Powers of 3 with few nonzero bits

Everett W. Howe

Unaffiliated mathematician

Math Department Colloquium

University of Florida
25 October 2023

email: however@alumni.caltech.edu Web site: ewhowe.com Bluesky: @however.bsky.social Mastodon: @however@tech.lgbt Twitter: @howe

Acknowledgement and background

Non-historical parts of this talk are based on:

Vassil S. Dimitrov and Everett W. Howe,
Powers of 3 with few nonzero bits and a conjecture of Erdős,
Rocky Mountain J. Math. (to appear)
arXiv: 2105.06440

- Background needed: Congruences, the rings $\mathbb{Z}/m\mathbb{Z}$, "mathematical maturity."
- So we wrote the paper hoping to make it accessible to undergraduates.
- ArXiv versions 1 and 2 are especially approachable.
- There are complicated arguments! But no further background is needed.

Musical demonstration

Ratios of lengths, and pitches of musical notes

The first string on the ukulele is 34.4 cm long.

How much do we shorten the string to get basic musical intervals?

Relative pitch	Length of string (cm)	Decimal fraction	Rational fraction
Octave	17.2	0.50	1/2
Fifth	23.0	0.67	2/3
Fourth	25.8	0.75	3/4
Third	27.4	0.80	4/5
Whole step	30.6	0.89	8/9

- 14th century European music theorists didn't like the musical interval of a third.
- The intervals they *did* like correspond to the fractions 1/2, 2/3, 3/4, 8/9.
- What are some things you notice about these fractions?

Our 14th century cast of characters

Philippe de Vitry (1291–1361)

- French Catholic priest and musician
- Wrote *Ars nova notandi* (“The new art of notation”) in 1322; ushered in a new age of medieval European music, known as the “Ars nova” style
- Became Bishop of Meaux in 1351

Levi ben Gerson (1288–1344)

- French rabbi, philosopher, mathematician, and scientist
- Also known as Gersonides, Magister Leo Hebraeus, and RaLBaG

What de Vitry noticed

Music and number theory

- de Vitry called an integer "harmonic" if it was of the form $2^a \cdot 3^b$.
- The numerators and denominators of the musical fractions ($1/2$, $2/3$, $3/4$, $8/9$) are all harmonic numbers!
- And the numerators and denominators differ by 1.

The numerators and denominators give solutions to

$$3^x = 2^y \pm 1.$$

de Vitry asked ben Gerson whether there were any other pairs of harmonic numbers that differ by 1.

ben Gerson's answer

- ben Gerson wrote *De numeris harmonicis* ("On harmonic numbers") in 1342.
- Written in Hebrew. No contemporaneous Hebrew copies known to still exist.
- 14th century Latin translations do exist.
- ben Gerson begins by saying that de Vitry asked him this question.
- He shows that no other such pairs exist!

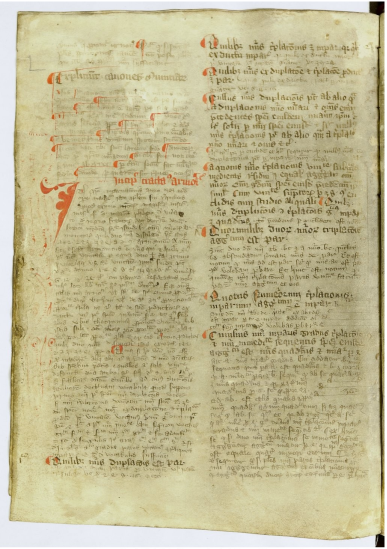
De numeris harmonicis

de Vitry asked ben Gerson whether there were any other pairs of harmonic numbers that differ by 1.

ben Gerson's answer

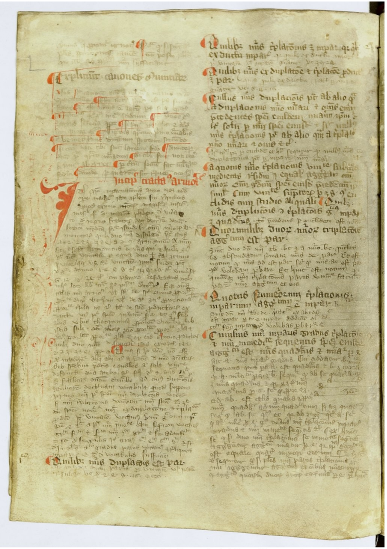
- ben Gerson wrote *De numeris harmonicis* ("On harmonic numbers") in 1342.
- Written in Hebrew. No contemporaneous Hebrew copies known to still exist.
- 14th century Latin translations do exist.
- ben Gerson begins by saying that de Vitry asked him this question.
- He shows that no other such pairs exist!

