Math from Medieval Musicians

Everett W. Howe

Unaffiliated mathematician

San Marcos Informal Mathematics In-person Colloquium

California State University San Marcos
16 February 2023

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

Land acknowledgement

- We are meeting today on the traditional territory and homelands of the Luiseño/Payómkawichum people.
- I did the research described in this talk in my home about 30 miles south of here, on unceded Kumeyaay territory.
- I would like to
  - honor the legacy of the continued presence of the native peoples of San Diego County;
  - recognize the violent history of colonization in California.

Moving beyond acknowledgements

- CSUSM hosts the California Indian Culture and Sovereignty Center.
- Located in SBSB 1118, open to all faculty, staff, and students.
- The CICSC web site suggests ways for those of us who are guests on this land to support, and build accountable relationships with, native peoples.

Acknowledgement and references

The non-historical parts of this talk are based on joint work with Vassil Dimitrov (University of Calgary and IOTA Foundation, Berlin).

Our paper describing further applications of today's talk

Vassil S. Dimitrov and Everett W. Howe,
Powers of 3 with few nonzero bits and a conjecture of Erdős,
arXiv: 2105.06440

- This paper was written with the intent of being accessible to undergraduates.
- It assumes the reader knows about congruences and about the rings $\mathbb{Z}/m\mathbb{Z}$.
- It has complicated arguments! But no further technical background is needed.

Musical demonstration

Ratios of lengths and pitches of musical notes

The first string on my friend's ukulele is 34.6 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	17.3	0.50	1/2
Fifth	23.3	0.67	2/3
Fourth	25.9	0.75	3/4
Third	27.6	0.80	4/5
Whole step	30.9	0.89	8/9

- In the 14th century, music theorists did not like the musical interval of a third.
- The intervals they liked 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 a number “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

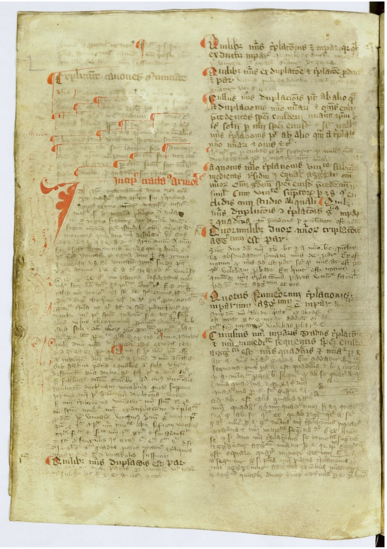
de Vitry asked ben Gerson whether there were any other pairs of harmonic numbers that differ by 1.

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!

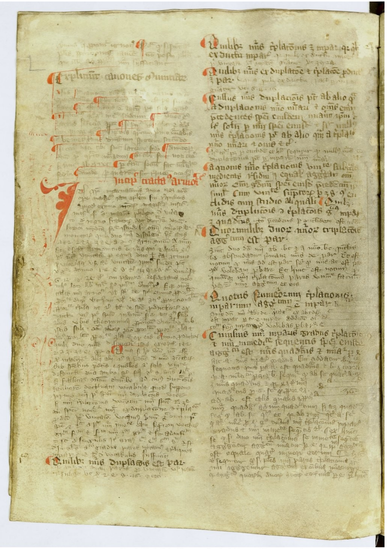
Remarkable when you consider that mathematicians did not yet use letters for variables!

What a 14th century manuscript looks like



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

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

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

- $3^x \equiv 1 \mod 8$, so left hand side is 2 $\mod 8$.
- 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 $3^x - 1 = 2^y$

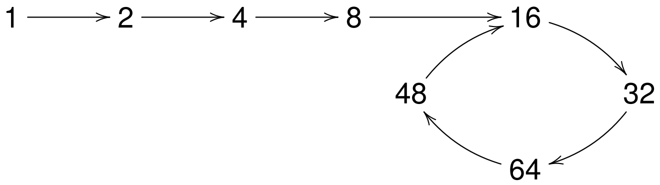
- If $x = 2z$ then $3^x - 1 = 3^{2z} - 1 = (3^z + 1)(3^z - 1)$.
- If this is a power of 2, then both factors are powers of 2.
- The two factors differ by 2, so we must have $3^z - 1 = 2$.
- This gives $z = 1$, so $x = 2$.

