COMPOSITES THAT REMAIN COMPOSITE AFTER CHANGING A DIGIT

Michael Filaseta
Mathematics Department
University of South Carolina
Columbia, SC 29208-0001

Mark Kozek
Department of Mathematics
Whittier College
Whittier, CA 90608-0634

Charles Nicol
Mathematics Department
University of South Carolina
Columbia, SC 29208-0001

John Selfridge
Dept. of Mathematical Sciences
Northern Illinois University
DeKalb, IL 60115-2888

1 Introduction

We begin with a simple example. Let m be a positive integer. Let

$$N = (11 \cdot 13 \cdot 17 \cdot 19 \cdot 10)\, m + 15.$$

The right-most digit of N is 5. Thus, N is composite, and if we replace any digit of N, other than the right-most digit, with a different digit, then the new number obtained will be divisible by 5 and, hence, be composite. On the other hand, if we replace the right-most digit of N by a different digit, then we obtain one of $N \pm j$ where $j \in \{1, 2, 3, 4, 5\}$ and each of these is easily seen to be composite. Thus, N has the property that if we replace any one of its digits with an arbitrary digit, the number we obtain is composite.

Constructing examples of N having the above property is simplified by the fact that changing digits (arbitrarily many) of a natural number N, other than the right-most digit, results in a number divisible by $\gcd(N, 10)$. Thus, if we allow $\gcd(N, 10) \neq 1$, then we can easily construct examples of N with the property that replacing any one of its digits with an arbitrary digit results in a composite number.

2000 Mathematics Subject Classification: 11B25 (11A07, 11A63).
The first author was supported by the National Security Agency during the writing of this paper.

Our goal is to address here the more difficult issue of constructing such N but with the restriction $\gcd(N, 10) = 1$. For example, the number $N = 212159$ has this property. In other words, every number in the set,

$$\big\{d12159, 2d2159, 21d159, 212d59, 2121d9, 21215d : d \in \{0, 1, 2, \ldots, 9\}\big\}$$

is composite. In fact, it can be checked that 212159 is the smallest composite natural number, coprime to 10, such that if we replace any one of the digits of its decimal expansion with a $d \in \{0, \ldots, 9\}$, then the number created by this replacement is composite. We prove the following:

Theorem 1. *There are infinitely many composite natural numbers N, coprime to 10, with the property that if we replace any digit in the decimal expansion of N with $d \in \{0, \ldots, 9\}$, then the number created by this replacement is composite.*

After establishing Theorem 1, we will examine a similar problem in which the *insertion* of any one digit into a composite natural number N results in a number that is composite. As in the previous paragraph, we are interested in N that are coprime to 10. For example, the number $N = 25011$ has this property. In other words, every number in the set,

$$\big\{d25011, 2d5011, 25d011, 250d11, 2501d1, 25011d : d \in \{0, 1, 2, \ldots, 9\}\big\}$$

is composite. The number 25011 is the smallest composite natural number, coprime to 10, such that if you insert any digit $d \in \{0, \ldots, 9\}$ anywhere in its decimal expansion, then the number created by this insertion is composite. Analogous to Theorem 1, we establish the following:

Theorem 2. *There are infinitely many composite natural numbers N, coprime to 10, with the property that if you insert any digit $d \in \{0, \ldots, 9\}$ anywhere in the decimal expansion of N, then the number created by this insertion is composite.*

Another problem that could be considered along similar lines is whether there are infinitely many composite numbers such that when you remove any one digit, then the number remains composite. This problem is easier, however, as can be seen by considering a number consisting of a string of 3's. Further, a string of 1's of the form $(10^{15k+10} - 1)/9$, where k is an arbitrary positive integer, provides a further slightly less obvious example.

We turn to some open questions. We were able to obtain analogous results to Theorem 1 and Theorem 2 for all bases $b < 12$, but do analogous results hold for all bases? Do there exist infinitely many composite numbers N satisfying the conditions of both Theorem 1 and Theorem 2? Are there infinitely many *primes* p that are composite for every replacement (or insertion) of a digit? Does there exist a k_0 such that for every positive integer $k \geq k_0$ there is a composite number N with exactly k digits having the property of Theorem 1 (or Theorem 2)? Do there exist infinitely many composite numbers N that remain composite when any two digits (not necessarily consecutive) are changed (or inserted)? Based on heuristics, we conjecture that the answers to all of the above questions except the last is in the affirmative.