Remarkable when you consider that mathematicians did not yet use letters for variables!



First page of Gersonides's proof, courtesy of the Bibliothèque national de France

What a 14th century manuscript looks like



First page of Gersonides's proof, courtesy of the Bibliothèque national de France

A more legible paraphrase is given in:

Karine Chemla and Serge Pahaut,
Remarques sur les ouvrages mathématiques de Gersonide,
pp. 149–191 in:

G. Freudenthal (ed.),
Studies on Gersonides —
A Fourteenth-Century Jewish Philosopher-Scientist,
E. J. Brill, Leiden, 1992

Five cases of ben Gerson's proof

ben Gerson's proof involves proving thirty (!) intermediate cases and results.

The critical results

26. $3^{2n+1} - 1$ is not a power of 2, unless $n = 0$, which gives $3^1 - 1 = 2^1$.
27. $3^{4n} - 1$ is not a power of 2.
28. $3^{4n+2} - 1$ is not a power of 2, unless $n = 0$, which gives $3^2 - 1 = 2^3$.
29. $3^{2n} + 1$ is not a power of 2, unless $n = 0$, which gives $3^0 + 1 = 2^1$.
30. $3^{2n+1} + 1$ is not a power of 2, unless $n = 0$, which gives $3^1 + 1 = 2^2$.

Five cases of ben Gerson's proof

ben Gerson's proof involves proving thirty (!) intermediate cases and results.

The critical results

26. $3^{2n+1} - 1$ is not a power of 2, unless $n = 0$, which gives $3^1 - 1 = 2^1$.
27. $3^{4n} - 1$ is not a power of 2.
28. $3^{4n+2} - 1$ is not a power of 2, unless $n = 0$, which gives $3^2 - 1 = 2^3$.
29. $3^{2n} + 1$ is not a power of 2, unless $n = 0$, which gives $3^0 + 1 = 2^1$.
30. $3^{2n+1} + 1$ is not a power of 2, unless $n = 0$, which gives $3^1 + 1 = 2^2$.

If you squint hard enough, he proves these by showing that:

26. $3^{2n+1} - 1 \equiv 2 \bmod 4$.
27. $3^{4n} - 1 \equiv 0 \bmod 5$.
28. $3^{4n+2} - 1 \equiv 8 \bmod 16$.
29. $3^{2n} + 1 \equiv 2 \bmod 4$.
30. $3^{2n+1} + 1 \equiv 4 \bmod 8$.

The proof I saw in graduate school

Problem: Find all x and y with $3^x \pm 1 = 2^y$.

The proof I saw in graduate school

Problem: Find all x and y with $3^x \pm 1 = 2^y$.

Case 1: x is odd

- $3^x \equiv 3 \bmod 8$, so left hand side is 2 or 4 $\bmod 8$.
- Left hand side can't be a power of 2 unless it is equal to 2 or 4.

The proof I saw in graduate school

Problem: Find all x and y with $3^x \pm 1 = 2^y$.

Case 1: x is odd

- $3^x \equiv 3 \bmod 8$, so left hand side is 2 or 4 $\bmod$ 8.
- Left hand side can't be a power of 2 unless it is equal to 2 or 4.

Case 2: x is even and $3^x + 1 = 2^y$

- $3^x \equiv 1 \bmod 8$, so left hand side is 2 $\bmod$ 8.
- Left hand side can't be a power of 2 unless it is equal to 2.

The proof I saw in graduate school

Problem: Find all x and y with $3^x \pm 1 = 2^y$.

Case 1: x is odd

- $3^x \equiv 3 \bmod 8$, so left hand side is 2 or 4 $\bmod 8$.
- Left hand side can't be a power of 2 unless it is equal to 2 or 4.

