Three algorithms related to the number-field sieve

D. J. Bernstein

Thanks to:
University of Illinois at Chicago
NSF DMS–0140542
Alfred P. Sloan Foundation

The number-field sieve

Goal: Find
$\{(x, y) \in \mathbf{Z}^2 : xy = 611\}$.

The $\mathbf{Q}$ sieve forms a square
as product of $c(c + 611d)$
for several pairs (c, d):
$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410000\}$
$= 47$.
47 and $611/47 = 13$ are prime,
so $\{x\} = \{\pm 1, \pm 13, \pm 47, \pm 611\}$.

The $\mathbf{Q}(\sqrt{14})$ sieve forms a square as product of $(c + 25d)(c + \sqrt{14}d)$ for several pairs (c, d):

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

Compute

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

$v = 112 - 16 \cdot 25$,

$\gcd\{611, u - v\} = 13$.

How to find these squares?

Traditional approach:

Choose H, R with $26 \cdot 14 \cdot R^3 = H$.

Look at all pairs (c, d)
in $[-R, R] \times [0, R]$
with $(c + 25d)(c^2 - 14d^2) \neq 0$
and $\gcd\{c, d\} = 1$.

$(c + 25d)(c^2 - 14d^2)$ is small:
between $-H$ and H. Conjecturally,
good chance of being smooth.
Many smooths $\Rightarrow$ square.

Find more pairs (c, d)
with $\left|(c+25d)(c^2-14d^2)\right| \le H$
in a less balanced rectangle.
(1999 Brian Murphy)

Can do better: set of (c, d)
with $\left|(c+25d)(c^2-14d^2)\right| \le H$
extends far beyond any inscribed
rectangle. Find c range for each d.
(Bob Silverman, Scott Contini,
Arjen Lenstra)

Algorithm 1 of this talk:
estimate, much more quickly,
accurately, number of pairs (c, d).

Take any nonconstant $f \in \mathbf{Z}[x]$,
all real roots order $< (\deg f)/2$:
e.g., $f = (x + 25)(x^2 - 14)$.

Area of $\{(c, d) \in \mathbf{R} \times \mathbf{R} : d > 0,$
$|d^{\deg f} f(c/d)| \leq H\}$
is $(1/2)H^{2/\deg f} Q(f)$ where
$Q(f) = \int_{-\infty}^{\infty} dx/(f(x)^2)^{1/\deg f}$.
Will explain fast $Q(f)$ bounds.

Extremely accurate estimate:
$\#\{(c, d) \in \mathbf{Z} \times \mathbf{Z} : \gcd\{c, d\} = 1,$
$d > 0, |d^{\deg f} f(c/d)| \leq H\}$
$\approx (3/\pi^2)H^{2/\deg f} Q(f)$.

Can verify accuracy of estimate by finding all integer pairs (c, d), i.e., by solving equations

$d^{\deg f} f(c/d) = \pm 1$,
$d^{\deg f} f(c/d) = \pm 2$, ...
$d^{\deg f} f(c/d) = \pm H$.

Slow but convincing.

Another accurate estimate, easier to verify:

$\#\{(c, d) \in \mathbf{Z} \times \mathbf{Z} : \gcd\{c, d\} = 1,$
$d > 0, |d^{\deg f} f(c/d)| \le H,$
d not very large$\}$
$\approx (3/\pi^2) H^{2/\deg f} Q(f)$.

To compute
good approximation to $Q(f)$,
and hence good approximation to
distribution of $d^{\deg f} f(c/d)$:

$\int_{-s}^{s} dx/(f(x)^2)^{1/\deg f}$ is within

$$\left|\binom{-2/\deg f}{n+1}\right| \frac{2s^{1-2e/\deg f}}{3(1-2e/\deg f)4^n}$$

of $$\sum_{i\in\{0,2,4,\ldots\}} 2q_i \frac{s^{i+1-2e/\deg f}}{i+1-2e/\deg f}$$

if $f(x) = x^e(1+\cdots)$ in $\mathbf{R}[[x]]$,
$|\cdots| \le 1/4$ for $x \in [-s, s]$,
$\sum_{0\le j\le n} \binom{-2/\deg f}{j} (\cdots)^j = \sum q_i x^i$.

Handle constant factors in f.
Handle intervals $[v - s, v + s]$.

Partition $(-\infty, \infty)$:
one interval around each
real root of f; one interval
around ∞, reversing f;
more intervals with $e = 0$.
Be careful with roundoff error.

This is not the end of the story:
can handle some f's more quickly
by arithmetic-geometric mean.

How to find good polynomials?

Many f's possible for n.
How to find f that
minimizes number-field-sieve time?

