Polynomial selection for the number-field sieve, part 2: polynomial merit

D. J. Bernstein

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

"Degree $1 + 5$ monic" NFS
tries to factor n
using an auxiliary polynomial
$(x - m)(x^5 + f_4 x^4 + \cdots + f_0)$
with $n = m^5 + f_4 m^4 + \cdots + f_0$.

(Various generalizations:
$m_1 x - m_0$; $f_5 x^5$; et al.)

NFS succeeds for practically
all choices of polynomials.
NFS speed depends heavily
on choice of polynomial.

on

ld sieve,

l merit

is at Chicago

42

oundation

"Degree $1 + 5$ monic" NFS
tries to factor n
using an auxiliary polynomial
$(x - m)(x^5 + f_4 x^4 + \cdots + f_0)$
with $n = m^5 + f_4 m^4 + \cdots + f_0$.

(Various generalizations:
$m_1 x - m_0$; $f_5 x^5$; et al.)

NFS succeeds for practically
all choices of polynomials.
NFS speed depends heavily
on choice of polynomial.

How NFS uses a p

Given $m, f_4, \ldots, f$

For each small irre
consider image of
$\mathbf{Z}[x]/(x - m) \simeq \mathbf{Z}$
and image of g in
$\mathbf{Z}[x]/(x^5 + f_4 x^4 +$

Factor some of the
e.g., the 2^{40}-smoo

Use factorizations
interesting multipl

“Degree $1+5$ monic” NFS
tries to factor n
using an auxiliary polynomial
$(x-m)(x^5+f_4x^4+\cdots+f_0)$
with $n=m^5+f_4m^4+\cdots+f_0$.

(Various generalizations:
m_1x-m_0; f_5x^5; et al.)

NFS succeeds for practically
all choices of polynomials.
NFS speed depends heavily
on choice of polynomial.

<u>How NFS uses a polynomial</u>

Given $m, f_4, \ldots, f_0$:

For each small irred $g \in \mathbf{Z}[x]$,
consider image of g in
$\mathbf{Z}[x]/(x-m) \simeq \mathbf{Z}$,
and image of g in
$\mathbf{Z}[x]/(x^5+f_4x^4+\cdots+f_0)$.

Factor some of these images:
e.g., the 2^{40}-smooth images.

Use factorizations to find
interesting multiplicative relations.

nic" NFS

polynomial

${}^4 + \cdots + f_0)$

$m^4 + \cdots + f_0$.

ations:

et al.)

practically

nomials.

ds heavily

omial.

<u>How NFS uses a polynomial</u>

Given $m, f_4, \ldots, f_0$:

For each small irred $g \in \mathbf{Z}[x]$,
consider image of g in
$\mathbf{Z}[x]/(x - m) \simeq \mathbf{Z}$,
and image of g in
$\mathbf{Z}[x]/(x^5 + f_4 x^4 + \cdots + f_0)$.

Factor some of these images:
e.g., the 2^{40}-smooth images.

Use factorizations to find
interesting multiplicative relations.

What is a "small"

Traditional definiti
$a - bx$ with $1 \leq a$

Much better defini
$a - bx$ with $1 \leq a$
$|(a - bm)(a^5 + \cdot$

Smaller product of
as measured by no
$(a - bm)(a^5 + \cdots$
is more likely to be

Is $a - bx + cx^2$ us
But this talk will f

How NFS uses a polynomial

Given $m, f_4, \ldots, f_0$:

For each small irred $g \in \mathbf{Z}[x]$, consider image of g in $\mathbf{Z}[x]/(x - m) \simeq \mathbf{Z}$, and image of g in $\mathbf{Z}[x]/(x^5 + f_4 x^4 + \cdots + f_0)$.

Factor some of these images: e.g., the 2^{40}-smooth images.

Use factorizations to find interesting multiplicative relations.

What is a "small" g?

Traditional definition: e.g., $a - bx$ with $1 \le a \le 2^{30}$, $|b| \le 2^{30}$.

Much better definition: e.g., $a - bx$ with $1 \le a \le 2^{40}$, $|b| \le 2^{40}$, $\left|(a - bm)(a^5 + \cdots + f_0 b^5)\right| \le 2^{300}$.

Smaller product of g images, as measured by norm $(a - bm)(a^5 + \cdots + f_0 b^5)$, is more likely to be factored.

Is $a - bx + cx^2$ useful? Maybe! But this talk will focus on $a - bx$.

polynomial

f_0:

ed $g \in \mathbf{Z}[x]$,
g in
$\mathbf{Z}$,

$\cdots + f_0)$.

ese images:
th images.

to find
icative relations.

What is a "small" g?

Traditional definition: e.g.,
$a - bx$ with $1 \le a \le 2^{30}$, $|b| \le 2^{30}$.

Much better definition: e.g.,
$a - bx$ with $1 \le a \le 2^{40}$, $|b| \le 2^{40}$,
$\left|(a - bm)(a^5 + \cdots + f_0 b^5)\right| \le 2^{300}$.

Smaller product of g images,
as measured by norm
$(a - bm)(a^5 + \cdots + f_0 b^5)$,
is more likely to be factored.