Case 2: x is even and $3^x + 1 = 2^y$

- $3^x \equiv 1 \bmod 8$, so left hand side is $2 \bmod 8$.
- Left hand side can't be a power of 2 unless it is equal to 2.

Case 3: x is even and $3^x - 1 = 2^y$

- If $x = 2z$ then $3^x - 1 = 3^{2z} - 1 = (3^z + 1)(3^z - 1)$.
- If this is a power of 2, then both factors are powers of 2.
- The two factors differ by 2, so we must have $3^z - 1 = 2$.
- This gives $z = 1$, so $x = 2$.

The nicest proof I know

Let's go to the blackboard. . .

Let's go to the blackboard...

Powers of 2 mod 80:

$$\begin{tikzcd}
1 \arrow[r] & 2 \arrow[r] & 4 \arrow[r] & 8 \arrow[rr] & & 16 \arrow[dr, bend left] & \\
& & & & 48 \arrow[ur, bend left] & & 32 \arrow[dl, bend left] \\
& & & & & 64 \arrow[ul, bend left] &
\end{tikzcd}$$

Powers of 3 mod 80:

$$\begin{tikzcd}
& 1 \arrow[dr, bend left] & \\
27 \arrow[ur, bend left] & & 3 \arrow[dl, bend left] \\
& 9 \arrow[ul, bend left] &
\end{tikzcd}$$

New (?) topic: Powers of 3 in binary

n	binary representation of 3^n	#bits	#ones
1	11	2	2
2	1001	4	2
3	11011	5	4
4	1010001	7	3
5	11110011	8	6
6	1011011001	10	6
7	100010001011	12	5
8	1100110100001	13	6
9	100110011100011	15	8
10	1110011010101001	16	9
11	101011001111111011	18	13
12	10000001101111110001	20	10
13	110000101001111010011	21	11
14	10010001111101101111001	23	14
15	110110101111001001101011	24	15
16	10100100001101011101000001	26	11
17	111101100101000010111000011	27	14
18	10111000101111001000101001001	29	14
19	1000101010001101011001111011011	31	17
20	11001111110101000001101110010001	32	17
21	1001101111011111000101001010110011	34	20
22	11101001110011101001111100000011001	35	19
23	1010111101011010111101110100001001011	37	22
24	100000111000010000111001011100011100001	39	16
25	1100010101000110010101100010101010100011	40	18

New (?) topic: Powers of 3 in binary

n	binary representation of 3^n	#bits	#ones
1	11	2	2
2	1001	4	2
3	11011	5	4
4	1010001	7	3
5	11110011	8	6
6	1011011001	10	6
7	100010001011	12	5
8	1100110100001	13	6
9	100110011100011	15	8
10	1110011010101001	16	9
11	101011001111111011	18	13
12	10000001101111110001	20	10
13	110000101001111010011	21	11
14	10010001111101101111001	23	14
15	110110101111001001101011	24	15
16	10100100001101011101000001	26	11
17	111101100101000010111000011	27	14
18	10111000101111001000101001001	29	14
19	1000101010001101011001111011011	31	17
20	11001111110101000001101110010001	32	17
21	1001101111011111000101001010110011	34	20
22	11101001110011101001111100000011001	35	19
23	1010111101011010111101110100001001011	37	22
24	100000111000010000111001011100011100001	39	16
25	1100010101000110010101100010101010100011	40	18

What do you notice? What do you wonder?

Conjectures inspired by observation

A perfectly reasonable conjecture suggested by this data:

Conjecture 1

The number of ones in the binary expansion of 3^n *is asymptotic to* $n \cdot (\log_2 3)/2$.

This seems far too difficult to prove by current methods. A weaker conjecture:

Conjecture 2

The number of ones in the binary expansion of 3^n *tends to infinity with* n.

Equivalently:

Conjecture 3

For every positive b*, there are only finitely many* n *such that* 3^n *has exactly* b *ones in its binary representation.*

Some conjectures are true!

Conjectures 2 and 3 are true:

Proof by H. G. Senge and E. G. Straus, 1970

- Based on results about approximating algebraic numbers by rational numbers.
- "Ineffective" — does not give information about *how big* an n can be if 3^n has only b bits equal to one.

