Doubly focused enumeration of locally square polynomial values

D. J. Bernstein

Thanks to:
University of Illinois at Chicago
NSF DMS–0140542
Alfred P. Sloan Foundation
Math Sciences Research Institute
University of California at Berkeley

If x is a positive integer and $x^2 - 314159265358979323$ is square then $x \geq 560499122$;
$x \bmod 4 \in \{2\}$;
$x \bmod 9 \in \{2, 7\}$;
$x \bmod 5 \in \{2, 3\}$;
$x \bmod 7 \in \{0, 2, 5\}$;
$x \bmod 11 \in \{0, 1, 3, 8, 10\}$;
$x \bmod 13 \in \{0, 1, 3, 6, 7, 10, 12\}$;
etc.

How to find such x's?

Unfocused enumeration

For each successive x,
check x mod 4, x mod 9, etc.

560499122: 4 9 5 ~~7~~
560499123: ~~4~~
560499124: ~~4~~
560499125: ~~4~~
560499126: 4 ~~9~~
$\vdots$

Each test weeds out $\approx$ 50%
of the remaining x's.

For each modulus m,
precompute m-bit table for
$x \bmod m \mapsto [x$ works modulo $m]$.

Merge primes into larger moduli,
at the expense of memory.

Handle 32 or 64 successive x's
using a few word operations.

(Hardware optimization: different.)

Focused enumeration

Focus on $x \in 2 + 4\mathbf{Z}$:

560499122: 9 5 ~~7~~

560499126: ~~9~~

560499130: ~~9~~

560499134: ~~9~~

560499138: ~~9~~

560499142: ~~9~~

560499146: ~~9~~

560499150: ~~9~~

560499154: 9 ~~5~~

$\vdots$

$4\times$ speedup.

Even better, focus on
$x \in 2 + 36\mathbf{Z}$, $x \in 34 + 36\mathbf{Z}$.
$18\times$ speedup.

Even better, focus on
$x \in 2 + 180\mathbf{Z}$, $x \in 38 + 180\mathbf{Z}$,
$x \in 142 + 180\mathbf{Z}$, $x \in 178 + 180\mathbf{Z}$.
$45\times$ speedup.

Keep going. How far?

Using all primes $p \le y$:

Identify arithmetic progressions modulo $\prod p \approx e^y$.

Time $\approx \dfrac{H + e^y}{2^{y/\log y}}$
to handle H successive x's.

Optimum: $y \approx \log H$.
Speedup factor $\approx H^{1/\lg \log H}$.

Doubly focused enumeration

Write x as $x_1 - x_2$ where
x_1 is a multiple of $4 \cdot 9 \cdot 11$;
$0 \le x_2 < 4 \cdot 5 \cdot 7 \cdot 9 \cdot 11 \cdot 13$;
x_2 is a multiple of $5 \cdot 7 \cdot 13$.

x works modulo $4, 5, 7, 9, 11, 13$
if and only if
x_1 works modulo $5, 7, 13$ and
$-x_2$ works modulo $4, 9, 11$.

Possibilities for $x_1 - 560499122$:

$466, 14326, 19870, 20266, 25810, 28186, 53530, 55906, 61450, 61846, 67390, 81250, 89566, 95110, \ldots$.

Possibilities for x_2:

$6370, 10010, 26390, 39130, 59150, 121030, 141050, 153790, \ldots$.

If $0 \le x - 560499122 \le 3000$

then

$x_2 \le x_1 - 560499122 \le x_2 + 3000$.

Merge sorted lists

to discover these coincidences:

$(28186, 26390)$,

$(61450, 59150)$,

$(61846, 59150)$, etc.

Using all primes $p \le y$,
split between x_1 and x_2:

Time $\approx \dfrac{H}{2^{y/\log y}} + e^{y/2}$
to handle H successive x's.

Optimum: $y \approx 2 \log H$.
Speedup factor $\approx H^{2/\lg \log H}$.

More applications

Search for square values of
$x^3 + 1^7$, $x^3 + 2^7$, etc.

$4562214641070025 7^3 + 892^7$
is locally square
at all primes below 300.

No positive non-square $x \leq 24 \cdot 2^{64}$ is locally square at all primes ≤ 283. (Bernstein 2001)

Useful for, inter alia, proving primality of small numbers.

(Reasonable conjecture:
No $x \leq 2^{y/\log y}$ for primes $\leq y$.
Gives deterministic primality test taking essentially cubic time.)

No positive non-square $x \le 120 \cdot 2^{64}$ is locally square at all primes ≤ 331.

214220286037026991612 9

is locally square (and unit) at all primes ≤ 317.

(Williams, Wooding 2003)