Solution of Nathanson's Exponential Congruence

By Samuel S. Wagstaff, Jr.

Abstract. The exponential congruence $5^n \equiv 2 \pmod{3^n}$ has no solution $n > 1$. This result is proved by using a theorem of van der Poorten to produce an upper bound for the size of such solutions n which is within range of machine verification, and then checking that no n below this bound satisfies the congruence.

Nathanson [1] conjectured that the congruence

$$(1) \quad 5^n \equiv 2 \pmod{3^n}$$

has no solution $n > 1$. Shortly after his paper appeared we searched for solutions to (1). We will describe below how we showed that there are none in the range $1 < n < 10^{104}$.

Recent work of van der Poorten [2] allows one to prove an upper bound on the size of any n satisfying (1). Happily, this bound is less than 10^{104} . Thus, we now know the general solution to (1).

THEOREM. *The only positive integer solution to (1) is $n = 1$.*

We next quote Theorem 4 of [2]. To avoid complicated notation, we restrict it to two rational integers α_i . (The original theorem considers several algebraic numbers α_i .) Let $\text{ord}_p(a)$ denote the ordinal of a at the prime p .

PROPOSITION (VAN DER POORTEN [2]). *Let α_1 and α_2 be nonzero rational integers. Let $\Omega' = \log \max \{|\alpha_1|, e^e\}$ and $A = \max \{|\alpha_1|, |\alpha_2|, e^e\}$. Let p be a rational prime and $T = 48^{36} p \Omega' \log \Omega'$. If $0 < \delta < 1$ and there exists a positive integer b such that*

$$\infty > \text{ord}_p(\alpha_1^b \alpha_2^{-1} - 1) > \delta b,$$

then

$$b < \delta^{-1} T (\log(\delta^{-1} T)) \log A.$$

The constant 48^{36} has no special significance and is not best possible. As van der Poorten notes, it is just a tidy constant which works.

LEMMA. *Let n, u, v , and w be integers such that $v > 1$, $(v, w) = 1$, $u^n \neq w$, and*

$$(2) \quad u^n \equiv w \pmod{v^n}.$$

Then $n \leq T(\log T) \log A$, where $T = 48^{36} v \Omega' \log \Omega'$, $\Omega' = \log \max \{|u|, e^e\}$, and $A = \max \{|u|, |w|, e^e\}$.

Received October 26, 1978.

AMS (MOS) subject classifications (1970). Primary 10A10.

Key words and phrases. Exponential congruence.

© 1979 American Mathematical Society
0025-5718/79/0000-0118/\$02.00

Proof. Let $0 < \delta < 1$. Clearly, we may assume $n > e^2$. Let p be a prime divisor of v . Then $p \nmid w$ because $(v, w) = 1$. Also, $u^n \equiv w \pmod{p^n}$, so that

$$\infty > \text{ord}_p(u^n w^{-1} - 1) = n > \delta n.$$

From the proposition, the hypotheses of which we have just verified, we have

$$n < \delta^{-1} T' (\log(\delta^{-1} T')) \log A,$$

where $T' = 48^{36} p \Omega' \log \Omega'$. Our lemma follows when we replace p by v in T' and let $\delta \rightarrow 1$.

Let us apply the lemma to (1). We have $\Omega' = e$, $A = e^e$, and $T = 3e48^{36}$. From the lemma we find that if n satisfies (1), then

$$n \leq 3e^2 48^{36} (1 + \log 3 + 36 \log 48) < 48^{38} < 10^{104}.$$

Although machine verification of the first 48^{38} cases of (1) may appear hopeless, the task is really quite easy. Note that since 5 is a primitive root modulo 3^n for each $n \geq 1$ and $(2, 3^n) = 1$, there is a unique integer a_n such that

$$5^{a_n} \equiv 2 \pmod{3^n} \quad \text{and} \quad 0 < a_n < \phi(3^n),$$

where ϕ is Euler's function. For $n \geq 1$, define integers k_n by

$$(3) \quad a_{n+1} = a_n + k_n \cdot \phi(3^n),$$

so that $k_n = 0, 1$, or 2 .

Table 1 gives values of 3^n , $\phi(3^n)$, a_n , and k_n for $1 \leq n \leq 20$. Table 2 shows k_n for $1 \leq n \leq 219$. The calculation of these tables required about five minutes on the IBM 360/75 at the University of Illinois. The program was run twice to insure accuracy. When these tables were made, we did not know what upper bound could eventually be proved for n . Checking the first 219 values of n represented a modest search for solutions to (1). We could easily have continued to $n = 1000$ or so.