Proof by Cameron Stewart, 1980

- Based on Baker's theorem about linear forms in logarithms.
- "Effective" — the result *does* give bounds on how big n can be if 3^n has only b bits equal to one.
- Impractical — the bounds are very, very large.

Effective vs. practical

How big are the bounds?

- Stewart gives a function $S(b)$ so that if $n \geq S(b)$, then 3^n has more than b bits equal to one.
- S is hard to calculate, but we can compute upper and lower bounds for it.
- For example: $S(3) > 5000$; $S(4) > 300{,}000$; $S(22) > 4.9 \times 10^{46}$.
- There's no reason to think Stewart's lower bound $S(b)$ is the *best* lower bound.

The table of binary expansions of 3^n a few slides ago showed that 3^n has at most 22 bits equal to one when $n \leq 25$.

Calculating further, when $n > 25$ we find that 3^n always seems to have more than 22 bits equal to one.

Do we really have to check more than 4.9×10^{46} values of n to verify this?

Better bounds for particular values of b

Recall Conjecture 3:

For every positive b, there are only finitely many n such that 3^n has exactly b ones in its binary representation.

Theorem 4 (Dimitrov/H.)

The powers of 3 with at most 22 ones in their binary representations are exactly the powers of 3 in the table given earlier: 3^n with $n \leq 25$.

Better bounds for particular values of b

Recall Conjecture 3:

For every positive b, there are only finitely many n such that 3^n has exactly b ones in its binary representation.

Theorem 4 (Dimitrov/H.)

The powers of 3 with at most 22 ones in their binary representations are exactly the powers of 3 in the table given earlier: 3^n with $n \leq 25$.

We don't use difficult theorems. We only use modular arithmetic!

Some more recent history

Looking for a specific number of 1s

ben Gerson and beyond

- ben Gerson [1342]: If 3^n has two 1s in binary then $n = 1$ or $n = 2$.

Looking for a specific number of 1s

ben Gerson and beyond

- ben Gerson [1342]: If 3^n has two 1s in binary then $n = 1$ or $n = 2$.
- Pillai [1945]: If 3^n has three 1s in binary then $n = 4$.

Looking for a specific number of 1s

ben Gerson and beyond

- ben Gerson [1342]: If 3^n has two 1s in binary then $n = 1$ or $n = 2$.
- Pillai [1945]: If 3^n has three 1s in binary then $n = 4$.
  - Uses a complicated congruence argument.

Looking for a specific number of 1s

ben Gerson and beyond

- ben Gerson [1342]: If 3^n has two 1s in binary then $n = 1$ or $n = 2$.
- Pillai [1945]: If 3^n has three 1s in binary then $n = 4$.
  - Uses a complicated congruence argument.
- Bennett, Bugeaud, and Mignotte [2011 and 2013]: If 3^n has four 1s in binary then $n = 3$.

Looking for a specific number of 1s

ben Gerson and beyond

- ben Gerson [1342]: If 3^n has two 1s in binary then $n = 1$ or $n = 2$.
- Pillai [1945]: If 3^n has three 1s in binary then $n = 4$.
  - Uses a complicated congruence argument.
- Bennett, Bugeaud, and Mignotte [2011 and 2013]: If 3^n has four 1s in binary then $n = 3$.
  - Uses a powerful advanced tool: linear forms in logarithms.
  - Their result is much more general: If y^n has four 1s in binary then $n \leq 4$.

Skip ahead to the case $b = 6$

In the early 2000s my coauthor wanted to show there are no solutions to

$$3^n = 103 + 2^x = 1 + 2^1 + 2^2 + 2^5 + 2^6 + 2^x.$$

A special case of our question, for $b = 6$!

Advice from analytic number theorists

- Use a theorem of W. J. Ellison from 1970.
- Explicit version of a special case of a theorem of Pillai.
- Used Baker's method — linear forms in logarithms.
- Ellison's result: For $x > 27$ we have $|3^n - 2^x| > (9/5)^x$.