General strategy:
Enumerate many f's.
For each f, estimate time using
information about f arithmetic,
distribution of $d^{\deg f} f(c/d)$,
distribution of smooth numbers.

Let's restrict attention to $f(x) = (x - m)(f_5 x^5 + f_4 x^4 + \cdots + f_0)$.

Take m near $n^{1/6}$.
Expand n in base m:
$n = f_5 m^5 + f_4 m^4 + \cdots + f_0$.
Can use negative coefficients.

Have $f_5 \approx n^{1/6}$.
Typically all the f_i's
are on scale of $n^{1/6}$.

(1993 Buhler Lenstra Pomerance)

To reduce f values by factor B:

Enumerate many possibilities
for m near $B^{0.25}n^{1/6}$.

Have $f_5 \approx B^{-1.25}n^{1/6}$.
f_4, f_3, f_2, f_1, f_0 could be
as large as $B^{0.25}n^{1/6}$.
Hope that they are smaller,
on scale of $B^{-1.25}n^{1/6}$.

Conjecturally this happens
within roughly $B^{7.5}$ trials.
Then $(c - dm)(f_5c^5 + \cdots + f_0d^5)$
is on scale of $B^{-1}R^6n^{2/6}$
for c, d on scale of R.

Can force f_4 to be small.

Say $n = f_5 m^5 + f_4 m^4 + \cdots + f_0$.

Choose integer $k \approx f_4/5f_5$.
Write n in base $m + k$:

$$n = f_5(m+k)^5 + (f_4 - 5kf_5)(m+k)^4 + \cdots.$$

Now degree-4 coefficient
is on same scale as f_5.

Hope for small f_3, f_2, f_1, f_0.
Conjecturally this happens
within roughly B^6 trials.

Improvement: Skew the coefficients.
(1999 Murphy, without analysis)

Enumerate many possibilities
for m near $Bn^{1/6}$.

Have $f_5 \approx B^{-5} n^{1/6}$.
f_4, f_3, f_2, f_1, f_0 could be
as large as $Bn^{1/6}$.

Force small f_4. Hope for
f_3 on scale of $B^{-2} n^{1/6}$,
f_2 on scale of $B^{-0.5} n^{1/6}$.

Conjecturally this happens
within roughly $B^{4.5}$ trials:
$(2+1)+(0.5+1)=4.5$.

For c on scale of $B^{0.75}R$
and d on scale of $B^{-0.75}R$
have $c-md$ on scale of $B^{0.25}Rn^{1/6}$
and $f_5c^5+f_4c^4d+\cdots+f_0d^5$
on scale of $B^{-1.25}R^5n^{1/6}$.

Product $B^{-1}R^6n^{2/6}$.

Similar effect of B on $Q(f)$;
can afford to compute Q
for many attractive f's.

Can we do better? Yes!

Algorithm 2 of this talk:
only about $B^{3.5}$ trials,
conjecturally.

Each trial is fairly expensive,
using four-dimensional
integer-relation finding,
but worthwhile for large B.

This is so fast that
we should start searching
$(m_2 x - m_1)(c_5 x^5 + c_4 x^4 + \cdots + c_0)$.

Say $n = f_5 m^5 + f_4 m^4 + \cdots + f_0$.

Choose integer $k \approx f_4/5f_5$
and integer $\ell \approx m/5f_5$.

Find all short vectors
in lattice generated by
$(m/B^3, 0, 0, 10f_5k^2 - 4f_4k + f_3)$,
$(0, m/B^4, 0, 20f_5k\ell - 4f_4\ell)$,
$(0, 0, m/B^5, 10f_5\ell^2)$,
$(0, 0, 0 \qquad\quad , m)$.

Hope for j below B^1
with $(10f_5k^2 - 4f_4k + f_3)$
$+ (20f_5k\ell - 4f_4\ell)j$
$+ (10f_5\ell^2)j^2$
below m/B^3 modulo m.

Write n in base $m + k + j\ell$.
Obtain degree-5 coefficient
on scale of $B^{-5}n^{1/6}$;
degree-4 coefficient
on scale of $B^{-4}n^{1/6}$;
degree-3 coefficient
on scale of $B^{-2}n^{1/6}$.
Hope for good degree 2.

How to recognize smooth numbers?

Sieve $d^{\deg f} f(c/d)$
to find primes $\le y^\theta$;
say time S per pair (c, d).

Keep pairs (c, d) with small
unfactored parts of $d^{\deg f} f(c/d)$.

Use second test to find primes $\le y$;
say time T per pair (c, d).

Total time with tests balanced:
roughly $RS^\theta T^{1-\theta}$
where R is smoothness ratio.
(1982 Pomerance)

How to do second test?