Let $k_0 = 1$. From (3) we have $a_n = \sum_{i=0}^{n-1} k_i \cdot \phi(3^i)$ and $a_{n+1} \geq a_n$ for $n \geq 1$. Also, $0 < n < \phi(3^n)$ for $n \geq 1$, so n is a solution of (1) if and only if $a_n = n$. Let $n > 1$ be a solution of (1). From Table 1, we have $n > 20$. Also, $a_6 = 317$, so $n \geq 317$. Finally,

$$a_{219} = \sum_{i=0}^{218} k_i \cdot \phi(3^i) = 1 + 2 \sum_{i=1}^{218} k_i \cdot 3^{i-1} \approx 1.4141967 \cdot 10^{104}$$

from Table 2, so that $n > 10^{104}$. This completes the proof of the theorem.

Using the method described above, one can solve many exponential congruences of the type (2). In the special case $u > v > w = 1$, Nathanson [1] proved that $2^n/n < u^v$, which is better than the lemma.

Among the numbers $k_1, k_2, \dots, k_{219}$, the value 0 appears 70 times, 1 appears 76 times, and 2 appears 73 times, or 32%, 35%, and 33% of the time, respectively. This data suggests the conjecture that k_n takes on the three values with equal frequency on the average, that is, $d(\{n: k_n = j\}) = 1/3$ for $j = 0, 1, 2$, where $d(A)$ denotes the asymptotic density of the set A of integers. It is easy to see that the numbers k_n are the 3-adic digits of $(\text{Log}(-2)/\text{Log}(-5) - 1)/2$, where Log is the 3-adic logarithm.

Thus, the conjecture asserts that this number is simply normal in the scale of 3. Since it is irrational and arises naturally, it is probably normal, too.

TABLE 1

n	3^n	$\phi(3^n)$	a_n	k_n
1	3	2	1	2
2	9	6	5	1
3	27	18	11	2
4	81	54	47	2
5	243	162	155	1
6	729	486	317	1
7	2187	1458	803	1
8	6561	4374	2261	2
9	19683	13122	11009	0
10	59049	39366	11009	0
11	177147	118098	11009	1
12	531441	354294	129107	1
13	1594323	1062882	483401	0
14	4782969	3188646	483401	0
15	14348907	9565938	483401	2
16	43046721	28697814	19615277	0
17	129140163	86093442	19615277	1
18	387420489	258280326	105708719	1
19	1162261467	774840978	363989045	0
20	3486784401	2324522934	363989045	1

The referee notes that a better result than the lemma may be derived from Theorem 1, p. 180, of [3]. It leads to $n < 10^{18}$ in our theorem, so that we only needed to compute about the first 40 k_n 's.

TABLE 2

Values of k_n for $1 \leq n \leq 219$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	2	1	2	2	1	1	1	2	0	0	1	1	0	0	2	0	1	1	0	1
21	0	2	1	2	2	1	2	0	2	2	2	2	0	1	1	1	0	1	1	2
41	0	2	0	0	2	1	2	2	2	0	1	1	1	2	1	1	1	2	1	0
61	1	0	1	2	1	2	0	1	2	2	0	2	2	2	1	1	0	2	1	1
81	2	0	0	1	2	0	1	2	0	2	2	0	2	1	2	0	0	2	2	2
101	2	0	1	1	1	2	0	1	0	0	0	2	1	1	2	0	1	0	2	0
121	1	1	1	2	2	1	0	2	2	2	1	0	1	0	1	1	0	2	0	0
141	1	1	2	0	1	0	0	0	1	1	1	0	2	2	2	2	0	1	1	2
161	0	2	2	0	1	1	0	0	2	0	2	2	1	0	1	1	0	2	0	1
181	1	0	0	0	1	2	2	1	0	1	2	1	0	1	1	2	2	1	2	1
201	0	0	0	0	2	0	0	0	0	1	2	2	2	1	1	0	0	2	0	-

The author thanks the Research Board of the University of Illinois for providing the computer time.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

1. M. B. NATHANSON, "An exponential congruence of Mahler," *Amer. Math. Monthly*, v. 79, 1972, pp. 55–57. MR 46 #133.
2. A. J. VAN DER POORTEN, "Linear forms in logarithms in the p -adic case," Chapter 2 of *Transcendence Theory: Advances and Applications*, (A. Baker and D. W. Masser, Eds.), Academic Press, London, 1977.
3. A. SCHINZEL, "On two theorems of Gelfond and some of their applications," *Acta Arith.*, v. 13, 1967, pp. 177–236. MR 36 #5086.