POWERS OF 3 WITH FEW NONZERO BITS AND A CONJECTURE OF ERDŐS

VASSIL S. DIMITROV AND EVERETT W. HOWE

Abstract. Using completely elementary methods, we find all powers of 3 that can be written as the sum of at most twenty-two distinct powers of 2, as well as all powers of 2 that can be written as the sum of at most twenty-five distinct powers of 3. The latter result is connected to a conjecture of Erdős, namely, that 1, 4, and 256 are the only powers of 2 that can be written as a sum of distinct powers of 3.

We present this work partly as a reminder that for certain exponential Diophantine equations, elementary techniques based on congruences can yield results that would be difficult or impossible to obtain with more advanced techniques involving, for example, linear forms in logarithms.

1. Introduction

To introduce our topic, we begin with some numerical observations. For an integer $x \geq 0$, consider the binary representation of 3^x. In Table 1 we give this representation for $x \leq 25$, and we tabulate the number of bits in the binary representation together with the number of those bits that are equal to 1.

Based on this limited data, it looks like about half of the bits of the binary representation of 3^x are equal to 1, which is what you would expect if 3^x were to behave like a random integer of the appropriate size. Computations with larger values of x seem to indicate that the fraction of 1s does tend toward $1/2$ as x increases to infinity, but proving that this is the case seems far beyond the reach of existing techniques.

A much weaker observation is that as x goes to infinity, the number of 1s in the binary representation of 3^x tends to infinity as well; that is, one would certainly be tempted to guess that there are only finitely many x such that the binary representation of 3^x contains fewer than ten 1s, or a hundred 1s, or any given finite number of 1s. This observation *is* in fact true, and was proven by Senge and Straus in 1973; their result [19, Theorem 3, p. 100] implies that for any given n, there are only finitely many x such that the binary representation of 3^x has n or fewer bits equal to 1. In 1980 Cameron Stewart proved an effective version of this result [20, Theorem 1, p. 64] — which means that given a value of n, Stewart's arguments produce a bound $B(n)$ so that if $x > B(n)$, then 3^x has more than n bits equal

Date: May 16, 2023.
2020 *Mathematics Subject Classification.* Primary 11D61; Secondary 11A63, 11D72, 11D79.
Key words and phrases. Exponential Diophantine equation, binary digit.

TABLE 1. For each x between 0 and 25 we give the binary representation of x, together with the total number of bits in the representation and the number of those bits that are equal to 1.

x	Binary representation of 3^x	#Bits	#Ones
0	1	1	1
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	11000010100111010011	21	11
14	10010001111101101111001	23	14
15	11011010111001001101011	24	15
16	10100100001101011101000001	26	11
17	11110110010100001011000011	27	14
18	10111000101111001000101001001	29	14
19	10001010100011010110011111011011	31	17
20	11001111110101000001101110010001	32	17
21	10011011110111110001010010110011	34	20
22	11101001110011101001111100000011001	35	19
23	10101111010110101111011101000010011011	37	22
24	10000011100001000011100101110001110001	39	16
25	11000101010001100101011000101010100011	40	18

to 1. Unfortunately, the values of $B(n)$ produced by Stewart's method grow very quickly; for example, we can show[1] that $B(22) > 4.9 \times 10^{46}$.

In this paper, we use completely elementary techniques to find all powers of 3 whose binary representations have at most twenty-two bits equal to 1. In fact, these powers of 3 are exactly the ones displayed in Table 1.

Theorem 1.1. *The only powers of* 3 *that can be written as the sum of twenty-two or fewer distinct powers of* 2 *are* 3^x*, where* $0 \le x \le 25$.

In other words, there are more than twenty-two 1s in the binary representation of 3^x exactly when $x > 25$. Clearly, this bound is much smaller than the one obtained from Stewart's theorem!

We also look at the complementary problem of finding powers of 2 whose base-3 representations contain no 2s and at most twenty-five 1s. Stewart's theorem applies

[1]Stewart's Theorem 1 shows that the largest x for which 3^x has at most 22 bits equal to 1 satisfies $23 > (\log\log 3^x)/(C + \log\log\log 3^x)$ for some positive constant C. We only get a stronger upper bound on x if we solve for x when $C = 0$, and this is how we get our lower bound for $B(22)$.

16 May 2023 08:21:31 PDT
210723-Howe Version 2 - Submitted to Rocky Mountain J. Math.

here as well, and says that if 2^x can be expressed in this manner, then x is less than a computable bound that is larger than 5.4×10^{54}. Our result shows that in fact $x \leq 8$.

Theorem 1.2. *The only powers of* 2 *that can be written as the sum of twenty-five or fewer distinct powers of* 3 *are*:

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

Put differently, if $x \notin \{0, 2, 8\}$ then the base-3 representation of 2^x will contain either at least one 2, or at least twenty-six 1s. This provides a tiny bit of confirmation for a conjecture of Erdős [14, Problem 1, p. 67], which states that the only powers of 2 whose base-3 representations contain only 0s and 1s are the three examples given in Theorem 1.2. (For work on Erdős's conjecture and closely related problems, see for example [5, 13, 16, 17] and the papers these articles cite.)

Theorems 1.1 and 1.2 can be expressed in terms of exponential Diophantine equations. In particular, Theorem 1.1 gives us all solutions of

$$3^x = 2^{a_1} + \cdots + 2^{a_n}, \qquad x \geq 0, \quad 0 \leq a_1 < \cdots < a_n \tag{1}$$

for $n \leq 22$, and Theorem 1.2 gives us all solutions to

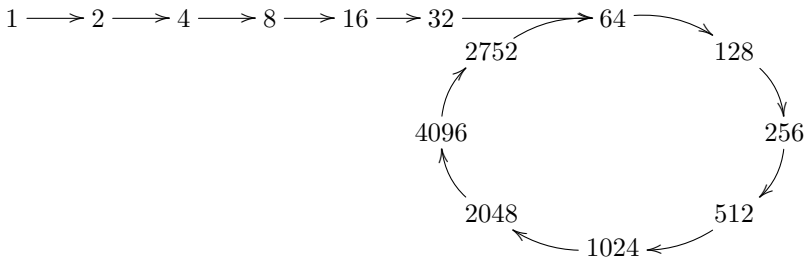
$$2^x = 3^{a_1} + \cdots + 3^{a_n}, \qquad x \geq 0, \quad 0 \leq a_1 < \cdots < a_n \tag{2}$$

for $n \leq 25$.

Our method for solving equations (1) and (2) involves considering the equations modulo M for a sequence of well-chosen moduli M, each one dividing the next. We will postpone our discussion of what "well-chosen" means, and for now we will simply illustrate our method with an example.

Let us look at the case $n = 3$ of equation (1). We start by considering the related problem of writing a power of 3 as the sum of three powers of 2 in the finite ring $\mathbf{Z}/M_1\mathbf{Z}$ for $M_1 = 5440 = 2^6 \cdot 5 \cdot 17$, where we no longer insist that the powers of 2 be distinct. The following diagram enumerates the powers of 2 in modulo M_1; here the arrows indicate multiplication by 2.

(3)



We see there are 14 distinct powers of 2 modulo M_1, and likewise we find that there are 16 distinct powers of 3. Using a computer to enumerate sums of three powers of 2 in $\mathbf{Z}/M_1\mathbf{Z}$, we find that (up to the order of the summands) there are only three

ways to write a power of 3 in $\mathbf{Z}/M_1\mathbf{Z}$ as a sum of three powers of 2:

$$3^1 \equiv 2^0 + 2^0 + 2^0 \bmod M_1 \tag{4}$$

$$3^2 \equiv 2^0 + 2^2 + 2^2 \bmod M_1 \tag{5}$$

$$3^4 \equiv 2^0 + 2^4 + 2^6 \bmod M_1. \tag{6}$$

For each of the summands 2^i on the right-hand side of one of these equations, we can ask for the exponents b such that $2^b \equiv 2^i \bmod M_1$. Looking at diagram (3), we see that for $i = 0, 2$, and 4, the only exponent b with $2^b \equiv 2^i \bmod M_1$ is i itself, because 1, 4, and 16 are all on the "tail" of the diagram. On the other hand, the exponents b with $2^b \equiv 2^6 \bmod M_1$ are $\{6, 14, 22, 30, \ldots\} = \{6 + 8j : j \geq 0\}$, because the "loop" part of diagram (3) goes around in a cycle of 8 steps.