Acknowledgment: The first two authors note that Theorem 1 was established some years ago by the latter two authors. As it never appeared in print, the first two authors reconstructed a proof and included Theorem 2 which, as we will see, follows rather easily from the argument for Theorem 1.

2 Proof of Theorem 1

We give a construction of an infinite sequence of composite natural numbers N satisfying the conditions in the theorem. We write the decimal expansion of N as

$$N = d_{n-1}d_{n-2}\dots d_1d_0, \quad d_i \in \{0,\dots,9\}, \quad n \geq 1, \quad d_{n-1} \neq 0.$$

We also express N in the form

$$N = \frac{10^n - 1}{9} + M,$$

where M is a fixed natural number to be determined and n is a large natural number. Observe that our last expression for N is equivalent to

$$N = \underbrace{11\dots11}_{n\text{-many 1's}} + M$$

where the number $11\dots11$ is a string of n digits that are 1. To establish the theorem, we will find an infinite arithmetic progression of natural numbers n, a fixed natural number M, and a finite set of primes $\mathcal{P}$, such that when we replace any digit in the decimal expansion of N with $x \in \{0,\dots,9\}$, then the number created by this replacement is divisible by at least one of the primes in $\mathcal{P}$. We suppose throughout that n is large enough to imply that the left-most digit of N is 1.

Let $N^{(k)}(x)$ be the number that is obtained by replacing the digit d_k of the decimal expansion of N with $x \in \{0,\dots,9\}$. For example, if $N = 212159 = d_5d_4d_3d_2d_1d_0$, then $N^{(2)}(3) = 212359$. Since M is fixed, there exists a non-negative integer $K \leq n-1$ such that $d_k = 1$ for all $k \geq K$. We first consider these large values of k. For these k, we have that $N^{(k)}(x)$ takes the form

$$N^{(k)}(x) = \frac{10^n - 1}{9} + M + (x-1)\cdot 10^k.$$

Observe that if

$$\begin{aligned} n &\equiv 0 \pmod 3 \\ M &\equiv 1 \pmod 3 \\ x &\equiv 0 \pmod 3, \end{aligned}$$

then $N^{(k)}(x)$ is divisible by 3 since, in this case,

$$\begin{aligned} N^{(k)}(x) &= \frac{10^n - 1}{9} + M + (x-1)\cdot 10^k \\ &\equiv 0 + 1 + (-1) \pmod 3. \end{aligned}$$

Thus, the conditions $n \equiv 0 \pmod 3$ and $M \equiv 1 \pmod 3$ imply that for large k if we replace d_k with $x \in \{0,3,6,9\}$, then we obtain a composite number $N^{(k)}(x)$.

Similarly, we observe that if

$$\begin{aligned} n &\equiv 0 \pmod 6 \\ M &\equiv 0 \pmod 7 \\ x &\equiv 1 \pmod 7, \end{aligned}$$

then $N^{(k)}(x)$ is divisible by 7. Thus, for large k we know that our original N is necessarily composite and that if we replace d_k by $x = 8$, then we obtain the composite number $N^{(k)}(x)$.

Combining the above, we see that if

$$n \equiv 0 \pmod 6 \quad \text{and} \quad M \equiv 7 \pmod{21}$$

and if, for an arbitrary $k \geq K$, we replace d_k in N with any digit in $\{0, 1, 3, 6, 8, 9\}$, then the number $N^{(k)}(x)$ obtained is divisible by either 3 or 7.

To address the remaining cases of $N^{(k)}(x)$ for $x \in \{2, 4, 5, 7\}$ when k is large, we will use the following.

Definition. A finite system of congruences $x \equiv a_i \pmod{m_i}$, $1 \leq i \leq t$, is called a *covering of the integers* if each integer satisfies at least one congruence in the system.