Is $a - bx + cx^2$ useful? Maybe!
But this talk will focus on $a - bx$.

Polynomial merit

Given m, $f_4, \ldots, f$

How many irreds c
$\left|(a - bm)(a^5 + \cdots\right.$
How many $\le H$ ar

Want fast, accurat

Analytic number t
crude asymptotic
Want something n

What is a "small" g?

Traditional definition: e.g.,
$a - bx$ with $1 \le a \le 2^{30}$, $|b| \le 2^{30}$.

Much better definition: e.g.,
$a - bx$ with $1 \le a \le 2^{40}$, $|b| \le 2^{40}$,
$\left|(a - bm)(a^5 + \cdots + f_0 b^5)\right| \le 2^{300}$.

Smaller product of g images,
as measured by norm
$(a - bm)(a^5 + \cdots + f_0 b^5)$,
is more likely to be factored.

Is $a - bx + cx^2$ useful? Maybe!
But this talk will focus on $a - bx$.

Polynomial merit

Given $m, f_4, \ldots, f_0, H, y$:

How many irreds $a - bx \in \mathbf{Z}[x]$ have
$\left|(a - bm)(a^5 + \cdots + f_0 b^5)\right| \le H$?
How many $\le H$ and y-smooth?

Want fast, accurate estimates.

Analytic number theory gives
crude asymptotic conjectures.
Want something more explicit.

g?

on: e.g.,

$\leq 2^{30}$, $|b| \leq 2^{30}$.

ition: e.g.,

$\leq 2^{40}$, $|b| \leq 2^{40}$,

$\cdot + f_0 b^5)\big| \leq 2^{300}$.

f g images,

rm

$+ f_0 b^5)$,

e factored.

seful? Maybe!

focus on $a - bx$.

Polynomial merit

Given $m, f_4, \ldots, f_0, H, y$:

How many irreds $a - bx \in \mathbf{Z}[x]$ have $\big|(a - bm)(a^5 + \cdots + f_0 b^5)\big| \leq H$?

How many $\leq H$ and y-smooth?

Want fast, accurate estimates.

Analytic number theory gives crude asymptotic conjectures.

Want something more explicit.

Use answers to est

total time for NFS

Given n,

consider many pol

and select polynon

smallest (estimated

Trying all possible

becomes a bottlen

as n increases.

Use faster estimat

"want small coeffi

as preliminary filte

Polynomial merit

Given m, $f_4, \ldots, f_0$, H, y:

How many irreds $a - bx \in \mathbf{Z}[x]$ have $\left|(a - bm)(a^5 + \cdots + f_0 b^5)\right| \le H$?
How many $\le H$ and y-smooth?

Want fast, accurate estimates.

Analytic number theory gives crude asymptotic conjectures.
Want something more explicit.

Use answers to estimate total time for NFS.

Given n,
consider many polynomials and select polynomial with smallest (estimated) NFS time.

Trying all possible polynomials becomes a bottleneck as n increases.
Use faster estimates (e.g., "want small coefficient sum") as preliminary filters.

f_0, H, y:

$a - bx \in \mathbf{Z}[x]$ have
$\cdots + f_0 b^5)\big| \le H$?
nd y-smooth?

te estimates.

heory gives
conjectures.
more explicit.

Use answers to estimate
total time for NFS.

Given n,
consider many polynomials
and select polynomial with
smallest (estimated) NFS time.

Trying all possible polynomials
becomes a bottleneck
as n increases.
Use faster estimates (e.g.,
"want small coefficient sum")
as preliminary filters.

Number of $a - bx$
with $a > 0$, gcd$\{a$
$(a - bm)(a^5 + \cdots$
is extremely close
$(3/\pi^2) H^{2/6} \int_{-\infty}^{\infty} d$
where
$f(x) = (x - m)(x$

Evaluate superellip
by standard techni
partition, use serie
Not much slower t

Use answers to estimate total time for NFS.

Given n, consider many polynomials and select polynomial with smallest (estimated) NFS time.

Trying all possible polynomials becomes a bottleneck as n increases. Use faster estimates (e.g., "want small coefficient sum") as preliminary filters.

Number of $a - bx \in \mathbf{Z}[x]$ with $a > 0$, $\gcd\{a, b\} = 1$, $(a - bm)(a^5 + \cdots + f_0 b^5) \in [-H, H]$ is extremely close to $(3/\pi^2) H^{2/6} \int_{-\infty}^{\infty} dx/(f(x)^2)^{1/6}$ where $f(x) = (x - m)(x^5 + \cdots + f_0)$.

Evaluate superelliptic integral by standard techniques: partition, use series expansions. Not much slower than AGM etc.

timate
5.

ynomials
mial with
d) NFS time.

polynomials
eck

es (e.g.,
cient sum")
ers.

Number of $a - bx \in \mathbf{Z}[x]$
with $a > 0$, $\gcd\{a, b\} = 1$,
$(a - bm)(a^5 + \cdots + f_0 b^5) \in [-H, H]$
is extremely close to
$(3/\pi^2) H^{2/6} \int_{-\infty}^{\infty} dx/(f(x)^2)^{1/6}$
where
$f(x) = (x - m)(x^5 + \cdots + f_0)$.