Every solution to equation (1) with $n = 3$ must reduce modulo M_1 to one of the three equations (4), (5), or (6). However, no solution to equation (1) can reduce to (4), because the summands in (1) would have to be 2^0, 2^0, and 2^0, which are not distinct. Likewise, no solution to equation (1) can reduce modulo M_1 to (5), because two of the summands in (1) would have to be 2^2. Therefore, every solution to equation (1) with $n = 3$ reduces modulo M_1 to (6), and we see that two of the summands in (1) must be 2^0 and 2^4.

Now we consider information modulo $M_2 = 2^7 \cdot 5 \cdot 17 \cdot 257$. If a solution to equation (1) reduces modulo M_1 to (6), what can it reduce to modulo M_2? There are 16 powers of 3 in $\mathbf{Z}/M_2\mathbf{Z}$ that reduce to 3^4 in $\mathbf{Z}/M_1\mathbf{Z}$, namely $3^4, 3^{4+16}, \ldots, 3^{4+15\cdot 16}$, and there are 3 powers of 2 in $\mathbf{Z}/M_2\mathbf{Z}$ that reduce to 2^6 in $\mathbf{Z}/M_1\mathbf{Z}$, namely 2^6, 2^{14}, and 2^{22}. We check that in $\mathbf{Z}/M_2\mathbf{Z}$ neither $2^0 + 2^4 + 2^{14}$ nor $2^0 + 2^4 + 2^{22}$ is equal to any of the possible powers of 3. However, $3^4 \equiv 2^0 + 2^4 + 2^6$ in $\mathbf{Z}/M_2\mathbf{Z}$.

Therefore, every solution to equation (1) with $n = 3$ must reduce modulo M_2 to the congruence $3^4 \equiv 2^0 + 2^4 + 2^6 \bmod M_2$. But we check that 2^0, 2^4, and 2^6 lie on the tail of the analog of diagram (3) for M_2, so the only powers of 2 in the integers that reduce to 2^0, 2^4, and 2^6 modulo M_2 are 2^0, 2^4, and 2^6 themselves. We see that if there is a solution to equation (1) with $n = 3$, the right-hand side must be $2^0 + 2^4 + 2^6$. As it happens, in the integers this sum is equal to 3^4, so $3^4 = 2^0 + 2^4 + 2^6$ is the unique solution to equation (1) with $n = 3$.

This simple example displays the basic idea that we use to prove Theorem 1.1. For such a small example we could have *started* by considering the equation modulo M_2, instead of first looking modulo M_1, but for larger examples it is much more efficient to cut down the solution space by looking first at small moduli before building up to larger ones.

Solving exponential Diophantine equations using congruence arguments is not a new technique. In 1976, for example, Alex [2] used congruences to find all solutions to $x + y = z$, where x, y, and z are mutually coprime integers divisible by no prime larger than 7. In 1982, Brenner and Foster [10] presented a whole bestiary of exponential Diophantine equations that can be solved in this way. (They mention in particular that Alex found all solutions to our example $3^x = 2^{a_1} + 2^{a_2} + 2^{a_3}$ using "a few small moduli," although this had been solved earlier by Pillai, as we discuss below.) In 2009, Ádám, Hajdu, and Luca [1] used a result of Erdős, Pomerance, and Schmutz [15] to show that for every finite set S of primes and finite set $A \subset \mathbf{Z}$ of coefficients, the number of integers less than x that can be written as the sum of a fixed number of terms of the form as, where $a \in A$ and $s \in \mathbf{Z}$ is a product of powers of primes in S, grows more slowly than a specific power of $\log x$. Independently,

16 May 2023 08:21:31 PDT
210723-Howe Version 2 - Submitted to Rocky Mountain J. Math.

in a 2011 paper [12] we studied representations of integers as sums of terms of the form $\pm 2^a 3^b$, which is the case $A = \{\pm 1\}$, $S = \{2, 3\}$ of the problem studied in [1]. We presented one way of finding moduli m that could be used to prove that certain integers cannot be represented by a given number of such terms, and we used the same result of Erdős, Pomerance, and Schmutz to show that there is a positive constant c such that infinitely many integers n cannot be written as a sum of fewer than $c \log n/(\log \log n \log \log \log n)$ such terms.

In 2016 Bertók and Hajdu [7] studied exponential Diophantine equations in general, again using arguments based on [15], and they conjectured that if an exponential Diophantine equation has a finite number of solutions[2] and satisfies some other natural restrictions, then there is an integer M such that the solutions to the equation modulo M lift uniquely to the solutions in $\mathbf{Z}$. In a later paper [8] the same authors generalized this conjecture to number fields. One can view our work in this paper as providing evidence in support of the Bertók–Hajdu conjectures.

Our main contribution in this paper is the method we describe for choosing a sequence of moduli that allows us to refine the collection of solutions modulo M, for larger and larger M, until every solution modulo M can be lifted to at most one solution in the integers. Our moduli are chosen in a careful order that makes each refinement step computationally feasible. The closest predecessor to our technique seems to be the method used by Bertók and Hajdu in [7], in which they choose a modulus M and then piece together information gleaned from solutions to the original Diophantine equation modulo the prime power divisors of M. Another new observation in this paper appears in Section 3, where we show that any modulus M that provides us with all solutions to equation (1) or (2) must satisfy an unexpected condition.

We study the problem of writing powers of 2 as sums of distinct powers of 3, as well as the complementary problem of writing powers of 3 as sums of distinct powers of 2, for several reasons. First, these problems are simply-stated and natural. Second, we wanted to see what we could say about Erdős's conjecture. Third, we were curious how far the modular methods discussed by Brenner and Foster can be pushed, since even modest laptop computers are much more powerful than anything available at the time their paper was written. And finally, we hope to bring these straightforward modular techniques to the attention of the community of mathematicians who are interested in exponential Diophantine equations.

As a historical note, we observe that the solutions to the case $n = 2$ of equations (1) and (2) were determined nearly seven centuries ago by Levi ben Gerson [4], who showed that the only pairs of integers of the form $2^r 3^s$ that differ by 1 are $(1, 2)$, $(2, 3)$, $(3, 4)$, and $(8, 9)$. A paraphrase of ben Gerson's argument, more legible[3] than [4], is given in [11, Appendice, pp. 183–191]. One way to prove ben Gerson's theorem is to observe that every solution to ben Gerson's problem is a solution to the case $n = 2$ of either equation (1) or equation (2), and then to consider those two equations modulo 80.

In 1945, Pillai [18] found all solutions to $\pm(2^x - 3^y) = 2^X + 3^Y$; taking either x or y to be 0 leads to the solutions for the case $n = 3$ of equations (1) and (2).

[2]The statement of the conjecture [7, p. 849] only applies to Diophantine equations with *no* solutions, but later in the paper the authors show how the conjecture, if true, can be applied to equations that have finitely many solutions.

[3]The adjective is chosen with intention. Follow the link in the bibliography to understand why.

Between 2011 and 2013, Bennett, Bugeaud, and Mignotte [5, 6] used linear forms in two logarithms to find all perfect powers whose binary representations have at most four bits equal to 1 (extending a result of Szalay [21] that gives all perfect squares with at most three bits equal to 1), and this solves the case $n = 4$ of equation (1). These are all of the previous solutions to cases of equations (1) and (2) that we are aware of; however, the paper of Bertók and Hajdu [7] discussed earlier includes solutions to many very similar equations, including, for example, finding all powers of 17 that can be expressed as the sum of nine distinct powers of 5. Surely their methods could have been used to solve some more instances of equations (1) and (2).

The structure of this paper is as follows: In Section 2 we briefly review some notation. In Section 3 we observe that in some situations there will necessarily be solutions to equations (1) or (2) modulo M that are not reductions of solutions in the integers, unless some specific conditions on M hold. These conditions shape our strategy of choosing a specific sequence of moduli to use in the proofs of Theorems 1.1 and 1.2. In Section 4 we give examples of two different ways of lifting solutions to (1) modulo M_1 to solutions modulo M_2, suitable for two different circumstances. These examples help clarify the process by which we proved Theorems 1.1 and 1.2. We present the proofs of these theorem in Sections 5 and 6.

The programs we used to complete our calculations were written in Magma [9] and are available as supplementary material attached to the ArXiv version of this paper. They are also available on the second author's web site.

