The algorithm of Hastad, Vallée, Girault, Toffin, Coppersmith, Guruswami, Goldreich, Ron, Sudan, Durfee, Howgrave-Graham, and Boneh

D. J. Bernstein
University of Illinois at Chicago

Input to the algorithm

$d \in \mathbf{Z}$, $d \geq 1$;

$f \in \mathbf{Q}[x]$, $\deg f = d$, $f_d > 0$;

$H \in \mathbf{Z}$, $H \geq 1$;

$k \in \mathbf{Z}$, $k \geq 1$;

$m \in \mathbf{Z}$, $m \geq dk$.

Simple case: $k = 1$, $m = 2d$.

Goal of the algorithm

Would like to find all $r \in \mathbf{Q}$ such that $f(r)$ has small height.

Algorithm finds all $r \in \mathbf{Z}$ such that $|r| \leq H$ and $\gcd\{1, f(r)\}/f_d > G$.

Here $\log\log G \approx \frac{1}{2}(\log\log(1/f_d) + \log\log((2H)^d))$.

The algorithm

Define $L \subset \mathbf{Q}[x]$ as

$$\mathbf{Z} + \mathbf{Z}x + \mathbf{Z}x^2 \cdots + \mathbf{Z}x^{d-1}$$
$$+ \mathbf{Z}f + \cdots + \mathbf{Z}x^{d-1}f$$
$$+ \mathbf{Z}f^2 + \cdots + \mathbf{Z}x^{d-1}f^2$$
$$+ \cdots$$
$$+ \mathbf{Z}f^{k-1} + \cdots + \mathbf{Z}x^{d-1}f^{k-1}$$
$$+ \mathbf{Z}f^k + \cdots + \mathbf{Z}x^{m-dk-1}f^k.$$

Define $|\varphi| = \sqrt{\sum_i (H^i \varphi_i)^2}$.

L is a rank-m lattice under metric $\varphi \mapsto |\varphi|$.

$\det L = H^{\frac{1}{2}m(m-1)} f_d^{km - \frac{1}{2}dk(k+1)}$.

Use LLL to find nonzero $\varphi \in L$ with $|\varphi| \le 2^{(m-1)/2} (\det L)^{1/m}$.

Print all rational roots of φ.

Speed of the algorithm

Tolerable.

$\varphi(r) = 0$ if $r \in \mathbf{Z}$, $|r| \leq H$, and $\gcd\{1, f(r)\}/f_d > G$.

Here $G = m^{1/2k}(2H)^{(m-1)/2k} f_d^{-d(k+1)/2m}$.

Proof: $|\varphi(r)| \leq m^{1/2} |\varphi|$
$\leq m^{1/2} 2^{(m-1)/2} (\det L)^{1/m}$
$= G^k f_d^k < \gcd\{1, f(r)\}^k$;
but $\varphi(r) \in \gcd\{1, f(r)\}^k \mathbf{Z}$.

Good choice of m

Assume $1/f_d \geq (2H)^d$.
Take $m = \lceil \alpha d(k+1) \rceil$ where
$\alpha = \sqrt{\log(1/f_d)/\log((2H)^d)}$.

Then $G \leq m^{1/2k}(2H)^{\alpha d(1+1/2k)}$.

So $\varphi(r) = 0$ if $r \in \mathbf{Z}$, $|r| \leq H$,
and $\gcd\{1, f(r)\}/f_d >$
$m^{1/2k}(2H)^{\alpha d(1+1/2k)}$.

Application: roots mod n

$$f = \frac{(x+31415926000)^3 - 35083765367852945}{38785285061353277}$$

$d = 3$, $H = 500$, $k = 1$, $m = 5$.

$L = \mathbf{Z} + \mathbf{Z}x + \mathbf{Z}x^2 + \mathbf{Z}f + \mathbf{Z}xf$.

$G < 20076370177628953 < 1/f_d$.

Find $\varphi \in L$ with $38785285061353277\varphi = 250x^4 + 4480597x^3 - 3789099173x^2 + 1135485860787x - 172139635662493$.

Integer roots of φ: 467.

$$f(467) = \frac{31006276476301184532318266236618}{38785285061353277} = 799434023167634.$$

Given $n \ge 1$, $H \ge 1$, $d \ge 1$,
$p \in \mathbf{Z}[x]$, $\deg p = d$, $p_d = 1$:

Can apply algorithm
with $f = p/n$, $k = 1$, $m = d + 1$
to find all $r \in \mathbf{Z}$ with
$|r| \le H$ and $p(r) \in n\mathbf{Z}$,
if $H < n^{2/d(d+1)}/2(d+1)^{1/d}$.

(Hastad 1985; complicated dual:
Vallée, Girault, Toffin 1988)

Can apply algorithm
with $f = p/n$, $k \geq 1$, $m = dk + d$
to find all $r \in \mathbf{Z}$ with
$|r| \leq H$ and $p(r) \in n\mathbf{Z}$,
if $H < n^{k/(m-1)}/2m^{1/(m-1)}$.

(dual: Coppersmith 1996;
Howgrave-Graham 1997)

Application: high-power factors

$$f = \frac{(4349000 + x)^2}{1038397528952788140203}$$

$d = 2$, $H = 500$, $k = 2$, $m = 9$.

$L = \mathbf{Z} + \mathbf{Z}x + \mathbf{Z}f + \mathbf{Z}xf + \mathbf{Z}f^2$
$+ \mathbf{Z}xf^2 + \mathbf{Z}x^2f^2 + \mathbf{Z}x^3f^2 + \mathbf{Z}x^4f^2$.

$G < 4348500^2$.

Find small $\varphi \in L$.

Integer roots of φ: 353.

$f(353) = 1/54892667$.

Try to factor integers this way.

Sometimes faster than ECM.

(Boneh, Durfee,
Howgrave-Graham 1999)

Application: CRT with errors

$$f = \frac{x - 18001400090020646934}{91560016674010125\,67}$$

$d = 1$, $H = 5000$, $k = 1$, $m = 3$.

$L = \mathbf{Z} + \mathbf{Z}f + \mathbf{Z}xf$.

$f(3277) = -8675309/44124979$.

$915600166740101256 7 =$

$11 \cdot 13 \cdot 17 \cdot \cdots \cdot 59.$

3277 mod $11, 13, 17, \ldots, 59$:

$10, 1, 13, 9, 11, 0, 22,$

$21, 38, 9, 34, 44, 32.$

18001400900206469 34 mod $\ldots$:

$10, 1, 4, 9, 11, 28, 22,$

$4, 14, 9, 34, 44, 29.$

Given $H \geq 1$, $n \geq 2H$, $u \in \mathbf{Z}$:

Write $\alpha = \sqrt{\log(n)/\log(2H)}$.
Can apply algorithm with
$f = (x - u)/n$, $k \geq 1$,
$m = \lceil \alpha(k+1) \rceil$ to find all $r \in \mathbf{Z}$
with $|r| \leq H$ and $\gcd\{n, r - u\} >$
$m^{1/2k}(2H)^{\alpha(1+1/2k)}$.

(Boneh 2000;
dual with slightly worse result:
Goldreich, Ron, Sudan 1998)

Similarly for function fields.

(Guruswami, Sudan 1999;
slightly worse result: Sudan 1997)

Application: smoothness

$50!f = x^2 + 6563806563806000x$
$+ 14289695657685151430824671$

$d = 2,\ H = 1000,\ k = 2,\ m = 15.$

$50!f(823) =$
$2^{15}3^{10}5^{4}11^{3}13^{1}19^{2}29^{1}37^{1}41^{1}43^{1}.$

(Boneh 2000)