As an example, we note

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 1 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 9 \pmod{12} \end{aligned}$$

is a covering of the integers. In the way of notation, for a prime p and an integer a not divisible by p, we use $\mathrm{ord}_p(a)$ to denote the order of a modulo p, that is the least positive integer k such that $a^k \equiv 1 \pmod p$.

Lemma 1. *Let N and M be natural numbers such that*

$$N = \frac{10^n - 1}{9} + M,$$

where N has the decimal expansion

$$N = d_{n-1}d_{n-2}\ldots d_1 d_0, \quad d_i \in \{0, \ldots, 9\}, \quad n \geq 1, \quad d_{n-1} \neq 0.$$

Let K be a non-negative integer $\leq n-1$ such that $d_k = 1$ for $k \in \{K, K+1, \ldots, n-1\}$. For a fixed $x \in \{0, \ldots 9\}$, suppose we have distinct primes $p_1, \ldots, p_t$, each > 5, for which

(i) there exists a covering of the integers

$$k \equiv b_i \pmod{c_i}, \quad 1 \leq i \leq t,$$

where $c_i = \mathrm{ord}_{p_i}(10)$,

(ii) $n \equiv 0 \pmod{\mathrm{lcm}(c_1, \ldots, c_t)}$,

(iii) M is a solution to the system of congruences

$$M \equiv -(x-1) \cdot 10^{b_i} \pmod{p_i}, \quad 1 \leq i \leq t.$$

Then, for each $k \in \{K, K+1, \ldots, n-1\}$,

$$N^{(k)}(x) = \frac{10^n - 1}{9} + M + (x-1) \cdot 10^k$$

is divisible by at least one of the primes p_i *where* $1 \le i \le t$.

Proof. Suppose the conditions in the lemma hold. Let $k \in \{K, K+1, \ldots, n-1\}$. By (i), there is an $i \in \{1, \ldots, t\}$ such that $k \equiv b_i \pmod{c_i}$. Since $c_i = \mathrm{ord}_{p_i}(10)$ and $n \equiv 0 \pmod{\mathrm{lcm}(c_1, \ldots, c_t)}$, we have $p_i \mid (10^n - 1)/9$. Hence,

$$N^{(k)}(x) = \frac{10^n - 1}{9} + M + (x-1) \cdot 10^k \equiv M + (x-1) \cdot 10^{b_i} \pmod{p_i}.$$

From (iii), we deduce $N^{(k)}(x) \equiv 0 \pmod{p_i}$, completing the proof. □

Set

$$\mathcal{P}_0 = \mathcal{P}_3 = \mathcal{P}_6 = \mathcal{P}_9 = \{3\}, \quad \mathcal{P}_1 = \mathcal{P}_8 = \{7\}.$$

For $x \in \{2, 4, 5, 7\}$, let $\mathcal{P}_x$ denote a set of primes, if it exists, as in Lemma 1 so that $N^{(k)}(x)$ is divisible by some prime from $\mathcal{P}_x$ for each $k \in \{K, K+1, \ldots, n-1\}$ provided (ii) and (iii) hold for some covering as in (i). For primes $p \notin \{2, 5\}$, we define $c(p) = \mathrm{ord}_p(10)$. For $x \in \{2, 4, 5, 7\}$, we write the covering system in (i) as

$$k \equiv b(x, p) \pmod{c(p)}, \quad p \in \mathcal{P}_x. \tag{1}$$

To establish Theorem 1, we will take n in the definition of N so that it is divisible by the least common multiple of the numbers in the set

$$\bigcup_{x=0}^{9} \{c(p) : p \in \mathcal{P}_x\}.$$

We will also take M so that the various congruences

$$\begin{aligned} &M \equiv 7 \pmod{21} \\ &M \equiv -(x-1) \cdot 10^{b(x,p)} \pmod{p}, \quad \text{where } x \in \{2, 4, 5, 7\} \text{ and } p \in \mathcal{P}_x, \end{aligned} \tag{2}$$

simultaneously hold. It is clear that we can find infinitely many n as above, but we need our choice of coverings as in (1) and prime sets $\mathcal{P}_x$ to be such that (2) has a solution. We justify that this is possible with explicit sets $\mathcal{P}_x$ and coverings as in (1).