Elliptic-curve method conjecturally finds primes $\le y$ in time $\exp((\lg y)^{1/2+o(1)})$ per input bit. (1987 Lenstra)

Faster batch algorithm: time $\exp((3 + o(1)) \log \lg y)$ per bit. (2000 Bernstein)

Variant: $\exp((2 + o(1)) \log \lg y)$ per bit, conjecturally. (2004 Franke Kleinjung Morain Wirth, in ECPP context)

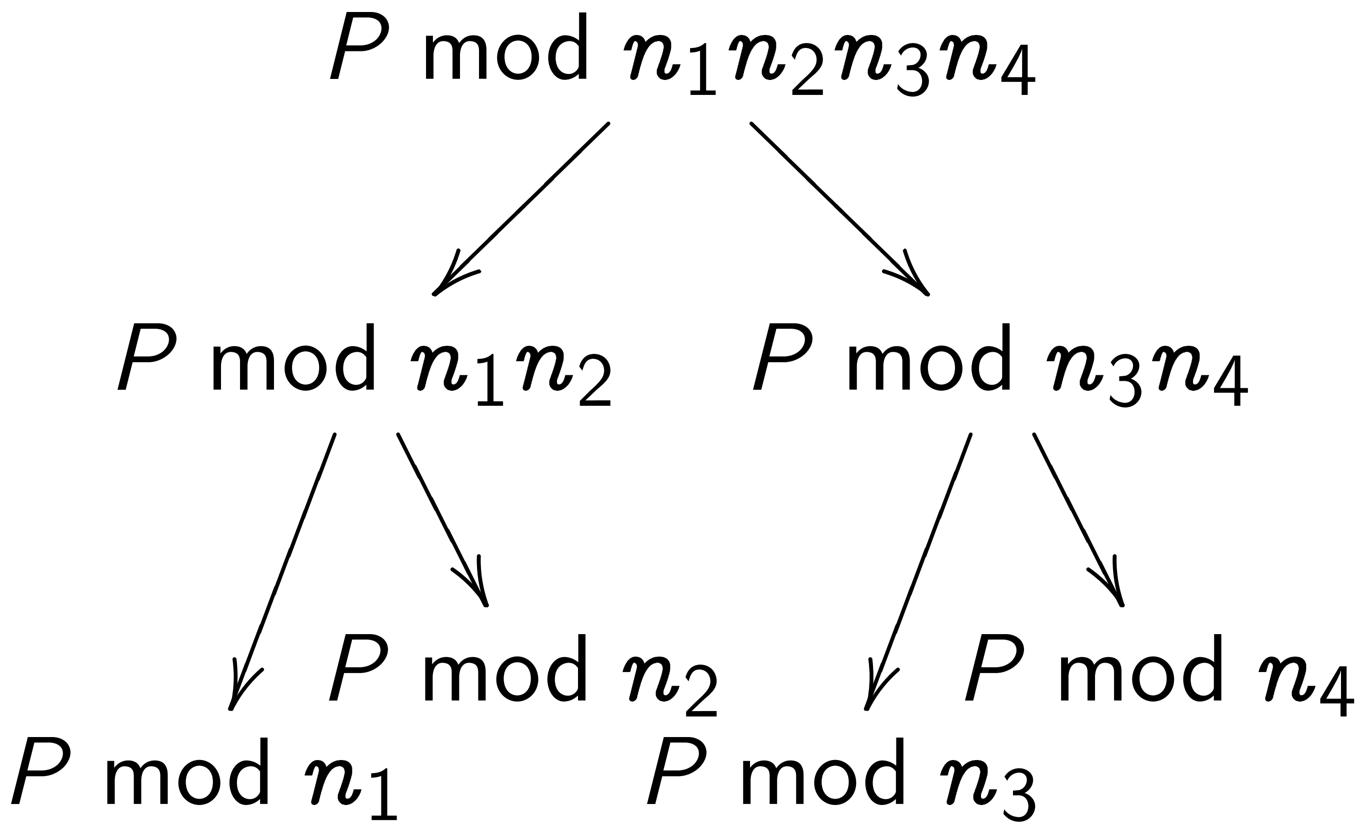
Slightly faster variant
(2004 Bernstein):

Compute product P of the primes.
Compute $P \bmod n_1, P \bmod n_2, \ldots$.
Now n_j is smooth if and only if
$((P \bmod n_j)^{\text{big}}) \bmod n_j = 0$.

Use the $\exp((3 + o(1)) \log \lg y)$
algorithm to factor the smooths;
conjecturally not a bottleneck.

Let's focus on time-consuming step:
compute $P \bmod n_1, P \bmod n_2, \ldots$.