Acknowledgments. We are grateful to Lajos Hajdu for his comments on an earlier version of this paper, and to the anonymous referees for their helpful suggestions.

2. Notation and conventions

In this paper we will often want to count or enumerate the number of solutions to an exponential Diophantine equation modulo M, but there is some natural ambiguity as to what this might mean. For instance, there are infinitely many pairs of integers $x \geq 0$ and $y \geq 0$ for which the congruence $3^x \equiv 2^y + 5 \bmod 28$ holds, but for every such x and y we have $3^x \equiv 9 \bmod 28$ and $2^y \equiv 1 \bmod 28$, so it might not be unreasonable to say that there is only one solution. In order to avoid any confusion, we remove this ambiguity by adopting the following convention.

Convention 2.1. *When we count or enumerate solutions to an exponential Diophantine equation modulo M, we will consider two solutions to be the same if the corresponding terms in the equation are congruent modulo M.*

This means, for example, that for the congruence $3^x \equiv 2^y + 5 \bmod 28$ we consider the solutions $(x, y) = (2, 2)$, $(x, y) = (8, 2)$, and $(x, y) = (8, 5)$ to be the same, because in each case $3^x \equiv 9 \bmod 28$ and $2^y \equiv 4 \bmod 28$.

This convention does have one drawback, which is that for some exponential Diophantine equation modulo M, there truly are only finitely many integer solutions. For example, the only integers $x \geq 0$ and $y \geq 0$ such that $3^x \equiv 2^y + 5 \bmod 216$ are $x = 2$ and $y = 2$. This distinction will in fact be important to us, so we make the following definition.

Definition 2.2. *Let $M > 0$ be an integer and p a prime. We say that a power of p, say p^i, is* determinate *modulo M if the only integer $b \geq 0$ with $p^b \equiv p^i \bmod M$ is $b = i$; otherwise, we say that p^i is an* indeterminate *power of p modulo M.*

Thus, we will say that the congruence $3^x \equiv 2^y + 5 \bmod 28$ has one solution, namely $3^2 \equiv 2^2 + 5 \bmod 28$, but that 3^2 is an indeterminate power of 3 modulo 28 and 2^2 is an indeterminate power of 2 modulo 28. On the other hand, $3^x \equiv 2^y + 5 \bmod 216$ also has only one solution, but the power of 3 and the power of 2 involved are both determinate.

Given a prime p and an integer $M > 0$, we can construct a diagram like diagram (3) of the powers of p modulo M. Note that a determinate power of p modulo M is exactly a power of p that lies on the tail of this diagram, and a straightforward argument shows that for $i \geq 0$, the integer p^i is a determinate power of p modulo M if and only if M is divisible by p^{i+1}.

Recall that if M is a positive integer then the group of units in the ring $\mathbf{Z}/M\mathbf{Z}$ has order $\varphi(M)$, where φ is the Euler φ-function, which can be computed using the formula $\varphi(n) = n\prod_{p|n}(1 - 1/p)$; see [3, §2.3, §2.5]. Also, if M is an odd prime power then the group of units in $\mathbf{Z}/M\mathbf{Z}$ is cyclic [3, Theorem 10.4, p. 207].

For every prime p, we let v_p be the *p-adic valuation* function, so that $v_p(M)$ is the largest x such that p^x divides M. And lastly, we set some notation related to the behavior of the numbers 2 and 3 in finite rings.

Notation 2.3. *Let M be a positive integer and write $M = 2^u 3^v M'$, where $u = v_2(M)$ and $v = v_3(M)$, so that M' is coprime to 6.*

- *We let $O_2(M)$ be the multiplicative order of 2 in the ring $\mathbf{Z}/3^v M'\mathbf{Z}$.*
- *We let $O_2'(M)$ be the multiplicative order of 2 in the ring $\mathbf{Z}/M'\mathbf{Z}$.*
- *We let $O_3(M)$ be the multiplicative order of 3 in the ring $\mathbf{Z}/2^u M'\mathbf{Z}$.*
- *We let $O_3'(M)$ be the multiplicative order of 3 in the ring $\mathbf{Z}/M'\mathbf{Z}$.*

We see, for example, that there are $v_2(M)+O_2(M)$ elements in the tail-and-loop diagram of the powers of 2 modulo M, with $v_2(M)$ in the tail and $O_2(M)$ in the loop. Similarly, there are $v_3(M) + O_3(M)$ elements in the tail-and-loop diagram of the powers of 3 modulo M.

3. Extraneous solutions to congruences

The basic heuristic behind our strategy for solving instances of equations (1) and (2) is that if M is large and there are very few powers of 2 in $\mathbf{Z}/M\mathbf{Z}$ and very few powers of 3 in $\mathbf{Z}/M\mathbf{Z}$, then there should be very few "extraneous" solutions to equations (1) or (2) modulo M — that is, solutions that are not the reduction modulo M of a solution in the integers. If M is divisible by sufficiently high powers of 2 and/or 3, we can hope that every solution modulo M to equation (1) or (2) will involve only determinate powers of 2 or of 3 modulo M (where *determinate* is as defined in Section 2). If this is the case, then each solution will lift uniquely to the integers, if it lifts at all. However, it turns out that for many moduli M, if there is *any* solution to one of these equations, then there is *also* a solution that includes indeterminate powers of 2 and of 3.

For example, we saw in the introduction that if $M_1 = 5440 = 2^6 \cdot 5 \cdot 17$ then the equation $3^x \equiv 2^{a_1} + 2^{a_2} + 2^{a_3} \bmod M_1$ has the three solutions given by (4), (5), and (6), and we see that (6) involves an indeterminate power of 2 (and of 3). If we look at the same equation modulo M_2, where $M_2 = 2M_1 = 2^7 \cdot 5 \cdot 17$, then we find four solutions, including $3^{20} \equiv 2^0 + 2^4 + 2^{14}$, and this involves indeterminate powers of 2 and of 3 modulo M_2. When we look at the same equation modulo M_3, where $M_3 = 41M_2 = 2^7 \cdot 5 \cdot 17 \cdot 41$, there is once again a solution with indeterminate

powers of 2 and 3, namely $3^{20} \equiv 2^0 + 2^4 + 2^{46}$. And the same happens yet again when we work modulo M_4, where $M_4 = 193M_3 = 2^7 \cdot 5 \cdot 17 \cdot 41 \cdot 193$.

And yet in the introduction, when we considered solutions to $3^x \equiv 2^{a_1} + 2^{a_2} + 2^{a_3}$ modulo $2^7 \cdot 5 \cdot 17 \cdot 257$, we did *not* wind up with extraneous solutions. What is the difference between $2^7 \cdot 5 \cdot 17 \cdot 257$ and $2^7 \cdot 5 \cdot 17 \cdot 41 \cdot 193$?

The following proposition, which uses Notation 2.3, explains one way in which solutions with indeterminate powers of 2 or 3 can arise, and suggests a condition that we will want to impose on the moduli we use.

Lemma 3.1. *Let M be a positive integer. Suppose $x > 2$, $y > 0$, and c are integers such that $3^y \equiv c + 2^x \bmod M$. If $O'_3(M)$ is not divisible by 2^{x-1} and $O'_2(M)$ is not divisible by 3^y, then there are integers $x' \geq 0$ and $y' \geq 0$ such that*

(a) $3^{y'} \equiv c + 2^{x'} \bmod M$,
(b) $2^{x'}$ *is an indeterminate power of* 2 *modulo* M, *and*
(c) $3^{y'}$ *is an indeterminate power of* 3 *modulo* M.

Lemma 3.1 shows that in the example we presented in the introduction, it was necessary for us to use a modulus divisible by a prime (in our case, 257) for which either the order of 3 is divisible by 2^5 or the order of 2 is divisible by 3^4. Since $3^4 = 2^0 + 2^4 + 2^6$, if we use a modulus M that is divisible by 2^7 (so that 2^0, 2^4, and 2^6 are determinate powers of 2 modulo M), Lemma 3.1 shows that there will be other, extraneous, solutions modulo M unless M is divisible by such a prime.

Proof of Lemma 3.1. Write $M = 2^u 3^v M'$ where M' is coprime to 6, and set $o_2 = O'_2(M)$ and $o_3 = O'_3(M)$. First we claim that there is an integer s such that $y + so_3 > v$ and $3^{y+so_3} \equiv c \bmod 2^u$.