The nicest proof I know

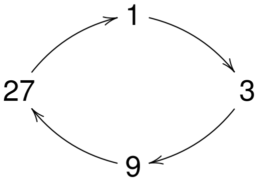
Let's go to the whiteboard. . .

Let's go to the whiteboard. . .

Powers of 2 mod 80:



Powers of 3 mod 80:



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	11001111111010100000110111001000 1	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?

Some things that are known about powers of 3 in binary

- Senge and Strauss [1973]: The number of 1s in 3^x goes to infinity with x.
- Stewart [1980]: Gives a computable lower bound $B(n)$:

$$\text{If } x > B(n), \text{ then } 3^x \text{ has more than } n \text{ ones in binary.}$$

- Stewart's bound is not very practical…

Some things that are known about powers of 3 in binary

- Senge and Strauss [1973]: The number of 1s in 3^x goes to infinity with x.
- Stewart [1980]: Gives a computable lower bound $B(n)$:

$$\text{If } x > B(n), \text{ then } 3^x \text{ has more than } n \text{ ones in binary.}$$

- Stewart's bound is not very practical…
- $B(3) > 5000$; $B(4) > 300{,}000$; $B(22) > 4.9 \times 10^{46}$.

What does this mean?

Suppose you would like to find all x such that 3^x has at most 22 bits equal to 1.

Stewart says: You can simply start checking values of x one by one, and stop at some point *after* you've checked 4.9×10^{46} values.

de Vitry and beyond

- Half of de Vitry's question was to solve $3^x = 1 + 2^y$.
- Rephrased: "What powers of 3 have two 1s when written in binary?"

de Vitry and beyond

- Half of de Vitry's question was to solve $3^x = 1 + 2^y$.
- Rephrased: "What powers of 3 have two 1s when written in binary?"

Looking for specific numbers of 1s

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

de Vitry and beyond

- Half of de Vitry's question was to solve $3^x = 1 + 2^y$.
- Rephrased: "What powers of 3 have two 1s when written in binary?"

Looking for specific numbers of 1s

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

de Vitry and beyond

- Half of de Vitry's question was to solve $3^x = 1 + 2^y$.
- Rephrased: "What powers of 3 have two 1s when written in binary?"

Looking for specific numbers of 1s

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

de Vitry and beyond

- Half of de Vitry's question was to solve $3^x = 1 + 2^y$.
- Rephrased: "What powers of 3 have two 1s when written in binary?"

Looking for specific numbers of 1s

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

- Half of de Vitry's question was to solve $3^x = 1 + 2^y$.
- Rephrased: "What powers of 3 have two 1s when written in binary?"

Looking for specific numbers of 1s

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

The powers of 3 in binary again

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

The powers of 3 in binary again

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	11101001110011101001111110000011001	35	19
23	1010111101011010111101110100001001011	37	22
24	100000111000010000111001011100011100001	39	16
25	1100010101000110010101100010101010100011	40	18

My work with Dimitrov [2020]: If 3^x has twenty-two 1s or fewer, it is on this table.

Our argument for finding powers of 3 with n ones in binary

Essentially the same as the simplified proof of ben Gerson's theorem!

Find a modulus m such that the following works:

- Compute the powers of 2 modulo m. Call this set S; it has a tail and a cycle.
- Compute the powers of 3 modulo m. Call this set T.
- Compute all solutions to
$$X \equiv A_1 + \cdots + A_n \tag{1}$$
with $X \in T$ and $A_i \in S$. We may assume that $A_1 = 1$.
- Hope that for each solution, all of the A_i are on the tail of S.
- If so, there is only one integer a_i with $2^{a_i} \equiv A_i \bmod m$.
- Lift all right hand side terms of (1) to the integers and check whether their sum is a power of 3.

