Rethinking the number field sieve

D. J. Bernstein
University of Illinois at Chicago

NSF DMS–9970409

Combining congruences

Want to factor n.

Consider pairs (g, h)
with $g \equiv h \pmod{n}$.

Find set S of pairs so that
$\prod_{(g,h)\in S} g$ is a square and
$\prod_{(g,h)\in S} h$ is a square.

Then $a^2 \equiv b^2 \pmod{n}$
where $a = \sqrt{\prod g}$, $b = \sqrt{\prod h}$.

The continued-fraction method

For each convergent p/q to $\sqrt{n}$:
$g = (p \bmod n)^2$, $h = p^2 - nq^2$.
Then $g \equiv h \pmod{n}$.

Focus on **smooth** h's:
no large prime factors.
Find square products of h's by
linear algebra on h factorizations.

(Lehmer, Powers,
Brillhart, Morrison)

How to find all prime factors $\leq y$ of a nonzero integer h?

Assume h has $(\log y)^{O(1)}$ digits.

Trial division: Time $\leq y^{1+o(1)}$.

Fast-factorials method:
Time $\leq y^{1/2+o(1)}$. (Pollard)

Hyperelliptic-curve method:
Time $\leq \exp((\log y)^{2/3+o(1)})$
with negligible chance of error.
(Lenstra, Pila, Pomerance)

Elliptic-curve method:
Conjectured time $\leq$
$\exp\sqrt{(2+o(1))\log y \log\log y}$
with negligible chance of error.
(Lenstra)

New method:
Time $(\log y)^{O(1)}$ if there are
at least $y/(\log y)^{O(1)}$
h's to handle at once.

Number of h's to handle
is roughly y^2 in
congruence-combining methods.

"How to find
small factors of integers"
`http://cr.yp.to/papers/sf.dvi`

"Factoring into coprimes
in essentially linear time"
`http://cr.yp.to/papers/dcba.dvi`

Given set P of primes,
set S of nonzero integers:

Find $x = \prod_{h \in S} h$.
Find $Q = \{q \in P : x \bmod q = 0\}$.
If $\#S \leq 1$: Print (Q, S) and stop.
Choose $T \subseteq S$, $\#T = \lfloor \#S/2 \rfloor$.
Recursively handle Q, T.
Recursively handle $Q, S - T$.

Find x mod q_1, x mod q_2, etc.
by computing
x mod $q_1 q_2$, x mod $q_3 q_4$, etc.
recursively, then
x mod $q_1 q_2$ mod q_1,
x mod $q_1 q_2$ mod q_2,
x mod $q_3 q_4$ mod q_3, etc.

(Borodin, Moenck)

The quadratic sieve

Combine pairs $(a^2, a^2 - n)$
where $a \approx \sqrt{n}$.

Sieving finds small primes in
$a^2 - n$ for many consecutive a's:

	2		2		2		2		2		2		2		2		2	
3	3		3	3		3	3		3	3		3	3		3	3		3
	11				11							11				11		
13					13								13					13
	17															17		17
										19								19
												31						31
																41		

(Schroeppel, Pomerance)

Multiple lattices

For many (d, k) with
d square, $k^2 \equiv n \pmod{d}$:
Sieve over $\{a : a \equiv k \pmod{d}\}$.

For S values of $a \equiv k \pmod{d}$:
$\left|a - \sqrt{n}\right|$ up to $\approx Sd/2$
so $\left|a^2 - n\right|/d$ up to $\approx S\sqrt{n}$.

("special d": Davis, Holdridge;
"MPQS": Montgomery;
"lattice sieve": Pollard)

How to choose S

Make S as large as possible:
overhead is divided by S.

Make S as small as possible:
then $(a^2 - n)/d$ is small
and random access is fast
in a size-S sieve array.

(Example of sieving in L1 cache:
`http://cr.yp.to`
`/primegen.html`)

Standard solution ("early abort," aka "multiple large prime"):

1. Sieve using *some* primes.
2. Discard unlikely a's.
3. Check each remaining $a^2 - n$.

Faster step 3
$\Rightarrow$ can keep more a's in step 2
$\Rightarrow$ can sieve less in step 1
$\Rightarrow$ can safely reduce S.

The number field sieve

Fix algebraic numbers γ_0, γ_1
and ring maps $\mathbf{Z}[\gamma_i] \xrightarrow{\text{mod } n} \mathbf{Z}/n$
with $\gamma_0 \bmod n = \gamma_1 \bmod n$.

Combine pairs $(a - b\gamma_0, a - b\gamma_1)$
with small $a, b \in \mathbf{Z}$.
Find smooth pairs by sieving.

(Pollard, Buhler, Lenstra,
Pomerance, Adleman)

e.g. $n \approx 10^{300}$:

Choose $\gamma_0 \in \mathbf{Z}$, $\gamma_0 \approx 10^{40}$.

Find polynomial f over $\mathbf{Z}$
with $n = f(\gamma_0)$,
$\deg f = 7$, small coefficients.
Assume that f_7 is coprime to n.

Let γ_1 be a root of f.

Use multiple lattices
as in quadratic sieve.
Faster factoring allows faster sieve
and smaller pairs (g, h).

Bound on (g, h) grows with d,
so use more pairs (a, b)
for smaller d.

Coppersmith's variant

Sieve to find smooth $a - b\gamma_0$.
For each smooth $a - b\gamma_0$:
Check $a - b\gamma_1$.

Faster than sieving $a - b\gamma_1$.

Have time to also try
$a - b\gamma_2, a - b\gamma_3, \ldots$.
Reduce bounds accordingly.

Parameter selection

How to choose $\deg f$, γ_0,
y for γ_0, y for γ_1, y for γ_2,
range of (a, b), sieve limit, etc.?

Many sensible possibilities
$\quad\downarrow$ quickly estimate NFS time
Attractive possibilities
$\quad\downarrow$ accurately estimate NFS time
Best of the attractive possibilities

Can compute at reasonable speed a conjecturally accurate estimate for NFS time. (new)

Highlight: Very fast algorithm to compute tight bounds on smoothness probabilities.

e.g. lower bounds on $\Psi(x, 10^6)$ for $x \in \{2^0, 2^{1/776}, \ldots, 2^{262143/776}\}$ with relative log error $< 10^{-4}$ in $7 \cdot 10^{10}$ Pentium-II cycles.

Method: Change primes slightly.
e.g. increase 3 to $2^{1230/776}$,
increase 5 to $2^{1802/776}$, etc.

This changes the Dirichlet series for smooth integers into a fractional power series.
Use fast series exponentiation.

`http://cr.yp.to`
`/psibound.html`