Suppose $u \leq x$, so that $3^y \equiv c \bmod 2^u$. We know that $3^s \equiv 1 \bmod 2^u$ if s is a multiple of $\varphi(2^u)$, so we can simply take s to be a large enough multiple $\varphi(2^u)$ so that $y + so_3 > v$, and this s meets the conditions of our claim.

Suppose $u > x$. Then M is even, and since c differs from 3^y by a multiple of the even number M, c must be odd. Therefore there is an integer d such that $cd \equiv 1 \bmod 2^u$. Choose such a d and consider the integer $z = 1 + 2^x d$, which is congruent to 1 mod 8 since $x > 2$. If we apply part 1 of Lemma 3.2 (below) to this z, we find that there is an integer e_0, divisible by 2^{x-2}, such that every integer e with $e \equiv e_0 \bmod 2^{u-2}$ satisfies $3^e \equiv 1 + 2^x d \bmod 2^u$. By assumption, the highest power of 2 that divides o_3 is at most 2^{x-2}. Therefore there is an integer s such that $so_3 \equiv -e_0 \bmod 2^{u-2}$, and we can choose such an s that is large enough so that $y + so_3 > v$.

We have $3^{-so_3} \equiv 1 + 2^x d \bmod 2^u$. Multiplying both sides of this congruence by $c\,3^{so_3}$ gives $c \equiv (c + 2^x)3^{so_3} \bmod 2^u$, and since $c + 2^x \equiv 3^y \bmod M$ and hence also modulo 2^u, we find that $c \equiv 3^{y+so_3} \bmod 2^u$. Thus, this s has the properties we desire, and we have proven our claim.

Similarly, using part 2 of Lemma 3.2, we can show that there is an integer r such that $x + ro_2 > u$ and $2^{x+ro_2} \equiv -c \bmod 3^v$.

Let $x' = x + ro_2$ and let $y' = y + so_3$. We claim that this x' and y' satisfy conditions (a), (b), and (c) from the lemma. It is easy to check conditions (b) and (c) because $x' > u$ and $y' > v$ by construction. To check condition (a), we use the Chinese Remainder Theorem: It suffices to check that $3^{y'} \equiv c + 2^{x'}$ modulo M', modulo 2^u, and modulo 3^v.

We have $2^{o_2} \equiv 1 \bmod M'$ and $3^{o_3} \equiv 1 \bmod M'$ by the definitions of o_2 and o_3, so $3^{y'} \equiv 3^y \bmod M'$ and $2^{x'} \equiv 2^x \bmod M'$, and we have $3^{y'} \equiv c + 2^{x'} \bmod M'$.

We have $2^{x'} \equiv 0 \bmod 2^u$ because $x + ro_2 > u$ by construction. Since $3^{y'} \equiv 3^{y+so_3} \equiv c \bmod 2^u$, we have $3^{y'} \equiv c + 2^{x'} \bmod 2^u$.

Likewise, we have $3^{y'} \equiv 0 \bmod 3^v$, and since $2^{x'} \equiv 2^{x+ro_2} \equiv -c \bmod 3^v$, we have $3^{y'} \equiv c + 2^{x'} \bmod 3^v$. This shows that condition (a) holds for this x' and y', and completes the proof of the lemma. □

Lemma 3.2.

(1) *Let z be an integer with $z \equiv 1 \bmod 8$. For every integer $u \geq 3$ there is an integer e_0 such that the integers e that satisfy $3^e \equiv z \bmod 2^u$ are precisely the integers e that satisfy $e \equiv e_0 \bmod 2^{u-2}$. If $x \leq u$ is an integer with $z \equiv 1 \bmod 2^x$, then e_0 is divisible by 2^{x-2}.*

(2) *Let z be an integer with $z \equiv 1 \bmod 3$. For every integer $v \geq 1$ there is an integer e_0 such that the integers e that satisfy $2^e \equiv z \bmod 3^v$ are precisely the integers e that satisfy $e \equiv e_0 \bmod 2 \cdot 3^{v-1}$. If $y \leq v$ is an integer with $z \equiv 1 \bmod 3^y$, then e_0 is divisible by $2 \cdot 3^{y-1}$.*

Proof. For statement 1: We leave the reader to show that for every $u \geq 3$, the order of 3 modulo 2^u is 2^{u-2}. (The proof can be modeled after the proof of [3, Theorem 10.11, p. 218].) Since there are 2^{u-1} units in $\mathbf{Z}/2^u\mathbf{Z}$, and the order of 3 is half of this, it follows that half of the units are powers of 3. A power of 3 is never congruent to 5 or 7 modulo 8, and this accounts for half of the units. Therefore, every unit that is 1 or 3 modulo 8 is a power of 3. Thus, there is an e_0 such that $3^{e_0} \equiv z$. The fact that $3^e \equiv z \bmod 2^u$ if and only if $e \equiv e_0 \bmod 2^{u-2}$ is simply a consequence of the fact that the order of 3 modulo 2^u is 2^{u-2}.

If $z \equiv 1 \bmod 2^x$ with $x \leq u$, then $3^{e_0} \equiv 1 \bmod 2^x$, so e_0 is a multiple of the order of 3 modulo 2^x, and hence e_0 is divisible by 2^{x-2}.

The proof of statement 2 is analogous, and we leave it to the reader. □

When we look at cases of equation (1) with larger values of n, we will find that Lemma 3.1 tells us that we will need to include information gleaned from moduli divisible by primes p such that the order of 3 modulo p is divisible by quite large powers of 2. In Section 5 we show how we can work our way up to such moduli.

4. Lifting solutions

Our proofs of Theorems 1.1 and 1.2 are computational. In each proof, we consider a sequence of moduli $M_1, M_2, \ldots$, each dividing the next. Roughly speaking, we first compute the solutions to equation (1) or (2) modulo M_1; then for each $i > 1$ in turn we "lift" the solutions modulo M_{i-1} to solutions modulo M_i. We stop when we have reached an M_i where all of the summands that appear on the right-hand side of the solutions modulo M_i are determinate (in the sense defined in Section 2); at that point, each solution modulo M_i can be lifted uniquely to a solution in the integers, if it lifts to a solution at all.

This strategy depends on our having efficient methods for lifting a solution modulo M_{i-1} to a solution modulo M_i. In Section 5 we will spell out our methods more formally, but in this section we would like to give two examples to help make the methods more clear. For the sake of exposition, we will focus on finding solutions

to equation (1) modulo M for various M, and as we did in the introduction, we will ignore the requirement that the summands be distinct.

As an example of one extreme case of the lifting problem, let $M_1 = 439$ and let $n = 12$ and consider the following solution to equation (1) modulo M_1:

$$3^{57} \equiv 2^0 + 2^1 + 2^{11} + 2^{12} + 2^{15} + 2^{16} + 2^{26} + 2^{27} + 2^{37} + 2^{57} + 2^{65} + 2^{68}. \tag{7}$$

Let p be the prime 9361973132609 and let $M_2 = pM_1$. We will try to find a lift of the solution (7) to a solution modulo M_2. We compute that the graph of the powers of 2 modulo M_1 forms a loop of cycle length 73 with no tail… and we compute that the graph of powers of 2 modulo M_2 is *also* a tailless loop of cycle length 73. That means that there is *exactly one* power of 2 in $\mathbf{Z}/M_2\mathbf{Z}$ that reduces to a given power of 2 in $\mathbf{Z}/M_1\mathbf{Z}$. If we can lift equation (7) to a solution modulo M_2, then the right-hand side of the lifted solution will have to be

$$2^0 + 2^1 + 2^{11} + 2^{12} + 2^{15} + 2^{16} + 2^{26} + 2^{27} + 2^{37} + 2^{57} + 2^{65} + 2^{68} \bmod M_2.$$

If we let z be this sum, then to determine whether there is a lift of equation (7) to a solution modulo M_2, we simply have to determine whether there is an x such that $3^x \equiv z \bmod M_2$.

It turns out that the graph of powers of 3 modulo M_2 is a tailless loop with cycle length $p - 1 = 9361973132608$, so we definitely do *not* want to find x (if it exists) by enumeration. Instead, we can find x by using discrete logarithms.