If you need heavy machinery to solve the case $b = 6$ with five of the powers of 2 fixed, maybe the general case is even harder…

Modular methods

ben Gerson's theorem via modular methods

Consider the argument we gave before for solving $3^n = \pm 1 + 2^x$.

Modulo 80:

- Powers of 2: $1, 2, 4, 8, 16, 32, 64, 48, 16, \ldots$
- Powers of 3: $1, 3, 9, 27, 1, \ldots$
- Only solutions modulo 80 are:
  $3 \equiv 1 + 2, \qquad 9 \equiv 1 + 8, \qquad 1 \equiv -1 + 2, \qquad 3 \equiv -1 + 4$
- Only powers of 2 that reduce modulo 80 to 2, 4, or 8 are 2, 4, and 8 themselves.
- (Depends on 80 being divisible by 16.)

Method of Leo J. Alex (early 1980s)

J. L. Brenner and Lorraine L. Foster write that Alex used "several small moduli" to solve the case $b = 3$: $3^n = 1 + 2^x + 2^y$.

Can be done all at once. For example, take $m = 2796160 = 2^7 \cdot 5 \cdot 17 \cdot 257$.

Modulo 2796160:

- Powers of 2: (23 numbers)
- Powers of 3: (256 numbers)
- Sums of two powers of 2: (275 numbers)
- Compare sums of two powers of 2 with powers of 3 minus 1.
- Find three solutions: $3 \equiv 1 + 1 + 1$, $9 \equiv 1 + 4 + 4$, $81 \equiv 1 + 16 + 64$.
- For $i < 7$, the only power of 2 that reduces modulo m to 2^i is 2^i itself.
- 81 is the only power of 3 with 3 ones in its binary expansion.

First attempt at an approach

1. Enumerate integer solutions to $3^n = \sum_{i=1}^{b} 2^{x_i}$ until you think you have them all.
2. Let 2^x be the largest power of 2 appearing in any right-hand side.
3. Find a modulus $m = 2^y 3^z m_0$ with $y > x$ such that
   - The multiplicative order of 2 in $\mathbb{Z}/m_0\mathbb{Z}$ is small.
   - The multiplicative order of 3 in $\mathbb{Z}/m_0\mathbb{Z}$ is small.
4. Enumerate solutions modulo m.
5. Hope: All solutions involve powers of 2 mod m that lift *uniquely* to the integers.

Choosing the modulus

Questions

- How do we find a good modulus m to try?
- What do we do if the m we choose doesn't work?
- Computational reasons suggest building up m by throwing in more prime factors. How to choose them?

Example with $b = 3$ again

A few slides ago we solved $3^n = 1 + 2^x + 2^y$ by looking modulo $2^7 \cdot 5 \cdot 17 \cdot 257$.

What if we had tried using $m_1 = 5440 = 2^6 \cdot 5 \cdot 17$ instead?

Modulo 5440:

- Powers of 2: (14 numbers)
- Powers of 3: (16 numbers)
- Sums of two powers of 2: (104 numbers)
- Compare sums of two powers of 2 with powers of 3 minus 1.
- Find three solutions: $3 = 1 + 1 + 1, \quad 9 = 1 + 4 + 4, \quad 81 = 1 + 16 + 64.$
- But now there are infinitely many y with $2^y = 64 \bmod m_1$.
- Let's just throw in another factor of 2 in the modulus to avoid this problem…

Extraneous solutions

Solutions modulo $m_2 = 2m_1 = 2^7 \cdot 5 \cdot 17$

$$
\begin{aligned}
3^1 &\equiv 2^0 + 2^0 + 2^0 \mod m_2 \\
3^2 &\equiv 2^0 + 2^2 + 2^2 \mod m_2 \\
3^4 &\equiv 2^0 + 2^4 + 2^6 \mod m_2
\end{aligned}
$$

Extraneous solutions

Solutions modulo $m_2 = 2m_1 = 2^7 \cdot 5 \cdot 17$

$$
\begin{aligned}
3^1 &\equiv 2^0 + 2^0 + 2^0 \mod m_2\\
3^2 &\equiv 2^0 + 2^2 + 2^2 \mod m_2\\
3^4 &\equiv 2^0 + 2^4 + 2^6 \mod m_2\\
3^{20} &\equiv 2^0 + 2^4 + 2^{14} \mod m_2
\end{aligned}
$$

