“Mathematics is like checkers
in being suitable for the young,
not too difficult, amusing,
and without peril to the state.”

—Plato

Counting rational points by brute force

D. J. Bernstein
University of Illinois at Chicago

NSF DMS–9600083

Elkies, 1988,
"On $A^4 + B^4 + C^4 = D^4$":

$$2682440^4 + 15365639^4 + 18796760^4$$
$$= 20615673^4$$

. . . "seems beyond the range
of reasonable exhaustive
computer search."

All solutions ≤ 21000000 with positive coordinates, mod scaling, permutations:

$$95800^4+217519^4+414560^4=422481^4$$

$$673865^4+1390400^4+2767624^4=2813001^4$$

$$1705575^4+5507880^4+8332208^4=8707481^4$$

$$5870000^4+8282543^4+11289040^4=12197457^4$$

$$4479031^4+12552200^4+14173720^4=16003017^4$$

$$3642840^4+7028600^4+16281009^4=16430513^4$$

$$2682440^4+15365639^4+18796760^4=20615673^4$$

(422481 Frye; 2813001 MacLeod; 20615673 Elkies; others new)

Standard method

To find all solutions $\le H$:

Sort $\{(a^4 + b^4, a, b) : a, b \le H\}$
into increasing order
in the first component.
Also $\{(d^4 - c^4, c, d) : c, d \le H\}$.

Merge the sorted lists,
looking for collisions.

MSD radix sort takes linear time in realistic machine model.

Time: $H^{2+o(1)}$.
Tolerable for large H.

Space: $H^{2+o(1)}$.
Impossible for large H.

Standard improvements

1. Reduce $\#\{(a,b)\}$, $\#\{(c,d)\}$ by carefully choosing representatives for $\{(a,b,c,d)\}$ mod scaling et al.

2. Chop $\mathbf{Z}$ into intervals in $\mathbf{R}$ or $\mathbf{Q}_p$. Enumerate a^4+b^4 and d^4-c^4 in each interval separately.

3. Prove theorems to exclude solutions in some intervals.

Assume $a\mathbf{Z} + b\mathbf{Z} + c\mathbf{Z} + d\mathbf{Z} = \mathbf{Z}$.

Permute a, b, c so that
$a \in 2\mathbf{Z}$ and $b \in 10\mathbf{Z}$.

Then $a \in 8\mathbf{Z}$, $b \in 40\mathbf{Z}$,
$d - 1 \in 8\mathbf{Z}$, $d \notin 5\mathbf{Z}$,
and $c \equiv \pm d \pmod{1024}$.

$\#\{(c, d)\} \approx 10^{-4} H^2$.
Can reduce further with
more p-adic restrictions.

(Morgan Ward, 1948)

Searching without sorting

Factor each $d^4 - c^4$ into primes,
write as sum of two squares
in all possible ways;
check for fourth powers.

No solutions for $H = 10^4$.
(Ward)

Time $H^{2+o(1)}$ with
modern factoring methods,
but still rather slow.

Alternative: For each (c, d),
enumerate possible b's,
see if $d^4 - c^4 - b^4$ is fourth power.

No solutions for $H = 2.2 \cdot 10^5$.
(Lander-Parkin-Selfridge, 1967)

Solutions for $H = 2 \cdot 10^6$.
$\approx 2 \cdot 10^{-6} H^3$ fourth-power tests.
(Frye, 1988)

Sorting without storing

For fixed b, easy to generate $a^4 + b^4$ in increasing order, using very little space.

Run one generator for each b, merge results.

(Lander-Parkin, 1967)

$\underline{2}=1^4+1^4$	$32=2^4+2^4$	$162=3^4+3^4$
$\underline{17}=2^4+1^4$	$32=2^4+2^4$	$162=3^4+3^4$
$82=3^4+1^4$	$\underline{32}=2^4+2^4$	$162=3^4+3^4$
$\underline{82}=3^4+1^4$	$97=3^4+2^4$	$162=3^4+3^4$
$257=4^4+1^4$	$\underline{97}=3^4+2^4$	$162=3^4+3^4$
$257=4^4+1^4$	$272=4^4+2^4$	$\underline{162}=3^4+3^4$
$\underline{257}=4^4+1^4$	$272=4^4+2^4$	$337=4^4+3^4$
$626=5^4+1^4$	$\underline{272}=4^4+2^4$	$337=4^4+3^4$
$626=5^4+1^4$	$641=5^4+2^4$	$\underline{337}=4^4+3^4$
$\underline{626}=5^4+1^4$	$641=5^4+2^4$	$706=5^4+3^4$

. . .

For each of the H^2 outputs,
search for smallest of H results.
Total time: $H^{3+o(1)}$.

Space: H generators.

Heaps

A **heap** is a sequence

$x_1, x_2, \ldots, x_n$ such that

$x_1 \leq x_2$, $x_1 \leq x_3$,

$x_2 \leq x_4$, $x_2 \leq x_5$,

$x_3 \leq x_6$, $x_3 \leq x_7$,

$x_4 \leq x_8$, $x_4 \leq x_9$,

etc.

e.g. $1, 4, 1, 5, 9, 2, 6, 5$

Smallest element of a heap $x_1, x_2, \ldots, x_n$ is x_1.

For any y, easy to permute $y, x_2, x_3, \ldots, x_n$ into a new heap:

1. $j \leftarrow 1$.
2. $k \leftarrow 2j$.
3. Stop if $k > n$.
4. $k \leftarrow k + 1$ if $k < n$, $x_{k+1} < x_k$.
5. Stop if $y \leq x_k$.
6. Swap y (in jth spot) with x_k.
7. $j \leftarrow k$.
8. Go back to step 2.

Use heap in Lander-Parkin method.
Space: H generators.
Time: $H^{2+o(1)}$.

Other data structures allowing fast find-and-replace-smallest: leftist trees, loser selection trees, balanced trees, B-trees, etc.

Heaps are small and very fast.

History

Heaps: J. W. J. Williams, 1964.
Improvements: Floyd, 1964.

Using heaps to enumerate sums in sorted order: W. S. Brown. See exercise in Knuth on multiplying sparse power series.

Speeding up Lander-Parkin: Randy Ekl (balanced trees); independently me (heaps); independently David W. Wilson (heaps).

Limiting precision

Search for solutions to
$(a^4 \bmod m) + (b^4 \bmod m) - \delta m$
$= (d^4 \bmod m) - (c^4 \bmod m)$
with $m = 2^{60} - 93$
and $\delta \in \{0, 1, 2\}$.

Use sorted table of
fourth powers mod m.

Other computations

Enumerating rational points on various cubic surfaces.

Distribution seems consistent with best available conjecture.

91 can be written in 2 ways
as sum of two coprime cubes:
$91 = (-5)^3 + 6^3 = 3^3 + 4^3$.

3367 in 3 ways.

16776487 in 4 ways. (Rathbun)

5064336677359393 in 5 ways.
1379046786966133339 in 5 ways.

http://pobox.com/~djb
/sortedsums.html

http://pobox.com/~djb
/papers/sortedsums.dvi