If there is an x with $3^x \equiv z \bmod M_2$, then that same x satisfies $3^x \equiv z \bmod p$ for the prime $p = M_2/M_1$. We can find an x that satisfies this congruence if and only if $z \in (\mathbf{Z}/p\mathbf{Z})^*$ lies in the subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$ generated by 3. Using the computer algebra package Magma, we find that in fact 3 generates the whole group of units, and Magma very quickly computes a discrete logarithm of z with respect to 3 — that is, an integer x with $3^x \equiv z \bmod p$. In fact, every integer x satisfying

$$x \equiv 3976447101915 \bmod (p - 1) \tag{8}$$

will give a solution to this congruence.

In order for x to give a solution modulo M_2, we also need to have $3^x \equiv z \bmod M_1$. The graph of powers of 3 modulo M_1 is a tailless loop with cycle length 146, and we find that for x to solve this congruence modulo M_1 we need to have $x \equiv 57 \bmod 146$.

But 146 is a divisor of $p - 1$, and reducing equation (8) modulo 146, we find that it becomes $x \equiv 31 \bmod 146$. This is incompatible with the congruence from the preceding paragraph, so there is no x with $3^x \equiv z \bmod M_2$. This shows that equation (7) cannot be lifted to a solution modulo M_2.

Let us turn to another example, which demonstrates a different approach to the lifting problem. We again take $M_1 = 439$ and start with the solution to equation (1) modulo M_1 given by (7). This time, however, we take $p = 1753$ and $M_2 = pM_1$. We will try to find a lift of the solution (7) to a solution modulo M_2.

The graph of powers of 2 modulo M_2 is a tailless loop of cycle length 146, which is exactly twice as long as the cycle of powers of 2 modulo M_1. That means that there are *exactly two* powers of 2 modulo M_2 that reduce to a given power of 2 modulo M_1. In particular, the two lifts to $\mathbf{Z}/M_2\mathbf{Z}$ of the element $2^i \in \mathbf{Z}/M_1\mathbf{Z}$ are 2^i and 2^{i+73}.

Similarly, we can also compute that there are six lifts of $3^{57} \in \mathbf{Z}/M_1\mathbf{Z}$ to powers of 3 in $\mathbf{Z}/M_2\mathbf{Z}$, namely 3^{57}, 3^{203}, 3^{349}, 3^{495}, 3^{641}, and 3^{787}.

We see that every summand on the right-hand side of (7) has two lifts to $\mathbf{Z}/M_2\mathbf{Z}$, and the left-hand side has six lifts. In principle, we could compute all $6 \cdot 2^{12} = 24{,}576$ lifts of the terms appearing in (7) and check to see which combinations of lifts give us an equality modulo M_2, but this would be inefficient… and for larger values of n, it would become more and more inefficient.

Instead, we use a "meet in the middle" technique. We rewrite equation (7) to get the following congruence modulo M_1:

$$3^{57} - 2^0 - 2^1 - 2^{11} - 2^{12} - 2^{15} \equiv 2^{16} + 2^{26} + 2^{27} + 2^{37} + 2^{57} + 2^{65} + 2^{68}. \tag{9}$$

There are $6 \cdot 2^5 = 192$ lifts to $\mathbf{Z}/M_2\mathbf{Z}$ of the terms appearing on the left-hand side of (9), and $2^7 = 128$ lifts of the terms on the right-hand side. We compute the values (modulo M_2) of all of the left-hand lifts, and the values of all of the right-hand lifts, and then compare the two lists to see whether there are any values in common. (We can quickly find these common values if we sort each list first.) Each such common value w gives us one (or more) lifts to $\mathbf{Z}/M_2\mathbf{Z}$ of (9), and hence also of (7). And clearly, all solutions to (1) modulo M_2 that are lifts of (7) will arise in this way. In point of fact, for this particular example we found eight values of w, from which we obtained eight solutions to (1) in $\mathbf{Z}/M_2\mathbf{Z}$ that were lifts of (7).

The two techniques we have demonstrated here for lifting solutions of (1) modulo M_1 to solutions modulo M_2 are the basis for the procedure for proving Theorem 1.1 that we sketch in the following section.

5. Proof of Theorem 1.1

To prove Theorem 1.1 we consider a sequence of moduli M_i, where $M_i = \prod_{j \le i} m_i$ for the factors $m_1, \ldots, m_{64}$ listed in Table 5, so that each M_i divides the next. As we explained in Section 4, roughly speaking we first compute the solutions to equation (1) in $\mathbf{Z}/M_1\mathbf{Z}$; then, using the ideas sketched out in the examples in Section 4, we lift the solutions to $\mathbf{Z}/M_2\mathbf{Z}$, then to $\mathbf{Z}/M_3\mathbf{Z}$, then to $\mathbf{Z}/M_4\mathbf{Z}$, and so on, stopping when we have reached an M_i where all of the powers of 2 that appear in the solutions are determinate. If all the powers of 2 in a solution are determinate, the solution can be lifted uniquely to a solution in the integers, if it lifts to a solution at all.

To be more precise: For a given i, we write $M_i = 2^{u_i} 3^{v_i} M_i'$ where M_i' is coprime to 6. As we noted in Section 2, there are $u_i + O_2(M_i)$ distinct powers of 2 modulo M_i, and $v_i + O_3(M_i)$ distinct powers of 3. For each M_i in turn, we set $M = M_i$ and compute the solutions $(x, a_1, \ldots, a_n)$ to

$$\begin{cases} 3^x \equiv 2^{a_1} + \cdots + 2^{a_n} \bmod M \\ 0 \le x < v + O_3(M) \\ 0 = a_1 \le \cdots \le a_n < u + O_2(M), \end{cases} \tag{10}$$

with the added condition that for every pair (j, k) of indices with $j \ne k$, if a_j and a_k are both less than u_i, then $a_j \ne a_k$. This last condition reflects the fact that if $a < u_i$, then 2^a is a determinate power of 2 in $\mathbf{Z}/M_1\mathbf{Z}$, and the right-hand side exponents in the solutions to equation (1) are required to be distinct. (Note that the upper bounds given in (10) have the effect of keeping us in line with Convention 2.1.)

For $M_1 = 2^4 \cdot 7 \cdot 73$ we compute the solutions to (10) by brute force. The powers of 2 in $\mathbf{Z}/M_1\mathbf{Z}$ are 2^0 through 2^{12}. To every n-tuple $(a_1, \ldots, a_n)$ of exponents between

TABLE 2. Data for the factors m_i and the moduli $M_i = \prod_{j \le i} m_j$ used in the proof of Theorem 1.1. The notation in the table headings is as in Notation 2.3.