Extraneous solutions

Solutions modulo $m_2 = 2m_1 = 2^7 \cdot 5 \cdot 17$

$$
\begin{aligned}
3^1 &\equiv 2^0 + 2^0 + 2^0 \mod m_2\\
3^2 &\equiv 2^0 + 2^2 + 2^2 \mod m_2\\
3^4 &\equiv 2^0 + 2^4 + 2^6 \mod m_2\\
3^{20} &\equiv 2^0 + 2^4 + 2^{14} \mod m_2
\end{aligned}
$$

Solutions modulo $m_3 = 41m_2 = 2^7 \cdot 5 \cdot 17 \cdot 41$

$$
\begin{aligned}
3^1 &\equiv 2^0 + 2^0 + 2^0 \mod m_3\\
3^2 &\equiv 2^0 + 2^2 + 2^2 \mod m_3\\
3^4 &\equiv 2^0 + 2^4 + 2^6 \mod m_3
\end{aligned}
$$

Extraneous solutions

Solutions modulo $m_2 = 2m_1 = 2^7 \cdot 5 \cdot 17$

$$
\begin{aligned}
3^1 &\equiv 2^0 + 2^0 + 2^0 \mod m_2\\
3^2 &\equiv 2^0 + 2^2 + 2^2 \mod m_2\\
3^4 &\equiv 2^0 + 2^4 + 2^6 \mod m_2\\
3^{20} &\equiv 2^0 + 2^4 + 2^{14} \mod m_2
\end{aligned}
$$

Solutions modulo $m_3 = 41m_2 = 2^7 \cdot 5 \cdot 17 \cdot 41$

$$
\begin{aligned}
3^1 &\equiv 2^0 + 2^0 + 2^0 \mod m_3\\
3^2 &\equiv 2^0 + 2^2 + 2^2 \mod m_3\\
3^4 &\equiv 2^0 + 2^4 + 2^6 \mod m_3\\
3^{20} &\equiv 2^0 + 2^4 + 2^{46} \mod m_3
\end{aligned}
$$

More extraneous solutions!

Solutions modulo $m_4 = 193m_3 = 2^7 \cdot 5 \cdot 17 \cdot 41 \cdot 193$

$$
\begin{aligned}
3^1 &\equiv 2^0 + 2^0 + 2^0 \mod m_4\\
3^2 &\equiv 2^0 + 2^2 + 2^2 \mod m_4\\
3^4 &\equiv 2^0 + 2^4 + 2^6 \mod m_4
\end{aligned}
$$

More extraneous solutions!

Solutions modulo $m_4 = 193m_3 = 2^7 \cdot 5 \cdot 17 \cdot 41 \cdot 193$

$$
\begin{aligned}
3^1 &\equiv 2^0 + 2^0 + 2^0 \mod m_4\\
3^2 &\equiv 2^0 + 2^2 + 2^2 \mod m_4\\
3^4 &\equiv 2^0 + 2^4 + 2^6 \mod m_4\\
3^{244} &\equiv 2^0 + 2^4 + 2^{46} \mod m_4
\end{aligned}
$$

More extraneous solutions!

Solutions modulo $m_4 = 193m_3 = 2^7 \cdot 5 \cdot 17 \cdot 41 \cdot 193$

$$
\begin{aligned}
3^1 &\equiv 2^0 + 2^0 + 2^0 \mod m_4 \\
3^2 &\equiv 2^0 + 2^2 + 2^2 \mod m_4 \\
3^4 &\equiv 2^0 + 2^4 + 2^6 \mod m_4 \\
3^{244} &\equiv 2^0 + 2^4 + 2^{46} \mod m_4
\end{aligned}
$$

Questions

- Why are we getting these extraneous solutions?
- (We wouldn't expect them by chance.)
- Why did we *not* get extraneous solutions modulo $m = 2^7 \cdot 5 \cdot 17 \cdot 257$?

