Doubly focused enumeration in two dimensions

D. J. Bernstein

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

A taste of computational geometry

Fix $d \in \{1, 2, 3, \ldots\}$.

The near-neighbor problem:
Given $R \in \mathbf{Z}$,
$u_1, u_2, \ldots, u_m \in \mathbf{Z}^d$, and
$v_1, v_2, \ldots, v_n \in \mathbf{Z}^d$,
find all pairs (i, j)
such that $\left|u_i - v_j\right|^2 \le R$.

Several standard solutions.
(1975 Bentley, et al.;
usually stated for $u = v$)

Sort-and-merge solution for $d = 1$:
Assume $u_1 \le u_2 \le \cdots \le u_m$
and $v_1 \le v_2 \le \cdots \le v_n$.
Tabulate $i \mapsto (\min\{j\}, \max\{j\})$.

Partitioning solution for $d = 1$:
Cover v range with intervals.
For each interval,
enumerate v's in interval,
then u's near interval.

For any d: Cover v range
with boxes. For each box,
enumerate v's in box,
then u's near box.

Proving primality

An integer $n \in [2^{20}, 2^{100}]$ is prime iff

- $r^{(n-1)/2} \equiv \pm 1 \pmod{n}$ for all primes $r \le 367$;
- $r^{(n-1)/2} \equiv -1 \pmod{n}$ for some odd prime $r \le 367$ if $n \bmod 8 = 1$;
- $2^{(n-1)/2} \equiv -1$ if $n \bmod 8 = 5$;
- n is not a perfect power; and
- n has no prime divisors below 2^{20}.

(1996 Lukes Patterson Williams, improving Selfridge Weinberger)

Proof relies on big computation:
each nonsquare in $\{1, \ldots, 2^{80}\}$
is nonsquare at some prime ≤ 367.
(2003 Williams Wooding)

2^{80} is scary but save roughly
2^{10} by focusing (standard);
save 2^{10} more by doubly focusing
(2001 Bernstein); streamline.

Generalize to arbitrary dimensions.
(2004 Bernstein, this talk)

In ring $R = \mathbf{Z}[i]/(i^2+1)$:

$837947981 + 2833822740i$

is a unit square mod $8, 3, 5, 7, 11,$
$13, 17, 29, 37, 41, 53, 61, 73, 89, 97,$
$101, 109, 113, 137, 149, 157, 173,$
$181, 193, 197, 229, 233, 241, 257$
but not a square mod 269.

Have computed all examples in
$\{0, 1, 2, \ldots, 2^{32}-1\}$
$+ \{0, 1, 2, \ldots, 2^{32}-1\}i.$

Computation took $1.3 \cdot 2^{50}$ cycles on an 1800MHz Athlon MP.

Focused enumeration

2^{64} small elements of R.

Focus on 4 possibilities mod 5, namely the unit squares mod 5: $1+5R, -1+5R, 2i+5R, -2i+5R$. $\approx 0.16 \cdot 2^{64}$ elements.

Or 224737099776 possibilities mod $199191720 = 8\cdot 3\cdot 5\cdot 7\cdot 13\cdot 17\cdot 29\cdot 37$. $\approx 0.00000566 \cdot 2^{64}$ elements.

Enumerating possibilities becomes a bottleneck, so limit modulus.

Doubly focused enumeration

Define $m_1 = 8 \cdot 3 \cdot 7 \cdot 13 \cdot 17 \cdot 37 \cdot 53$, $m_2 = 5 \cdot 29 \cdot 41 \cdot 61 \cdot 73$. Choose fundamental domain mod $m_1 m_2$.

Write each element of R
as $u - v$ where
u is a multiple of m_1,
v is a multiple of m_2,
v is in fundamental domain.

$u - v$ is unit square mod $m_1 m_2$
iff u is unit square mod m_2,
$-v$ is unit square mod m_1.

Want near neighbors between $S =$

$\{u : u$ is a multiple of m_1,

u is near fundamental domain,

u is unit square mod $m_2\}$

and $T =$

$\{v : v$ is a multiple of m_2,

v is in fundamental domain,

$-v$ is unit square mod $m_1\}$.

e.g. $837947981 + 2833822740i = u - v$ where

$u = (15960557 + 4504845i)m_1$

$= 1162056361740456 + 327988790798760i$,

$v = (43895735 + 12389412i)m_2$

$= 1162055523792475 + 327985956976020i$.

$m \approx 2^{51}$ where $m = m_1 m_2$.
$\#S \approx 2^{39}$. $\#T \approx 2^{38}$.

I covered fundamental domain
$\{0, \ldots, m-1\} + \{0, \ldots, m-1\}i$
with boxes of size $\approx 2^{34} \times 2^{32}$.
Number of boxes $\approx 2^{36}$.
Number of near neighbors $\approx 2^{39}$.

Also traded memory for time
to generate S and T in lex order.
Used $\approx 2^{31}$ bits of memory
with further split of m_1, m_2.
Bad for mesh computers but
good for conventional computers.

The doubly-focused advantage

Sieve N points for local squares.

Focused enumeration
takes time $N^{1-(1+o(1))/\lg\log N}$.

Doubly focused enumeration
takes time $N^{1-(2+o(1))/\lg\log N}$
on average; conjecturally always.
Allows about twice as many primes.

Speedup factor is roughly 2^{10}
for, e.g., $N \approx 2^{64}$.