i	m_i	$O_2(m_i)$	$O_2(M_i)$	$O_3'(m_i)$	$v_2(O_3'(M_i))$	i	m_i	$O_2(m_i)$	$O_2(M_i)$	$O_3'(m_i)$	$v_2(O_3'(M_i))$
1	$2^4 \cdot 7 \cdot 73$	3^2	3^2	$3 \cdot 2^2$	2	32	113246209	$2^{20} \cdot 3^2$	$2^{20} \cdot 3^2$	$27 \cdot 2^{19}$	20
2	$3^3 \cdot 19$	$2 \cdot 3^2$	$2 \cdot 3^2$	$9 \cdot 2^1$	2	33	319489	$2^{12} \cdot 3^0$	$2^{20} \cdot 3^2$	$39 \cdot 2^8$	20
3	$5 \cdot 13 \cdot 37 \cdot 109$	$2^2 \cdot 3^2$	$2^2 \cdot 3^2$	$27 \cdot 2^2$	2	34	1084521185281	$2^{21} \cdot 3^2$	$2^{21} \cdot 3^2$	$43095 \cdot 2^{22}$	22
4	$241 \cdot 433$	$2^3 \cdot 3^2$	$2^3 \cdot 3^2$	$135 \cdot 2^3$	3	35	2^2	—	$2^{21} \cdot 3^2$	—	22
5	17	$2^3 \cdot 3^0$	$2^3 \cdot 3^2$	2^4	4	36	7348420609	$2^{22} \cdot 3^1$	$2^{22} \cdot 3^2$	$73 \cdot 2^{24}$	24
6	2^2	—	$2^3 \cdot 3^2$	—	4	37	2^2	—	$2^{22} \cdot 3^2$	—	24
7	38737	$2^3 \cdot 3^2$	$2^3 \cdot 3^2$	$2421 \cdot 2^3$	4	38	448203325441	$2^{23} \cdot 3^1$	$2^{23} \cdot 3^2$	$26715 \cdot 2^{21}$	24
8	$97 \cdot 577$	$2^4 \cdot 3^2$	$2^4 \cdot 3^2$	$3 \cdot 2^4$	4	39	1107296257	$2^{24} \cdot 3^1$	$2^{24} \cdot 3^2$	$11 \cdot 2^{22}$	24
9	$257 \cdot 673$	$2^4 \cdot 3^1$	$2^4 \cdot 3^2$	$21 \cdot 2^8$	8	40	167772161	$2^{24} \cdot 3^0$	$2^{24} \cdot 3^2$	$5 \cdot 2^{25}$	25
10	2^4	—	$2^4 \cdot 3^2$	—	8	41	2	—	$2^{24} \cdot 3^2$	—	25
11	$193 \cdot 1153$	$2^5 \cdot 3^2$	$2^5 \cdot 3^2$	$9 \cdot 2^6$	8	42	74490839041	$2^{26} \cdot 3^1$	$2^{26} \cdot 3^2$	$185 \cdot 2^{26}$	26
12	6337	$2^5 \cdot 3^2$	$2^5 \cdot 3^2$	$99 \cdot 2^4$	8	43	2	—	$2^{26} \cdot 3^2$	—	26
13	65537	$2^5 \cdot 3^0$	$2^5 \cdot 3^2$	2^{16}	16	44	246423748609	$2^{26} \cdot 3^1$	$2^{26} \cdot 3^2$	$27 \cdot 2^{28}$	28
14	2^8	—	$2^5 \cdot 3^2$	—	16	45	2^2	—	$2^{26} \cdot 3^2$	—	28
15	641	$2^6 \cdot 3^0$	$2^6 \cdot 3^2$	$5 \cdot 2^7$	16	46	29796335617	$2^{27} \cdot 3^1$	$2^{27} \cdot 3^2$	$111 \cdot 2^{24}$	28
16	769	$2^7 \cdot 3^1$	$2^7 \cdot 3^2$	$3 \cdot 2^4$	16	47	3221225473	$2^{28} \cdot 3^1$	$2^{28} \cdot 3^2$	2^{27}	28
17	274177	$2^7 \cdot 3^0$	$2^7 \cdot 3^2$	$153 \cdot 2^5$	16	48	77309411329	$2^{29} \cdot 3^1$	$2^{29} \cdot 3^2$	2^{30}	30
18	18433	$2^8 \cdot 3^2$	$2^8 \cdot 3^2$	$9 \cdot 2^9$	16	49	2^2	—	$2^{29} \cdot 3^2$	—	30
19	101377	$2^9 \cdot 3^2$	$2^9 \cdot 3^2$	$99 \cdot 2^9$	16	50	5469640851457	$2^{30} \cdot 3^1$	$2^{30} \cdot 3^2$	$849 \cdot 2^{30}$	30
20	2424833	$2^{10} \cdot 3^0$	$2^{10} \cdot 3^2$	$37 \cdot 2^{16}$	16	51	28114855919617	$2^{31} \cdot 3^1$	$2^{31} \cdot 3^2$	$3273 \cdot 2^{30}$	30
21	12289	$2^{11} \cdot 3^1$	$2^{11} \cdot 3^2$	2^9	16	52	1095981164658689	$2^{31} \cdot 3^0$	$2^{31} \cdot 3^2$	$127589 \cdot 2^{33}$	33
22	974849	$2^{12} \cdot 3^0$	$2^{12} \cdot 3^2$	$119 \cdot 2^{13}$	16	53	2^3	—	$2^{31} \cdot 3^2$	—	33
23	114689	$2^{13} \cdot 3^0$	$2^{13} \cdot 3^2$	$7 \cdot 2^{14}$	16	54	87211	$2 \cdot 3^3$	$2^{31} \cdot 3^3$	$2907 \cdot 2^0$	33
24	39714817	$2^{14} \cdot 3^1$	$2^{14} \cdot 3^2$	$101 \cdot 2^{12}$	16	55	5566277615617	$2^{32} \cdot 3^3$	$2^{32} \cdot 3^3$	$3 \cdot 2^{32}$	33
25	1179649	$2^{15} \cdot 3^2$	$2^{15} \cdot 3^2$	$9 \cdot 2^{16}$	16	56	25048249270273	$2^{33} \cdot 3^3$	$2^{33} \cdot 3^3$	$81 \cdot 2^{34}$	34
26	7908360193	$2^{15} \cdot 3^2$	$2^{15} \cdot 3^2$	$419 \cdot 2^{20}$	20	57	2	—	$2^{33} \cdot 3^3$	—	34
27	2^4	—	$2^{15} \cdot 3^2$	—	20	58	942556342910977	$2^{34} \cdot 3^3$	$2^{34} \cdot 3^3$	$1143 \cdot 2^{37}$	37
28	171048961	$2^{16} \cdot 3^2$	$2^{16} \cdot 3^2$	$1305 \cdot 2^{15}$	20	59	2^3	—	$2^{34} \cdot 3^3$	—	37
29	786433	$2^{17} \cdot 3^1$	$2^{17} \cdot 3^2$	2^{16}	20	60	206158430209	$2^{35} \cdot 3^1$	$2^{35} \cdot 3^3$	2^{33}	37
30	14155777	$2^{18} \cdot 3^2$	$2^{18} \cdot 3^2$	$27 \cdot 2^{18}$	20	61	2748779069441	$2^{37} \cdot 3^0$	$2^{37} \cdot 3^3$	$5 \cdot 2^{39}$	39
31	13631489	$2^{19} \cdot 3^0$	$2^{19} \cdot 3^2$	2^{20}	20	62	2^2	—	$2^{37} \cdot 3^3$	—	39

0 and 12 with $0 = a_1 \le \cdots \le a_n$, we can associate the 13-tuple $(b_0, \ldots, b_{12})$, where b_i is the number of a_j that are equal to i. Then instead of enumerating all of the n-tuples $(a_1, \ldots, a_n)$, we can simply run through all of the 13-tuples $(b_0, \ldots, b_{12})$ of non-negative integers such that

$$b_0 + \cdots + b_{12} = n$$

and

$$b_0 = 1, \quad b_1 \le 1, \quad b_2 \le 1, \quad \text{and } b_3 \le 1.$$

When we find such a 13-tuple with the additional property that $\sum b_j 2^j$ is congruent to 3^x modulo M_1 for one of the 12 powers of 3 modulo M_1, we can compute the associated n-tuple $(a_1, \ldots, a_n)$ and add $(x, a_1, \ldots, a_n)$ to our list of solutions of equation (10) with $M = M_1$. We obtain all solutions to the equation in this way.

Now suppose we have a list of solutions to (10) with $M = M_{i-1}$, and we want to create the list of solutions with $M = M_i$, where $M_i = m_i M_{i-1}$. Write $M_i = 2^{u_i} 3^{v_i} M_i'$ with M_i' coprime to 6. For each solution $(x, a_1, \ldots, a_n)$ to the problem modulo M_{i-1}, we go through the following steps.

Step one: *Compute the powers of* 2 *in* $\mathbf{Z}/M_i\mathbf{Z}$ *that lift the* $2^{a_j} \in \mathbf{Z}/M_{i-1}\mathbf{Z}$.

For each $j = 1, \ldots, n$, we compute a list A_j of the values of a' with $0 \le a' < u_i + O_2(M_i)$ such that $2^{a'} \equiv 2^{a_j} \bmod M_{i-1}$.

Step two: *Compute the number of powers of* 3 *in* $\mathbf{Z}/M_i\mathbf{Z}$ *that lift* $3^x \in \mathbf{Z}/M_{i-1}\mathbf{Z}$.

Let χ denote the number of values of x' with $0 \le x' < v_i + O_3(M_i)$ such that $3^{x'} \equiv 3^x \bmod M_{i-1}$. If 3^x is a determinate power of 3 modulo M_{i-1}, then $\chi = 1$. If 3^x is an indeterminate power of 3 modulo M_i, then $\chi = O_3(M_i)/O_3(M_{i-1})$. And if 3^x is indeterminate modulo M_{i-1} but determinate modulo M_i, then $\chi = 1 + O_3(M_i)/O_3(M_{i-1})$.

Step three: *Compute the lifted solutions.*

We compute lifted solutions in one of two ways; to decide between the two methods, we check to see whether $\chi > \prod_{j=1}^n \#A_j$ and whether m_i is a prime that does not divide $6M_{i-1}$. If both these conditions hold, we say we are in the *unbalanced* case, and if not we say we are in the *balanced* case.

(1) *The unbalanced case.* In this case we must have $\chi > 1$, so 3^x is an indeterminate power of 3 modulo M_{i-1}; also, in this case we have $v_i = v_{i-1}$ because $m_i \ne 3$. We proceed as follows, for each n-tuple $(a_1', \ldots, a_n')$ in $A_1 \times \cdots \times A_n$:
   (a) *Compute the right-hand side sum.* Set $s := \sum_j 2^{a_j'}$.
   (b) *Check to see whether the right-hand side sum is a power of* 3 *modulo* M_i. To check to see whether there is a power of 3, say $3^{x'}$, with $3^{x'} \equiv s \bmod M_i$, we use discrete logarithms as follows.

   Let g be a generator of the group of units of $(\mathbf{Z}/m_i\mathbf{Z})^*$, let z be the smallest non-negative integer with $g^z \equiv s \bmod m_i$, and let y be the smallest positive integer with $g^y \equiv 3 \bmod m_i$, so that z and y are discrete logarithms of s and of 3 with respect to the base g. If there is an x' such that $3^{x'} \equiv s \bmod M_i$, then for this x' we have $3^{x'} \equiv s \bmod m_i$, so we must have $x'y \equiv z \bmod (p-1)$; for this x' we have $3^{x'} \equiv s \bmod 2^{v_i - 1} M_{i-1}$, so we must have $x' \equiv x \bmod O_3(M_{i-1})$; and for this x' we have $3^{x'} \equiv 3^x \equiv 0 \bmod 3^{v_i}$, so we must have $x' \ge v_i$.

Conversely, any x' that satisfies these three conditions will also satisfy $3^{x'} \equiv s \bmod M_i$.

For primes m_i of the size we are considering, the computation of the discrete logarithms z and y is easily done by the computer algebra package Magma, in which we have written our code. It is also a straightforward matter to compute the values of x' that meet the three conditions, if any exist.

For each x' that we find, we add $(x', a'_1, \dots, a'_n)$ to our list of solutions of equation (10) with $M = M_i$.

The time required to carry out this step is proportional to the number of n-tuples $(a'_1, \dots, a'_n)$ that we have to consider, which is $\prod \#A_i$.

(2) *The balanced case.* We proceed as follows.

(a) *Compute the left-hand side lifts.* We compute the set X of the values of x' with $0 \le x' < v_i + O_3(M_i)$ such that $3^{x'} \equiv 3^x \bmod M_{i-1}$.

(b) *Group the variables into two balanced sets.* Compute the value of k so that the product $\#X \cdot \prod_{j \le k} \#A_j$ and the product $\prod_{j>k} \#A_j$ are as close in size as possible.

(c) *Compute the lifts of the variables in each grouping.* We make two lists. The first is the list of all $(k+2)$-tuples

$$(3^{x'} - 2^{a'_1} - \cdots - 2^{a'_k}, x', a'_1, \dots, a'_k)$$

for all $(x', a'_1, \dots, a'_k) \in X \times A_1 \times \cdots \times A_k$, where we view the first entry of the tuple as an element of $\mathbf{Z}/M_i\mathbf{Z}$. The second is the list of all $(n-k+1)$-tuples

$$(2^{a'_{k+1}} + \cdots + 2^{a'_n}, a'_{k+1}, \dots, a'_n)$$

for all $(a'_{k+1}, \dots, a'_n) \in A_{k+1} \times \cdots \times A_n$, where again we view the first entry as an element of $\mathbf{Z}/M_i\mathbf{Z}$.

(d) *Compare the lists for matching values.* Sort each of these lists according to the value of the first entry of each tuple, and then compare the two sorted lists to find all pairs of elements, one from the first list and one from the second, whose first entries are equal. Every such pair gives us a solution to

$$3^{x'} \equiv 2^{a'_1} + \cdots + 2^{a'_n} \text{ in } \mathbf{Z}/M_i\mathbf{Z}$$

that reduces to our original solution in $\mathbf{Z}/M_{i-1}\mathbf{Z}$. Add each such solution to our list of solutions of equation (10) with $M = M_i$.

The time it takes to carry out this step is proportional to the larger of $\#X \cdot \prod_{j \le k} \#A_j$ and $\prod_{j>k} \#A_j$. If these two numbers are somewhat balanced, the time required for this step will be roughly proportional to the square root of $\#X \cdot \prod_{j \le n} \#A_j$.

Once we have computed all of the solutions to equation (10) with $M = M_i$ by this method, we check to see whether all of the powers of 2 that occur anywhere on our list are determinate. If they are not, then we increase i by 1 and iterate the procedure. If they are, then for each solution to (10) with $M = M_i$, we can check to see whether the (unique) lifts of the terms in the right-hand side of (10) to powers of 2 in $\mathbf{Z}$ add up to a power of 3. In this way, we hope to find all solutions to (1).

TABLE 3. For each n, we list the value of i such that our procedure for solving equation (1) iterated up to the modulus M_i from Table 5. We also give the wall-clock time it took for the computation to complete on a 2.8 GHz Quad-Core Intel Core i7 with 16GB RAM running Magma V2.23-1 on Mac OS 11.2.3. For $n \geq 20$ the computation was split into parts that were run by separate processes; the time given is the sum of the wall-clock times for each process.

n	i	Time (sec)	n	i	Time (sec)
3	10	0.01	13	37	19
4	10	0.02	14	45	52
5	14	0.04	15	45	145
6	14	0.07	16	59	457
7	14	0.14	17	59	1469
8	14	0.29	18	62	5746
9	14	0.62	19	62	17744
10	27	1.54	20	62	53617
11	37	3.81	21	62	139347
12	37	8.03	22	62	743737

Proof of Theorem 1.1. We ran through the procedure described above for all values of n from 3 to 22. For each n, the procedure did terminate before we ran out of values of M_i, so we successfully found all solutions to equation (1) for $n \leq 22$. We found that the binary representation of 3^x has at most twenty-two bits equal to 1 exactly when $x \leq 25$. □

In Table 5, we give for each n the value of i for which the modulus M_i gave us all solutions to the equation. We also give the total time for the computation. As mentioned earlier, the programs we used to implement this computation were written in Magma and are available as supplementary material attached to the ArXiv version of this paper, as well as on the second author's web site.

The procedure we described in the proof of Theorem 1.1 suggests the properties we looked for when choosing the factors m_i out of which our moduli M_i are built. In the balanced case, we want the sets A_j to be as small as possible, since the work in the balanced case is roughly on the order of the square root of the product $\#X \cdot \prod_{j \leq n} \#A_j$. Of course, we'd like $\#X$ to be small as well, but since there are n sets A_j we concentrate first on them.

For a given solution $(x, a_1, \ldots, a_n)$ to (10) with $M = M_{i-1}$, how large are the A_j? The answer is analogous to the computation of the value of χ given in Step Two of our procedure. Suppose we are in the case where m_i is odd. If 2^{a_j} is a determinate power of 2 modulo M_{i-1}, then $\#A_j = 1$. If 2^{a_j} is indeterminate modulo M_{i-1}, then it is indeterminate modulo M_i as well because m_i is odd, and we have $\#A_j = O_2(M_i)/O_2(M_{i-1})$. If m_i is coprime to M_{i-1}, which is the case for all of the values we chose, then $O_2(M_i)$ is the least common multiple of $O_2(m_i)$ and $O_2(M_{i-1})$.

The ideal case would be for $O_2(m_i)$ to be a divisor of $O_2(M_{i-1})$, so that the ratio $O_2(M_i)/O_2(M_{i-1})$ would be 1. The next-best case would be for $O_2(m_i)$ to divide $2O_2(M_{i-1})$ but not $O_2(M_{i-1})$, so that $O_2(M_i)/O_2(M_{i-1})$ would be 2. We

were able to stay in these two cases for every i with m_i odd, except for $i = 54$, where we have $O_2(M_i)/O_2(M_{i-1}) = 3$.