Evaluate superelliptic integral
by standard techniques:
partition, use series expansions.
Not much slower than AGM etc.

What is smoothne
$(a - bm)(a^5 + \cdots$

Can estimate accu
by sampling rando
but this takes tim
comparable to 1/c

Faster: Image of r
$\mathbf{Z}[x]/(x - m) \times \mathbf{Z}$
has similar smooth
random ideal with
distribution at ∞.

Number of $a - bx \in \mathbf{Z}[x]$
with $a > 0$, $\gcd\{a, b\} = 1$,
$(a - bm)(a^5 + \cdots + f_0 b^5) \in [-H, H]$
is extremely close to
$(3/\pi^2) H^{2/6} \int_{-\infty}^{\infty} dx/(f(x)^2)^{1/6}$
where
$f(x) = (x - m)(x^5 + \cdots + f_0)$.

Evaluate superelliptic integral
by standard techniques:
partition, use series expansions.
Not much slower than AGM etc.

What is smoothness chance of
$(a - bm)(a^5 + \cdots + f_0 b^5)$?

Can estimate accurately
by sampling random $a - bx$,
but this takes time
comparable to 1/chance.

Faster: Image of random $a - bx$ in
$\mathbf{Z}[x]/(x - m) \times \mathbf{Z}[x]/(x^5 + \cdots)$
has similar smoothness chance to
random ideal with same
distribution at ∞.

$\in \mathbf{Z}[x]$

$, b\} = 1,$

$+ f_0 b^5) \in [-H, H]$

to

$dx/(f(x)^2)^{1/6}$

$x^5 + \cdots + f_0).$

otic integral

iques:

es expansions.

than AGM etc.

What is smoothness chance of $(a - bm)(a^5 + \cdots + f_0 b^5)$?

Can estimate accurately by sampling random $a - bx$, but this takes time comparable to $1/$chance.

Faster: Image of random $a - bx$ in $\mathbf{Z}[x]/(x - m) \times \mathbf{Z}[x]/(x^5 + \cdots)$ has similar smoothness chance to random ideal with same distribution at ∞.

Enumerate small p

write down Dirichl

for smooth ideals.

Replace $2, 3, 5, 7, 1$

slightly larger real

$\overline{2} = 1.1^8$, $\overline{3} = 1.1^1$

to convert Dirichle

into power series.

Compute $(\log H)/$

of this power serie

to see $\approx$ distributi

smooth ideals.

What is smoothness chance of $(a - bm)(a^5 + \cdots + f_0 b^5)$?

Can estimate accurately by sampling random $a - bx$, but this takes time comparable to $1/\text{chance}$.

Faster: Image of random $a - bx$ in $\mathbf{Z}[x]/(x - m) \times \mathbf{Z}[x]/(x^5 + \cdots)$ has similar smoothness chance to random ideal with same distribution at ∞.

Enumerate small prime ideals to write down Dirichlet series for smooth ideals.

Replace $2, 3, 5, 7, 11, \ldots$ with slightly larger real numbers $\overline{2} = 1.1^8$, $\overline{3} = 1.1^{12}$, $\overline{5} = 1.1^{17}$, ... to convert Dirichlet series into power series.

Compute $(\log H)/(\log 1.1)$ coeffs of this power series to see $\approx$ distribution of smooth ideals.

ss chance of

$+ f_0 b^5)$?

rately

m $a - bx$,

e

chance.

andom $a - bx$ in

$[x]/(x^5 + \cdots)$

nness chance to

same

Enumerate small prime ideals to write down Dirichlet series for smooth ideals.

Replace $2, 3, 5, 7, 11, \ldots$ with slightly larger real numbers $\overline{2} = 1.1^8$, $\overline{3} = 1.1^{12}$, $\overline{5} = 1.1^{17}$, $\ldots$ to convert Dirichlet series into power series.

Compute $(\log H)/(\log 1.1)$ coeffs of this power series to see $\approx$ distribution of smooth ideals.

Can adapt metho

e.g., 2^{30}-smooth b

times one prime in

Can work with ser

$\mathbf{Z}$[class group]

to separate ideal c

but not worthwhil

all classes end up

same distribution.

Enumerate small prime ideals to write down Dirichlet series for smooth ideals.

Replace $2, 3, 5, 7, 11, \ldots$ with slightly larger real numbers $\overline{2} = 1.1^8$, $\overline{3} = 1.1^{12}$, $\overline{5} = 1.1^{17}$, $\ldots$ to convert Dirichlet series into power series.

Compute $(\log H)/(\log 1.1)$ coeffs of this power series to see $\approx$ distribution of smooth ideals.

Can adapt method to handle, e.g., 2^{30}-smooth below 2^{300} times one prime in $[2^{30}, 2^{40}]$.

Can work with series over $\mathbf{Z}$[class group] to separate ideal classes, but not worthwhile: all classes end up with same distribution.