Example: A simpler proof for $n = 4$

- Take $m = 2^{10} \cdot 5 \cdot 7 \cdot 13 \cdot 257$.
- The set S of powers of 2 mod m has 58 elements, 10 on the tail.
- The set T has 768 elements.
- Using a computer, compute all possible sums of 1 plus three elements of S.
- There are 26169 such sums.
- List the sums that are in T.

Example: A simpler proof for $n = 4$

- Take $m = 2^{10} \cdot 5 \cdot 7 \cdot 13 \cdot 257$.
- The set S of powers of 2 mod m has 58 elements, 10 on the tail.
- The set T has 768 elements.
- Using a computer, compute all possible sums of 1 plus three elements of S.
- There are 26169 such sums.
- List the sums that are in T.

$$\begin{aligned} 9 &\equiv 1 + 2 + 2 + 4 \\ 27 &\equiv 1 + 2 + 8 + 16 \\ 81 &\equiv 1 + 8 + 8 + 64 \\ 81 &\equiv 1 + 16 + 32 + 32 \end{aligned}$$

Difficulties

The moduli that work are rare

We need some method of choosing m that are likely to work.

The computations modulo m may be hard!

We need some efficient way of computing the solutions to (1).

Details for our result for $n = 22$

- 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.
- Took 207 hours on my previous laptop.

We started with a small divisor of m, computed solutions to (1) modulo that divisor, and then added in more primes one at a time to build up to the solutions modulo m.

Original motivation for my coauthor and me

- Dimitrov was looking at “double-base representations” of integers.
- Given n, what is the shortest expression

$$n = 2^{a_1}3^{b_1} \pm 2^{a_2}3^{b_2} \pm \cdots \pm 2^{a_r}3^{b_r}?$$

- (Harmonic numbers show up again!)
- Short representations give quick ways of multiplying a point on an elliptic curve by n. Useful for speeding up cryptography.
- Dimitrov wanted to show that 4985 could not be written with three such terms.
- Could prove this by looking modulo $5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 61 \cdot 73 \cdot 181$.

Further work?

Our computer code is tuned to the specific cases we considered in our paper:

- Finding powers of 3 with a given number of 1s in binary.
- Finding powers of 2 whose base-3 “digits” are all 0 or 1.

  (Erdős conjectured that 2, 4, and 256 are the only such powers of 2.)

Is there a way to make general “set and forget” code that will solve other equations of this type about as efficiently?

In case you want to know the m that worked for twenty-two bits

$$
\begin{aligned}
m = {} & 2^{37} \cdot 3^3 \cdot 5 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 97 \cdot 109 \cdot 193 \cdot 241 \cdot 257 \cdot 433 \cdot 577 \cdot 641 \cdot 673 \cdot \\
& 769 \cdot 1153 \cdot 6337 \cdot 12289 \cdot 18433 \cdot 38737 \cdot 65537 \cdot 87211 \cdot 101377 \cdot 114689 \cdot \\
& 274177 \cdot 319489 \cdot 786433 \cdot 9748491179649 \cdot 2424833 \cdot 13631489 \cdot \\
& 14155777 \cdot 39714817 \cdot 113246209 \cdot 167772161 \cdot 171048961 \cdot 1107296257 \cdot \\
& 3221225473 \cdot 7348420609 \cdot 7908360193 \cdot 29796335617 \cdot 74490839041 \cdot \\
& 77309411329 \cdot 206158430209 \cdot 246423748609 \cdot 448203325441 \cdot \\
& 1084521185281 \cdot 2748779069441 \cdot 5469640851457 \cdot 5566277615617 \cdot \\
& 25048249270273 \cdot 28114855919617 \cdot 942556342910977 \cdot 1095981164658689
\end{aligned}
$$