Integer factorization,
part 1: the $\mathbf{Q}$ sieve

Integer factorization,
part 2: detecting smoothness

Integer factorization,
part 3: the number-field sieve

D. J. Bernstein

Problem: Factor 611.

The $\mathbf{Q}$ sieve forms 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 forms 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 $\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/n$, $\sqrt{14} \mapsto 25$, since $25^2 = 14$ in $\mathbf{Z}/n$.

Apply ring morphism to square:

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

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

Unsurprising to find factor.

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

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

Asymptotic cost exponents

Number of bit operations in number-field sieve, with theorists' parameters, is $L^{1.90\ldots+o(1)}$ where $L = \exp((\log n)^{1/3}(\log\log n)^{2/3})$.

What are theorists' parameters?

Choose degree d with $d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.40\ldots+o(1)$.

Choose integer $m \approx n^{1/d}$.
Write n as
$m^d + f_{d-1}m^{d-1} + \cdots + f_1 m + f_0$
with each f_k below $n^{(1+o(1))/d}$.
Choose f with some randomness
in case there are bad f's.

Test smoothness of $i - jm$
for all coprime pairs (i, j)
with $1 \le i, j \le L^{0.95\ldots+o(1)}$,
using primes $\le L^{0.95\ldots+o(1)}$.

$L^{1.90\ldots+o(1)}$ pairs.
Conjecturally $L^{1.65\ldots+o(1)}$
smooth values of $i - jm$.

Use $L^{0.12\ldots+o(1)}$ number fields.

For each (i, j)
with smooth $i - jm$,
test smoothness of $i - j\alpha$
and $i - j\beta$ and so on,
using primes $\le L^{0.82\ldots+o(1)}$.

$L^{1.77\ldots+o(1)}$ tests.
Each $|j^d f(i/j)| \le m^{2.86\ldots+o(1)}$.
Conjecturally $L^{0.95\ldots+o(1)}$
smooth congruences.

$L^{0.95\ldots+o(1)}$ components
in the exponent vectors.

Three sizes of numbers here:

$(\log n)^{1/3}(\log\log n)^{2/3}$ bits:
y, i, j.

$(\log n)^{2/3}(\log\log n)^{1/3}$ bits:
m, $i - jm$, $j^d f(i/j)$.

$\log n$ bits: n.

Unavoidably $1/3$ in exponent:
usual smoothness optimization
forces $(\log y)^2 \approx \log m$;
balancing norms with m
forces $d \log y \approx \log m$;
and $d \log m \approx \log n$.

The number-field sieve
is asymptotically much faster
than the quadratic sieve
and the elliptic-curve method.

Also works well in practice.

Latest record: NFS found
two prime factors $\approx 2^{332}$
of "RSA-200" challenge, using
$\approx 5 \cdot 10^{18}$ Opteron cycles.

Batch NFS

The number-field sieve used
$L^{1.90\ldots+o(1)}$ bit operations
finding smooth $i - jm$; only
$L^{1.77\ldots+o(1)}$ bit operations
finding smooth $j^d f(i/j)$.

Many n's can share one m;
$L^{1.90\ldots+o(1)}$ bit operations
to find squares for *all* n's.

Oops, linear algebra hurts;
fix by reducing y.
But still end up factoring
batch in much less time than
factoring each n separately.