To obtain a set of primes $\mathcal{P}_x$ and a covering as in (1), we make use of the tables of factorizations of $10^c - 1$ in [1] to determine, for a given positive integer c, the set of primes p such that $c = \mathrm{ord}_p(10)$. For the purposes of finding a covering as in (1), each such p corresponds to a congruence of the form $k \equiv b \pmod{c}$ that we can use, where we have some freedom on how to choose b. Observe that, given c, there may be more than one prime p for which $c = \mathrm{ord}_p(10)$. Choosing b differently for different p allows us to use two or more different congruences with the same modulus in a covering. On the other hand, given c, it is also possible that there are no primes p for which $c = \mathrm{ord}_p(10)$. In this case, we cannot use the modulus c in (1).

To clarify, one can check that

$$\begin{aligned} 2 &= \mathrm{ord}_{11}(10) \\ 4 &= \mathrm{ord}_{101}(10) \\ 8 &= \mathrm{ord}_{73}(10) \\ 8 &= \mathrm{ord}_{137}(10). \end{aligned}$$

Thus, for a covering of the integers, we may use 2 and 4 each once as the modulus of a congruence of a covering, and we may use 8 twice as the modulus of a congruence. One checks that

$$\begin{aligned} k &\equiv 0 \pmod 2 \\ k &\equiv 1 \pmod 4 \\ k &\equiv 3 \pmod 8 \\ k &\equiv 7 \pmod 8 \end{aligned}$$

is a covering of the integers. To apply Lemma 1, we take

$$\mathcal{P}_2 = \{11, 73, 101, 137\},$$

n divisible by 8, and M so that

$$\begin{aligned} M &\equiv -(2-1)\cdot 10^0 \pmod{11} \\ M &\equiv -(2-1)\cdot 10^1 \pmod{101} \\ M &\equiv -(2-1)\cdot 10^3 \pmod{73} \\ M &\equiv -(2-1)\cdot 10^7 \pmod{137}. \end{aligned}$$

Note that these congruences on M are equivalent to a single congruence modulo $11 \cdot 73 \cdot 101 \cdot 137$ by the Chinese Remainder Theorem; in particular, such M exist. We deduce from Lemma 1 that, under these conditions, the number $N^{(k)}(2)$ is composite for $K \le k \le n-1$.

We write the congruence on M just alluded to above as

$$M \equiv B(2) \pmod{11 \cdot 73 \cdot 101 \cdot 137}.$$

Combining this with our previous results, we have that if

$$n \equiv 0 \pmod{24}$$

and M is a solution of the system of congruences

$$\begin{aligned} M &\equiv 7 \pmod{3 \cdot 7} \\ M &\equiv B(2) \pmod{11 \cdot 73 \cdot 101 \cdot 137}, \end{aligned}$$

which we know exists by the Chinese Remainder Theorem, then $N^{(k)}(x)$ will be divisible by at least one prime in $\{3, 7, 11, 73, 101, 137\}$ for each $x \in \{0, 1, 2, 3, 6, 8, 9\}$ and $K \le k \le n-1$.

Observe that to assure that M exists by using the Chinese Remainder Theorem above, we chose $\mathcal{P}_2$ so that it had an empty intersection with the previous sets

$$\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_3, \mathcal{P}_6, \mathcal{P}_8, \mathcal{P}_9$$

already constructed. This will be our strategy then for establishing that the congruences in (2) simultaneously hold. Thus, we follow the same approach for $N^{(k)}(x)$ when $x \in \{4, 5, 7\}$ as we did for $N^{(k)}(2)$, but, in each case, the covering of the integers will be more complicated because we do not wish to repeat using the same primes previously chosen. We list the coverings and the primes used for $x \in \{4, 5, 7\}$.

We begin with $x = 4$. Table 1 contains the needed information for us. To conserve space, we note here that

$$p_7 = 440334654777631, \quad p_{14} = 3199044596370769.$$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 3$	37
2	$k \equiv 1 \pmod 6$	13
3	$k \equiv 2 \pmod 9$	333667
4	$k \equiv 5 \pmod{18}$	19
5	$k \equiv 14 \pmod{18}$	52579
6	$k \equiv 8 \pmod{27}$	757
7	$k \equiv 17 \pmod{27}$	p_7

row	congruence	prime p_i
8	$k \equiv 26 \pmod{54}$	70541929
9	$k \equiv 53 \pmod{54}$	14175966169
10	$k \equiv 4 \pmod{12}$	9901
11	$k \equiv 10 \pmod{24}$	99990001
12	$k \equiv 22 \pmod{72}$	3169
13	$k \equiv 46 \pmod{72}$	98641
14	$k \equiv 70 \pmod{72}$	p_{14}

Table 1: Covering used in Lemma 1 (i) for $N^{(k)}(4)$

We observe that we are taking $\mathcal{P}_4$ to be the set of 14 primes appearing in the columns with the heading "prime p_i". The congruences in (1) appear in the columns with heading "congruence". Thus, if p appears in the column with heading "prime p_i", then the congruence in this same row takes the form $k \equiv b(4, p) \pmod{c(p)}$. In each row, one can check directly that $\mathrm{ord}_p(10) = c(p)$.

We also need to justify that the 14 congruences displayed in Table 1 form a covering. The least common multiple of the moduli appearing in these congruences is 216. One checks directly (by hand or computer) that the numbers $0, 1, 2, \ldots, 215$ each satisfy at least one of the congruences in the table. Now, suppose that m is an arbitrary integer. Let $m' \in \{0, 1, \ldots, 215\}$ such that $m \equiv m' \pmod{216}$. We deduce then, since each modulus in the congruences divides 216, that m is a solution of whatever congruence m' satisfies. Hence, the verification that the congruences in Table 1 form a covering is complete.

For $x \in \{5, 7\}$, we use the same approach as above. We give the tables explicitly but do not elaborate on the details. We simply note that in each case one should check that the congruence $k \equiv b(x, p) \pmod{c(p)}$ and p appearing on a row are such that $\mathrm{ord}_p(10) = c(p)$. For each table, one should also check that the congruences form a covering, and this can be done by simply checking if the non-negative integers up to one less that the least common multiple of the moduli each satisfy at least one congruence from the table.

For $x = 5$, we make use of the information in Table 2. To conserve space, we set

$$p_{10} = 5964848081, \quad p_{17} = 4185502830133110721.$$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 5$	41
2	$k \equiv 1 \pmod 5$	271
3	$k \equiv 2 \pmod{10}$	9091
4	$k \equiv 3 \pmod{20}$	3541
5	$k \equiv 13 \pmod{20}$	27961
6	$k \equiv 7 \pmod{30}$	211
7	$k \equiv 17 \pmod{30}$	241
8	$k \equiv 27 \pmod{30}$	2161
9	$k \equiv 8 \pmod{40}$	1676321
10	$k \equiv 28 \pmod{40}$	p_{10}

row	congruence	prime p_i
11	$k \equiv 18 \pmod{60}$	61
12	$k \equiv 38 \pmod{60}$	4188901
13	$k \equiv 58 \pmod{60}$	39526741
14	$k \equiv 4 \pmod{15}$	31
15	$k \equiv 9 \pmod{15}$	2906161
16	$k \equiv 14 \pmod{45}$	238681
17	$k \equiv 29 \pmod{45}$	p_{17}
18	$k \equiv 44 \pmod{90}$	29611
19	$k \equiv 89 \pmod{90}$	3762091

Table 2: Covering used in Lemma 1 (i) for $N^{(k)}(5)$

For $x = 7$, we use the information in Table 3. We note here that

$$p_{11} = 102598800232111471,\ p_{13} = 265212793249617641,\ p_{14} = 30703738801,$$
$$p_{15} = 625437743071,\ p_{16} = 57802050308786191965409441,$$
$$p_{21} = 4458192223320340849,\ p_{27} = 127522001020150503761,\ p_{31} = 60368344121,$$
$$p_{32} = 848654483879497562821,\ p_{34} = 73765755896403138401,$$
$$p_{35} = 11189053009,\ p_{36} = 603812429055411913,\ p_{37} = 148029423400750506553.$$

For $K \le k \le n-1$, our argument is complete upon noting that the sets $\{3, 7\}$, $\mathcal{P}_2$, $\mathcal{P}_4$, $\mathcal{P}_5$ and $\mathcal{P}_7$ are pairwise disjoint. This allows us then to take n so that it is divisible by 6 and each modulus appearing in (1) independent of the value of $x \in \{2, 4, 5, 7\}$ and also assures that there is a simultaneous solution to the congruences appearing in (2).

We fix C to be the least common multiple of the moduli appearing in the congruences in (1) for $x \in \{2, 4, 5, 7\}$. Note that 6 divides C. Thus, taking

$$\mathcal{P} = \{3, 7\} \cup \mathcal{P}_2 \cup \mathcal{P}_4 \cup \mathcal{P}_5 \cup \mathcal{P}_7,$$

we see that if $n \equiv 0 \pmod C$, $K \le k \le n-1$ and $x \in \{0, 1, \ldots, 9\}$, then $N^{(k)}(x)$ is divisible by at least one prime from $\mathcal{P}$.

It is worth noting here that the primes 2 and 5 are not in $\mathcal{P}$. This is done deliberately as Theorem 1 requires that N be coprime to 10. Combining the congruences appearing in (2) with the congruence $M \equiv 0 \pmod{10}$, for example, allows us to deduce that we can in fact take N coprime to 10.

For the remainder of this section, we fix $M \equiv 0 \pmod{10}$ so that N is coprime to 10 and if $n \equiv 0 \pmod C$, $K \le k \le n-1$ and $x \in \{0, 1, \ldots, 9\}$, then $N^{(k)}(x)$ is divisible by at least one prime from $\mathcal{P}$. Fix also some $n_0 \equiv 0 \pmod C$. We suppose that n_0 satisfies $10^{n_0-2} > M$. Then for $n \ge n_0$, the number

$$N = \frac{10^n - 1}{9} + M$$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 7$	239
2	$k \equiv 1 \pmod 7$	4649
3	$k \equiv 2 \pmod{21}$	43
4	$k \equiv 9 \pmod{21}$	1933
5	$k \equiv 16 \pmod{21}$	10838689
6	$k \equiv 3 \pmod{14}$	909091
7	$k \equiv 10 \pmod{28}$	29
8	$k \equiv 24 \pmod{28}$	281
9	$k \equiv 4 \pmod{35}$	71
10	$k \equiv 11 \pmod{35}$	123551
11	$k \equiv 18 \pmod{35}$	p_{11}
12	$k \equiv 25 \pmod{70}$	4147571
13	$k \equiv 60 \pmod{70}$	p_{13}
14	$k \equiv 32 \pmod{105}$	p_{14}
15	$k \equiv 67 \pmod{105}$	p_{15}
16	$k \equiv 102 \pmod{105}$	p_{16}
17	$k \equiv 5 \pmod{42}$	127
18	$k \equiv 26 \pmod{42}$	2689
19	$k \equiv 12 \pmod{42}$	459691

row	congruence	prime p_i
20	$k \equiv 33 \pmod{84}$	226549
21	$k \equiv 75 \pmod{84}$	p_{21}
22	$k \equiv 19 \pmod{63}$	10837
23	$k \equiv 40 \pmod{63}$	23311
24	$k \equiv 61 \pmod{63}$	45613
25	$k \equiv 6 \pmod{28}$	121499449
26	$k \equiv 13 \pmod{56}$	7841
27	$k \equiv 41 \pmod{56}$	p_{27}
28	$k \equiv 20 \pmod{140}$	421
29	$k \equiv 48 \pmod{140}$	3471301
30	$k \equiv 76 \pmod{140}$	13489841
31	$k \equiv 104 \pmod{140}$	p_{31}
32	$k \equiv 132 \pmod{140}$	p_{32}
33	$k \equiv 27 \pmod{112}$	113
34	$k \equiv 83 \pmod{112}$	p_{34}
35	$k \equiv 55 \pmod{168}$	p_{35}
36	$k \equiv 111 \pmod{168}$	p_{36}
37	$k \equiv 167 \pmod{168}$	p_{37}

Table 3: Covering used in Lemma 1 (i) for $N^{(k)}(7)$

has left-most digit 1. More importantly, as M is fixed, the number K is well-defined and does not vary as n varies over the integers $\geq n_0$.