Traditionally use **remainder tree** (1972 Fiduccia, 1972 Moenck Borodin):



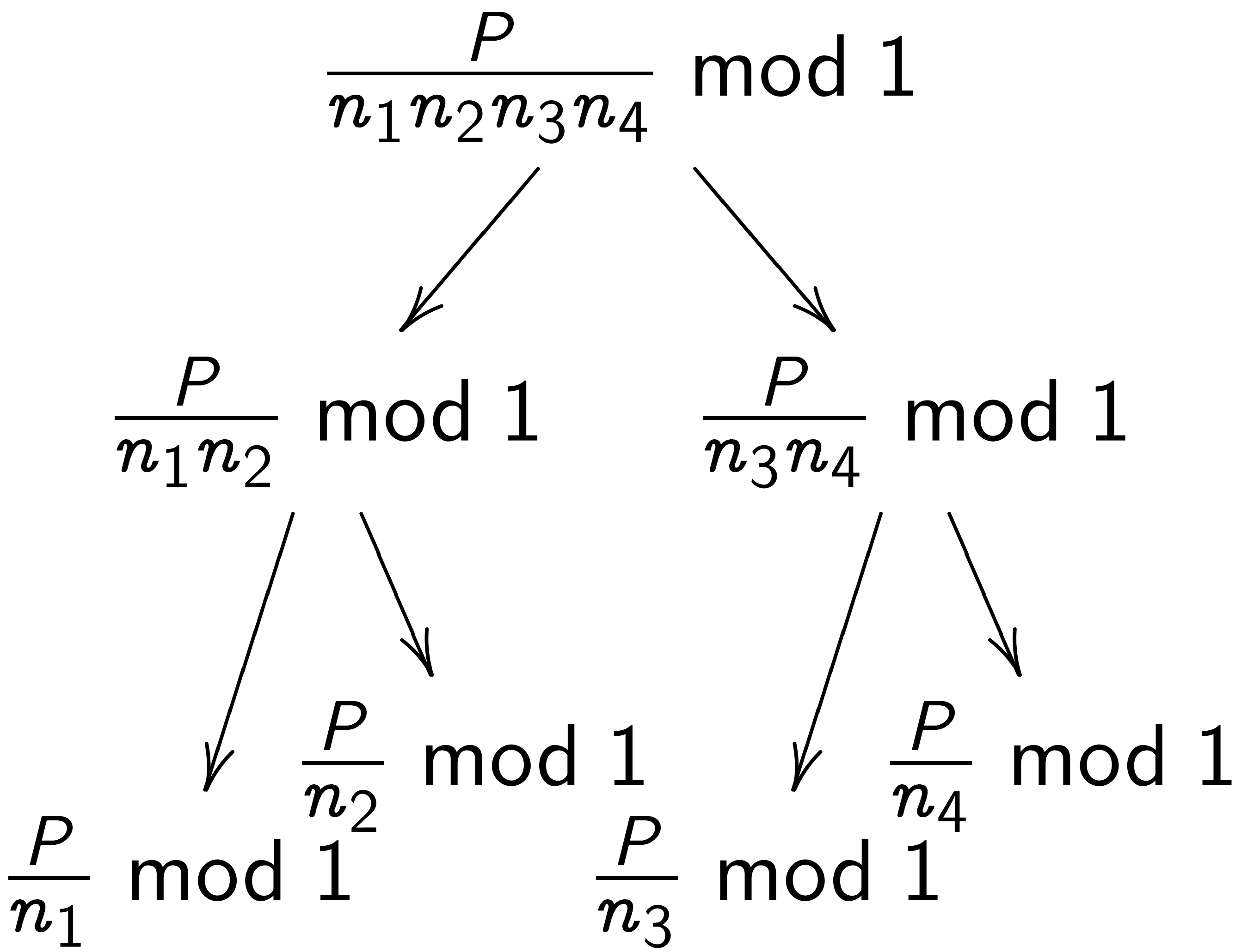
Represent each $P \bmod \cdots$ as a bit string in base 2: $b_0, b_1, \ldots$ represents $b_0 + 2b_1 + \cdots$.

Algorithm 3 of this talk:
use a different structure,
replacing almost all of the
divisions with multiplications.
Constant-factor speedup.

(speedup in function-field case,
using polynomial reversal etc.:
2003 Bostan Lecerf Schost;
structure: 2004 Bernstein)

With redundancies eliminated
(1992 Montgomery, 2004 Kramer):
new structure is $2.6 + o(1)$
times faster than remainder tree.

Scaled remainder tree:



Represent each $P/\cdots \bmod 1$ as a nearby real number in base 2: $b_{-1}, b_{-2}, \ldots$ represents $2^{-1}b_{-1} + 2^{-2}b_{-2} + \cdots$.

e.g. Scaled remainder tree for $P = 8675309$, $n_1 = 10$, $n_2 = 20$, $n_3 = 30$, $n_4 = 40$: