A NOTE ON ERDŐS PROBLEM #479: INFINITUDE OF THE SETS $A(2^i)$ AND RELATED RESULTS

QUANYU TANG

1. Introduction

For an integer k we consider the congruence

$$2^n \equiv k \pmod{n}, \tag{1.1}$$

and the associated set

$$A(k) \coloneqq \{n \geq 1 : 2^n \equiv k \pmod{n}\}.$$

In [2, p. 96], Graham proposed the following conjecture, which also appears as Problem #479 on Bloom's Erdős Problems website [1].

Conjecture 1.1. *Is it true that, for every integer $k \neq 1$, the set $A(k)$ is infinite? Equivalently, is it true that, for all $k \neq 1$, there are infinitely many n such that $2^n \equiv k \pmod{n}$?*

It is easy to see that $2^n \not\equiv 1 \pmod{n}$ for all $n > 1$ (see, e.g., the proof reproduced on the OEIS wiki [6]), so the restriction $k \neq 1$ is necessary. In fact $A(1) = \{1\}$.

In their monograph [2, p. 96], Erdős and Graham attribute the following partial result to Graham, Lehmer and Lehmer:

This is known to be true (see [Gr-Leh-Leh(xx)]) if $k = 2^i$, $i \geq 1$, and $k = -1$.

However, [Gr-Leh-Leh(xx)] refers to an unpublished manuscript, and, as noted on Bloom's Erdős Problems website [1], no published version of this manuscript seems to exist; it also does not appear in the standard bibliographies of Graham or D. H. Lehmer.

We remark that the statement for $k = -1$ is now standard: numbers n with $n \mid 2^n + 1$ are called Novák numbers, and their infinitude is well established (see Kalmynin [4] and OEIS [7]).

The main purpose of this note is twofold:

- in Section 2 we survey the existing results and record those integers k for which $A(k)$ is currently known to be infinite;
- and, for completeness, in Section 3 we give an explicit proof of the case $k = 2^i$, $i \geq 1$.

We do *not* claim any of the underlying number-theoretic statements as new; the novelty here is only expository. The proof in Section 3 is an independent argument using multiplicative orders and Dirichlet's theorem, and may or may not coincide with the (unpublished) proof of Graham–Lehmer–Lehmer [3].

2. Known results and OEIS data

2.1. **The sets $A(k)$ and OEIS entries.** For each fixed integer k, the set $A(k)$ collects all positive integers n with

$$n \mid 2^n - k.$$

The online database OEIS contains separate entries for many of these sets. A convenient starting point is the OEIS wiki page $2^n \bmod n$ [6] and the cross-references on the page for

Date: December 2, 2025.

$A334634$ [8]. In particular, the following table of integer values of k for which $A(k)$ has its own OEIS entry is adapted from the table on the OEIS wiki page [6].

k	OEIS entry for $A(k)$
-11	A334634
-10	A245594
-9	A240942
-8	A245319
-7	A240941
-6	A245728
-5	A245318
-4	A244673
-3	A015940
-2	A006517
-1	A006521
0	A000079
2	A015919
3	A050259
4	A015921
5	A128121
6	A128122
7	A033981
8	A015922
9	A051447
10	A128123
11	A033982
12	A128124
13	A051446
14	A128125
15	A033983
16	A015924
17	A124974
18	A128126
19	A125000
$32 = 2^5$	A015925
$64 = 2^6$	A015926
$128 = 2^7$	A015927
$256 = 2^8$	A015929
$512 = 2^9$	A015931
$1024 = 2^{10}$	A015932
$2048 = 2^{11}$	A015935
$4096 = 2^{12}$	A015937

TABLE 1. Integer values of k for which $A(k)$ currently has a dedicated OEIS entry (from the cross-references in [8]).

For $k = 1$ one has $A(1) = \{1\}$; this trivial case is discussed on the OEIS wiki [6], but (reasonably) does not have its own numbered sequence.

2.2. **Values of k with $A(k)$ known to be infinite.** We now summarize what is currently known about the infinitude of $A(k)$.

2.2.1. *The trivial cases.*

- $k = 0$: Here $2^n \equiv 0 \pmod{n}$ if and only if n is a power of 2. Thus
$$A(0) = \{2^m : m \geq 0\},$$
and $A(0)$ is clearly infinite. This is recorded as A000079 in the OEIS.
- $k = 2$: For every odd prime p we have $2^{p-1} \equiv 1 \pmod{p}$ and hence
$$2^p \equiv 2 \pmod{p}.$$
Thus all odd primes lie in $A(2)$, so $A(2)$ is infinite. This is sequence A015919.

2.2.2. *The Novák numbers: $k = -1$.* Numbers n with $n \mid 2^n + 1$ are called *Novák numbers.* They form OEIS sequence A006521. It is easy to see, using the lifting-the-exponent (LTE) lemma, that
$$3^{m+1} \mid 2^{3^m} + 1$$
for every $m \geq 0$, so in particular $3^m \in A(-1)$ for all m. Kalmynin [4] gives quantitative lower bounds for the counting function of Novák numbers, confirming that there are infinitely many such n. Thus the set $A(-1)$ is infinite.

2.2.3. *Numbers with $n \mid 2^n + 2$: $k = -2$.* The set
$$A(-2) = \{n \geq 1 : n \mid 2^n + 2\}$$
is OEIS A006517. Kin Y. Li et al. showed in [5] that $A(-2)$ is infinite.

2.2.4. *The powers of two: $k = 2^i$.* Erdős and Graham state (without proof) that Graham, Lehmer and Lehmer showed $A(2^i)$ is infinite for every integer $i \geq 1$ [2, p. 96]. We have not been able to locate a published proof of this statement, nor the original Graham–Lehmer–Lehmer manuscript. In Section 3 below we give an explicit proof that $A(2^i)$ is infinite for every $i \geq 1$, using multiplicative orders and Dirichlet's theorem on primes in arithmetic progressions.

For $i = 1$ this reduces to the case $k = 2$ discussed above; for $i \geq 2$ this seems not to be written down in detail elsewhere. The sequences $A(2^i)$ for $i = 1, 2, 3, \ldots$ correspond to the OEIS entries

A015919, A015921, A015922, A015924, A015925, A015926, ...,

cf. Table 1.

2.2.5. *Other values of k.* For the remaining k appearing in Table 1 (for example $k = 3, 5, -3, -4, \ldots$), the current state of knowledge is essentially experimental:

- for many k at least one solution $n \in A(k)$ is known, sometimes astronomically large (e.g. $k = 3$ has a known solution $n = 4700063497$, see A050259);
- but for no such k (besides those listed above) has it been proved that $A(k)$ is infinite, nor even that $A(k)$ is nonempty beyond a finite list of experimentally found n.

In particular, Conjecture 1.1 remains open for every fixed k other than
$$k \in \{0, 1, -1, -2, 2^i : i \geq 1\}.$$

3. The case $k = 2^i$

Theorem 3.1. *Let $i \geq 1$ be an integer. Then there exist infinitely many positive integers n such that*

$$2^n \equiv 2^i \pmod{n}.$$

Equivalently, $A(2^i)$ is infinite for every $i \geq 1$.

Proof. Fix $i \geq 1$. We shall construct infinitely many integers n of the form

$$n = ip,$$

where p runs over an infinite set of primes depending on i.

Let p be an odd prime with $p \nmid i$, and set $n = ip$. By Fermat's little theorem,

$$2^{p-1} \equiv 1 \pmod{p},$$

hence

$$2^p = 2 \cdot 2^{p-1} \equiv 2 \pmod{p}.$$

Therefore

$$2^n = 2^{ip} = (2^p)^i \equiv 2^i \pmod{p}$$

for every such prime p. Thus

$$p \mid (2^n - 2^i)$$

holds automatically for all odd primes p, independently of any further conditions.

Now, we must ensure additionally that

$$i \mid (2^n - 2^i).$$

Write a prime power factorization

$$i = 2^s \prod_{j=1}^{t} q_j^{e_j},$$

where $s \geq 0$, $t \geq 0$, and $q_1, \ldots, q_t$ are distinct odd primes. We have

$$2^n - 2^i = 2^i \big(2^{i(p-1)} - 1\big),$$

so it suffices to guarantee that each odd prime power $q_j^{e_j}$ divides $2^{i(p-1)} - 1$ (the 2-power part will be handled separately). Since $\gcd(2, q_j) = 1$, 2 is invertible modulo $q_j^{e_j}$, and the condition

$$2^{i(p-1)} \equiv 1 \pmod{q_j^{e_j}}$$

is equivalent to the statement that the multiplicative order

$$d_j := \operatorname{ord}_{q_j^{e_j}}(2)$$

divides $i(p-1)$. Let

$$g_j := \gcd(d_j, i), \qquad m_j := \frac{d_j}{g_j}.$$

Then $d_j \mid i(p-1)$ is equivalent to $m_j \mid (p-1)$: indeed, writing $d_j = g_j m_j$ and $i = g_j v_j$ with $\gcd(m_j, v_j) = 1$, we have

$$d_j \mid i(p-1) \iff g_j m_j \mid g_j v_j (p-1) \iff m_j \mid (p-1).$$

Thus, for each odd prime power $q_j^{e_j} \parallel i$, the requirement that $q_j^{e_j}$ divides $2^{i(p-1)} - 1$ is equivalent to the congruence

$$p \equiv 1 \pmod{m_j}.$$

Since $2^s \mid i$ and $2^s \mid 2^i$, automatically

$$2^s \mid 2^i \mid 2^i \big(2^{i(p-1)} - 1\big) = 2^n - 2^i$$

for every p. Thus the 2-part of i imposes no restriction on p.

Let

$$L := \mathrm{lcm}(m_1, \ldots, m_t),$$

with the convention that $L = 1$ if $t = 0$ (i.e., if i has no odd prime factors). If p is a prime such that

$$p \equiv 1 \pmod{L} \quad \text{and} \quad p \nmid i,$$

then for every j we have $p \equiv 1 \pmod{m_j}$ and hence $q_j^{e_j} \mid 2^{i(p-1)} - 1$, as required. As we have just seen, 2^s automatically divides $2^n - 2^i$, and we have already observed that $p \mid 2^n - 2^i$ always holds. Moreover, by construction $\gcd(i, p) = 1$, so the prime factors of i and p are disjoint. Thus the divisibility

$$i \mid (2^n - 2^i) \quad \text{and} \quad p \mid (2^n - 2^i)$$

combine to give

$$ip \mid (2^n - 2^i).$$

In other words, for any such p,

$$2^{ip} \equiv 2^i \pmod{ip},$$

so $n = ip$ lies in $A(2^i)$.

It remains to show that there are infinitely many primes p with

$$p \equiv 1 \pmod{L}, \qquad p \nmid i.$$

Since $L \geq 1$ is fixed and $\gcd(1, L) = 1$, Dirichlet's theorem on primes in arithmetic progressions implies that there are infinitely many primes $p \equiv 1 \pmod{L}$. Excluding the finitely many primes dividing i still leaves infinitely many such p. For each of these primes p, the integer $n = ip$ satisfies $2^n \equiv 2^i \pmod{n}$, and the resulting values n are clearly distinct and unbounded. Hence $A(2^i)$ is infinite, as claimed. □

To make the mechanism of the proof of Theorem 3.1 more transparent, let us examine in detail what the construction produces when $i = 3$.

Example 3.2. Taking $i = 3$, we have $i = 3 = 2^0 \cdot 3$, so the only odd prime factor is $q_1 = 3$ with $e_1 = 1$. The multiplicative order of 2 modulo 3 is

$$d_1 = \mathrm{ord}_3(2) = 2.$$

Thus

$$g_1 = \gcd(d_1, 3) = 1, \qquad m_1 = \frac{d_1}{g_1} = 2,$$

and hence

$$L = \mathrm{lcm}(m_1) = 2.$$

According to the proof of Theorem 3.1, any prime p with

$$p \equiv 1 \pmod{L}, \qquad p \nmid i$$

gives a solution $n = ip = 3p$. In this case $L = 2$, so p can be any odd prime different from 3. For instance,

$$p = 5, 7, 11, 13, 17, 19, \ldots$$

yield

$$n = 15, 21, 33, 39, 51, 57, \ldots,$$

and one checks that $2^n \equiv 8 \pmod{n}$ for all these n.

Comparing with the OEIS entry A015922, which begins

$$1, 2, 3, 4, 8, 9, 15, 21, 33, 39, 51, 57, 63, 69, \ldots,$$

we see that all the integers $3p$ produced by this construction indeed belong to $A(8)$.

References

[1] T. F. Bloom, Erdős Problem #479, `https://www.erdosproblems.com/479`, accessed 2025-12-02

[2] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographie No. 28 de L'Enseignement Mathématique, Geneva, 1980.

[3] R. L. Graham, D. H. Lehmer and E. Lehmer, *On values of* 2^n *modulo* n, unpublished manuscript; cited (as [Gr-Leh-Leh(xx)]) in [2].

[4] A. Kalmynin, On Novák numbers, *Sb. Math.* **209** (2018), no. 4, 520–541; see also arXiv:1611.00417.

[5] Kin Y. Li et al., Solution to Problem 323, *Mathematical Excalibur* **14** (2009), no. 2, 3–4. (online)

[6] OEIS Wiki, $2^n \bmod n$, The On-Line Encyclopedia of Integer Sequences, https://oeis.org/wiki/2%5En_mod_n.

[7] N. J. A. Sloane et al., OEIS sequence A006521: Numbers n such that n divides $2^n + 1$ (Novák numbers).

[8] M. Alekseyev, OEIS sequence A334634: Numbers m such that m divides $2^m + 11$, with detailed cross-references to all integer k for which $A(k)$ has an OEIS entry.

School of Mathematics and Statistics, Xi'an Jiaotong University, Xi'an 710049, P. R. China
Email address: `tang_quanyu@163.com`