There are a finitely many ways, independent of $n \geq n_0$, to have $k \in \{0, 1, \ldots, K-1\}$ and $x \in \{0, 1, \ldots, 9\}$. Fix

$$N_0 = \frac{10^{n_0} - 1}{9} + M.$$

Observe that N_0 is coprime to 10. Analogous to our previous notation, we refer to $N_0^{(k)}(x)$ as the number obtained by replacing the digit $x \in \{0, 1, \ldots, 9\}$ for the digit of N_0 appearing in the $(k+1)$st position on the right. For each $k \in \{0, 1, \ldots, K-1\}$ and $x \in \{0, 1, \ldots, 9\}$, we consider the least prime $q = q(k, x)$ dividing $N_0^{(k)}(x)$. If $q > 5$, $n \equiv n_0 \pmod{c(q)}$ and $n \geq n_0$, then q divides $N^{(k)}(x)$ since

$$N^{(k)}(x) - N_0^{(k)}(x) = \frac{10^n - 10^{n_0}}{9} = \frac{10^{n_0}}{9}\big(10^{n-n_0} - 1\big).$$

If $q \in \{2, 5\}$, then N_0 being coprime to 10 implies $k = 0$. It follows in this case that $N^{(k)}(x) = N^{(0)}(x)$ is also divisible by q. The definition of n_0 implies that if $q = 3$ and $n \equiv n_0 \pmod 3$, then both n and n_0 are divisible by 3 so that $10^{n-n_0} - 1$ is divisible by 27. Thus, in this case, we also have that $N^{(k)}(x)$ is divisible by q.

Set C' to be the least common multiple of C and the numbers $c(q)$ where q varies over the

primes $q(k,x) > 5$ with $0 \le k \le K-1$ and $x \in \{0,1,\dots,9\}$. Then we deduce that if

$$N = \frac{10^n - 1}{9} + M,$$

where

$$n \equiv n_0 \pmod{C'},$$

then $N^{(k)}(x)$ is divisible by the prime $q(k,x)$ provided $0 \le k \le K-1$ and $x \in \{0,1,\dots,9\}$. As such n are necessarily divisible by C, we further obtain for such n that $N^{(k)}(x)$ is divisible by at least one of the primes in $\mathcal{P}$ for $K \le k \le n-1$ and $x \in \{0,1,\dots,9\}$. Since the number N tends to infinity with n and the number of primes $q(k,x)$ as well as the set $\mathcal{P}$ are finite, the theorem follows.

3 Proof of Theorem 2

For a number $N' = d_r d_{r-1} \dots d_0$ written in base 10 with $d_r \neq 0$ and digit $x \in \{0,1,\dots,9\}$, we denote by $\widehat{N'}^{(k)}(x)$ the number obtained by inserting the digit x between d_k and d_{k-1}. For example,

$$\widehat{N'}^{(2)}(x) = d_r d_{r-1} \dots d_3 d_2 x d_1 d_0.$$

We also define $\widehat{N'}^{(0)}(x)$ as the number obtained by inserting in N' the digit x to the right of d_0 and $\widehat{N'}^{(r+1)}(x)$ as the number obtained by inserting in N' the digit x to the left of d_r. Thus,

$$\widehat{N'}^{(0)}(x) = d_r d_{r-1} \dots d_1 d_0 x \quad \text{and} \quad \widehat{N'}^{(r+1)}(x) = x d_r d_{r-1} \dots d_1 d_0.$$

We fix $\mathcal{P}$ to be the set of primes from the proof of Theorem 1 and C, M and K as determined there so that if $n \equiv 0 \pmod{C}$, then the number

$$N = \frac{10^n - 1}{9} + M$$

has the property that, for $K \le k \le n-1$, replacing the digit 1 that appears as the $(k+1)$st digit from the right with $x \in \{0,1,\dots,9\}$ results in a number $N^{(k)}(x)$ that is divisible by a prime in $\mathcal{P}$. Setting

$$N' = \frac{10^{n-1} - 1}{9} + M,$$

we see that

$$\widehat{N'}^{(k)}(x) = N^{(k)}(x) \quad \text{for } K \le k \le n-1.$$

Observe that, in the notation of the previous paragraph, $r = n-2$. Also, N' has the property that if $n \equiv 0 \pmod{C}$, then the insertion $\widehat{N'}^{(k)}(x)$, for $x \in \{0,1,\dots,9\}$ and $K \le k \le n-1$, is divisible by some prime from the set $\mathcal{P}$. Note that the exponent $n-1$ appearing in the definition of N' above is -1 modulo C.