For those i for which $O_2(M_i)/O_2(M_{i-1}) = 1$, we can focus more on the unbalanced case. These i give us the opportunity to build up the number of powers of 2 in $O_3'(M_i)$. For example, for $i = 13$ we have $O_2(M_i)/O_2(M_{i-1}) = 1$, and with the value of m_i that we chose, we increase the 2-part of the order of 3 from 2^8 in $O_3'(M_{i-1})$ to 2^{16} in $O_3'(M_i)$.

We found our m_i mostly by looking for primes p congruent to 1 modulo $2^a 3^b$ for various values of a and b, and computing the orders of 2 and 3 in $(\mathbf{Z}/p\mathbf{Z})^*$.

We make one final note about our choice of the m_i. We would also like the number of solutions we have to consider at any given stage to be small. This becomes especially critical for the larger values of n that we consider. Our choices for m_i, especially for small i, reflect this. For example, we have chosen m_4 to be $241 \cdot 433$, which puts us in the balanced case with $\#A_j = 2$ for most j and with $\#X = 10$. After this m_4, we have $m_5 = 17$, $m_6 = 2^2$, and $m_7 = 38737$. For smaller values of n, it turns out that it would be faster to take $m_4 = 433$ (which gives us $\#X = 1$), $m_5 = 17$, $m_6 = 2^2$, and then to add in a factor of 241 before moving on to $m_7 = 38737$. According to the heuristic mentioned in Step **??**, the time it takes to process a solution in the balanced case is very roughly proportional to $(\#X \cdot \prod_{j \le n} \#A_j)^{1/2}$, so having $\#X$ equal to 1 instead of 10 should speed up this step by a factor of about $\sqrt{10}$. But for large n, this improved speed for $i = 4$ would be outweighed by the extra time it would take to process the large number of solutions that would make it through to the next step. To simplify our exposition, we have simply given one single sequence of m_i to use for all n, optimized for large values of n, even though different choices would have made the program run faster for smaller n.

6. Proof of Theorem 1.2

The proof of Theorem 1.2 is also computational, and is essentially the same as that of Theorem 1.1. The sequence of moduli we use is given in Table 6, and the time it took to run our program for n up to 24 is given in Table 6. The only other comment we make here is that if n is odd and greater than 1, then there are no solutions to equation (2), because no power of 2 (other than 1) can be written as the sum of an odd number of powers of 3. □

References

[1] Zsolt Ádám, Lajos Hajdu, and Florian Luca, *Representing integers as linear combinations of S-units*, Acta Arith. **138** (2009), no. 2, 101–107. MR 2520130

[2] Leo J. Alex, *Diophantine equations related to finite groups*, Comm. Algebra **4** (1976), no. 1, 77–100. MR 424675

[3] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976, Undergraduate Texts in Mathematics. MR 0434929

[4] Levi ben Gerson [Magistri Leonis Hebraei], *De numeris harmonicis*, Scripta diversa super scientiam mathematicam et physicam, 14th century, Bibliothèque nationale de France, Département des manuscrits, Latin 7378A, pp. 55v–57r.

[5] Michael A. Bennett, Yann Bugeaud, and Maurice Mignotte, *Perfect powers with few binary digits and related Diophantine problems*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **12** (2013), no. 4, 941–953. MR 3184574

[6] ———, *Perfect powers with few binary digits and related Diophantine problems, II*, Math. Proc. Cambridge Philos. Soc. **153** (2012), no. 3, 525–540. MR 2990629

TABLE 4. Data for the factors m_i and the moduli $M_i = \prod_{j \le i} m_j$ used in the proof of Theorem 1.2. The notation in the table headings is as in Notation 2.3.

i	m_i	$O_3(m_i)$	$O_3(M_i)$	$O_2'(m_i)$	$v_3(O_2'(M_i))$
1	$2 \cdot 3^4 \cdot 13 \cdot 757$	3^2	3^2	$28 \cdot 3^3$	3
2	$7 \cdot 19 \cdot 37$	$2 \cdot 3^2$	$2 \cdot 3^2$	$4 \cdot 3^2$	3
3	$5 \cdot 73$	$2^2 \cdot 3$	$2^2 \cdot 3^2$	$4 \cdot 3^2$	3
4	530713	$2^2 \cdot 3^2$	$2^2 \cdot 3^2$	$91 \cdot 3^6$	6
5	3^3	—	$2^2 \cdot 3^2$	—	6
6	$41 \cdot 6481$	$2^3 \cdot 3$	$2^3 \cdot 3^2$	$20 \cdot 3^4$	6
7	282429005041	$2^3 \cdot 3^2$	$2^3 \cdot 3^2$	$66430 \cdot 3^{12}$	12
8	3^6	—	$2^3 \cdot 3^2$	—	12

TABLE 5. For each n, we list the value of i such that our procedure for solving equation (2) iterated up to the modulus M_i from Table 6. We also give the wall-clock time it took for the computation to complete on a 2.8 GHz Quad-Core Intel Core i7 with 16GB RAM running Magma V2.23-1 on Mac OS 11.2.3.

n	i	Time (sec)	n	i	Time (sec)
4	5	0.01	16	8	14
6	5	0.01	18	8	84
8	5	0.07	20	8	789
10	8	0.23	22	8	9792
12	8	0.92	24	8	140036
14	8	3.44			

[7] Csanád Bertók and Lajos Hajdu, *A Hasse-type principle for exponential Diophantine equations and its applications*, Math. Comp. **85** (2016), no. 298, 849–860. MR 3434884

[8] ———, *A Hasse-type principle for exponential Diophantine equations over number fields and its applications*, Monatsh. Math. **187** (2018), no. 3, 425–436. MR 3858424

[9] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). Software available at `http://magma.maths.usyd.edu.au/`. MR 1484478

[10] Joel Lee Brenner and Lorraine L. Foster, *Exponential Diophantine equations*, Pacific J. Math. **101** (1982), no. 2, 263–301. MR 675401

[11] Karine Chemla and Serge Pahaut, *Remarques sur les ouvrages mathématiques de Gersonide*, Studies on Gersonides — A Fourteenth-Century Jewish Philosopher-Scientist (G. Freudenthal, ed.), Collection de Travaux de l'Académie Internationale d'Histoire des Sciences, vol. 36, E. J. Brill, Leiden, 1992, pp. 149–191.

[12] Vassil S. Dimitrov and Everett W. Howe, *Lower bounds on the lengths of double-base representations*, Proc. Amer. Math. Soc. **139** (2011), no. 10, 3423–3430. MR 2813374

[13] Taylor Dupuy and David E. Weirich, *Bits of 3^n in binary, Wieferich primes and a conjecture of Erdős*, J. Number Theory **158** (2016), 268–280. MR 3393551

[14] Paul Erdős, *Some unconventional problems in number theory*, Math. Mag. **52** (1979), no. 2, 67–70. MR 527408

[15] Paul Erdős, Carl Pomerance, and Eric Schmutz, *Carmichael's lambda function*, Acta Arith. **58** (1991), no. 4, 363–385. MR 1121092

[16] Jeffrey C. Lagarias, *Ternary expansions of powers of 2*, J. Lond. Math. Soc. (2) **79** (2009), no. 3, 562–588. MR 2506687
[17] Władysław Narkiewicz, *A note on a paper of H. Gupta concerning powers of two and three*, Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz. (1980), no. 678-715, 173–174 (1981). MR 623247
[18] S. Sivasankaranarayana Pillai, *On the equation* $2^x - 3^y = 2^X + 3^Y$, Bull. Calcutta Math. Soc. **37** (1945), 15–20. MR 13386
[19] Hans Georg Senge and Ernst Gabor Straus, PV*-numbers and sets of multiplicity*, Period. Math. Hungar. **3** (1973), 93–100. MR 340185
[20] Cameron L. Stewart, *On the representation of an integer in two different bases*, J. Reine Angew. Math. **319** (1980), 63–72. MR 586115
[21] László Szalay, *The equations* $2^n \pm 2^m \pm 2^l = z^2$, Indag. Math. (N.S.) **13** (2002), no. 1, 131–142. MR 2014980

(Dimitrov) Center for Information Security and Cryptography, University of Calgary, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada
Email address: vdimitro@ucalgary.ca

(Dimitrov) Lemurian Labs, Inc.
Email address: vassil@lemurianlabs.com

(Howe) Independent mathematician, San Diego, CA 92104, USA
Email address: however@alumni.caltech.edu
URL: http://ewhowe.com