An unexpected condition

The multiplicative order of 3 modulo various m:

$$3^{16} \equiv 1 \bmod 5 \cdot 17$$
$$3^{16} \equiv 1 \bmod 5 \cdot 17 \cdot 41$$
$$3^{16} \equiv 1 \bmod 5 \cdot 17 \cdot 41 \cdot 193$$

$$3^{256} \equiv 1 \bmod 5 \cdot 17 \cdot 257$$

An unexpected condition

The multiplicative order of 3 modulo various m:

$$3^{16} \equiv 1 \bmod 5 \cdot 17$$
$$3^{16} \equiv 1 \bmod 5 \cdot 17 \cdot 41$$
$$3^{16} \equiv 1 \bmod 5 \cdot 17 \cdot 41 \cdot 193$$

$$3^{256} \equiv 1 \bmod 5 \cdot 17 \cdot 257$$

The source of extraneous solutions

It turns out: The solution $3^4 = 1 + 2^4 + 2^6$ leads to an additional extraneous solution modulo m unless $2^{6-1} = 32$ divides the multiplicative order of 3 modulo m.

Computational issues

Our method: Very special moduli

We carefully chose a sequence of moduli $m_1, \ldots, m_{62}$, each dividing the next.

Final algorithm

- Compute all solutions to $3^n \equiv 2^{x_1} + \cdots + 2^{x_{b-1}} + 2^{x_b} \bmod m_1$ by enumeration.
- Repeat the following:
  - Given the set of solutions modulo m_i, we consider each solution in turn.
  - For each solution, we lift the powers of 2 on the right-hand side from $\mathbb{Z}/m_i\mathbb{Z}$ to $\mathbb{Z}/m_{i+1}\mathbb{Z}$.
  - For each possible lifted right-hand side, we check: Is the sum is a power of 3 in $\mathbb{Z}/m_{i+1}\mathbb{Z}$?
  - If so, we add the lifted solution to the list of solutions modulo m_{i+1}.
- If we have lifted solutions to a modulus m_k, and if every power of 2 in every solution lifts uniquely from $\mathbb{Z}/m_k\mathbb{Z}$ to the integers, we are done.

Timings

Using this method, we solved the case $b = 14$ in under a minute on my previous laptop, a 2.8 GHz Quad-Core Intel Core i7 Macbook Pro.

This is an exponential Diophantine equation involving 14 variables!

Timings

Using this method, we solved the case $b = 14$ in under a minute on my previous laptop, a 2.8 GHz Quad-Core Intel Core i7 Macbook Pro.

This is an exponential Diophantine equation involving 14 variables!

The case $b = 19$ took 5 hours on one core.

Timings

Using this method, we solved the case $b = 14$ in under a minute on my previous laptop, a 2.8 GHz Quad-Core Intel Core i7 Macbook Pro.

This is an exponential Diophantine equation involving 14 variables!

The case $b = 19$ took 5 hours on one core.

Details for the case $n = 22$

- Took 207 core-hours, using four cores.
- Our m was a 376-digit number built up from 56 prime factors.
- There are 3,710,851,743,781 powers of 2 modulo m, with 37 on the tail.
- There are more than 7.4×10^{45} powers of 3 modulo m.

A related problem

A conjecture of Erdős:

If 2^n has only 0's and 1's in its base-3 representation, then $2^n = 1$, 4, or 256.

A related problem

A conjecture of Erdős:

If 2^n has only 0's and 1's in its base-3 representation, then $2^n = 1$, 4, or 256.

Theorem 5 (Dimitrov/H.)

The only powers of 2 *that can be written as the sum of twenty-one or fewer distinct powers of* 3 *are*:

$$2^0 = 3^0$$
$$2^2 = 3^0 + 3^1$$
$$2^8 = 3^0 + 3^1 + 3^2 + 3^5.$$

The computations for this are very similar to the ones already described.

Related work

Skolem (1937)

Conjecture: If an exponential Diophantine equation has no solutions, there is an m so that it has no solutions modulo m.

Alex, Brenner, and Foster (1980s)

Solved exponential Diophantine equations using congruences.
Limited computational resources compared to today.

Bertók and Hajdu (2010s)

Refined Skolem's conjecture. Used modular approaches to solve exponential Diophantine equations, but not as efficiently as using our method.

Largest example in their work: finding all powers of 17 that can be written a sum of nine powers of 5.