The rest of our argument is analogous to what we did at the end of the previous section. We fix M so that

$$N' = \frac{10^n - 1}{9} + M$$

is coprime to 10 and if $n \equiv -1 \pmod{C}$, $K \leq k \leq n$ and $x \in \{0, 1, \ldots, 9\}$, then $\widehat{N'}^{(k)}(x)$ is divisible by at least one prime from $\mathcal{P}$. Fix also some $n_0 \equiv -1 \pmod{C}$. We suppose that n_0 satisfies $10^{n_0-2} > M$. Then for $n \geq n_0$, the number N' has left-most digit 1. As M is fixed, the number K is well-defined and does not vary as n varies over the integers $\geq n_0$.

There are a finitely many ways, independent of $n \geq n_0$, to have $k \in \{0, 1, \ldots, K-1\}$ and $x \in \{0, 1, \ldots, 9\}$. Fix

$$N_0' = \frac{10^{n_0} - 1}{9} + M.$$

Observe that N_0' is coprime to 10. We refer to $\widehat{N_0'}^{(k)}(x)$ as the number obtained by inserting the digit $x \in \{0, 1, \ldots, 9\}$ to the left of the kth digit of N_0. For each $k \in \{0, 1, \ldots, K-1\}$ and $x \in \{0, 1, \ldots, 9\}$, we consider the least prime $q = q(k, x)$ dividing $\widehat{N_0'}^{(k)}(x)$. Recall the definition $c(p) = \mathrm{ord}_p(10)$, for p a prime, used in the previous section. Observe that if $q > 5$, $n \equiv n_0 \pmod{c(q)}$ and $n \geq n_0$, then q divides $\widehat{N'}^{(k)}(x)$ since

$$\widehat{N'}^{(k)}(x) - \widehat{N_0'}^{(k)}(x) = \frac{10^{n+1} - 10^{n_0+1}}{9} = \frac{10^{n_0+1}}{9}\big(10^{n-n_0} - 1\big).$$

If $q \in \{2, 5\}$, then N_0' being coprime to 10 implies $k = 0$. It follows in this case that $\widehat{N'}^{(k)}(x) = \widehat{N'}^{(0)}(x)$ is also divisible by q. If $q = 3$ and $n \equiv n_0 \pmod{3}$, then $n - n_0$ is divisible by 3 so that $10^{n-n_0} - 1$ is divisible by 27. Thus, in this case, we also have that $\widehat{N'}^{(k)}(x)$ is divisible by q.

Set C'' to be the least common multiple of C and the numbers $c(q)$ where q varies over the primes $q(k, x) > 5$ with $0 \leq k \leq K-1$ and $x \in \{0, 1, \ldots, 9\}$. Then we deduce that if

$$N' = \frac{10^n - 1}{9} + M,$$

where

$$n \equiv n_0 \pmod{C''},$$

then $\widehat{N'}^{(k)}(x)$ is divisible by the prime $q(k, x)$ provided $0 \leq k \leq K-1$ and $x \in \{0, 1, \ldots, 9\}$. As such n are necessarily -1 modulo C, we further obtain for such n that $\widehat{N'}^{(k)}(x)$ is divisible by at least one of the primes in $\mathcal{P}$ for $K \leq k \leq n$ and $x \in \{0, 1, \ldots, 9\}$. Since the number N' tends to infinity with n and the number of primes $q(k, x)$ as well as the set $\mathcal{P}$ are finite, the theorem follows.

Reference

[1] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ Up to High Powers, 3rd edition, Contemporary Mathematics, Vol. 22, American Math. Soc., Providence, 2002 (available online).