \mathbf{Q}(\alpha) \end{array} \right\} \arrow[u] \\
\mathbf{Z}[f_d\alpha] = \left\{ \begin{array}{l} i_0 + i_1 f_d\alpha + \\ \cdots + i_{d-1} f_d^{d-1}\alpha^{d-1} : \\ i_0, \ldots, i_{d-1} \in \mathbf{Z} \end{array} \right\} \arrow[u] \arrow[d, "f_d\alpha \mapsto f_d m"] \\
\mathbf{Z}/n = \{0, 1, \ldots, n-1\}
\end{tikzcd}
$$

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 $\varphi(r)^2 =$
$g'(f_d m)^2 \prod(i - jm)^2 f_d^2$.

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 $p \le y$.
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 $\leq y$;
$f_d \notin p\mathbf{Z}$; $\operatorname{disc} f \notin p\mathbf{Z}$;
$r \in \mathbf{F}_p$; $f(r) = 0$ 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.

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 $f_d \operatorname{disc} f$.
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.

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 $q \le y^2$.

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.