Absolute Prime Numbers

DMITRY MAVLO

A natural number is said to be an absolute prime if it is prime and remains prime after any permutation of its digits. Prove that the decimal representation of an absolute prime number can contain no more than three distinct digits.

A. T. Kolotov, SMO, 1984

Find all natural numbers n *such that all* n*-digit numbers with* n − 1 *ones and* 1 *seven in its decimal representation are prime.*

A. M. Slin'ko, Short-listed to the IMO, 1990.

For a long time prime numbers have attracted the attention of mathematicians, especially those primes that possess some sort of a symmetry. The mysterious repunits $A_n = 111\ldots 1_{(n)}$, whose decimal representations contain only units, form an important class of them. For a repunit to be prime the number n of its digits must be also prime. But this condition is far from being sufficient: for instance, $A_3 = 111 = 3.37$ and $A_5 = 11111 = 41.271$. Some of the repunits are nonetheless prime: A_2, A_{19}, A_{23}, A_{317} and A_{1031}, are the only known examples. The question of primeness of the repunits was discussed by M. Gardner [1] and later in [2-4]. It is not clear whether the number of prime repunits is finite or infinite.

The prime repunits are the most obvious examples of numbers that remain prime after an arbitrary permutation of their digits. The numbers with this property are called either the *permutable* primes according to H.-E. Richert [5], who introduced them some 40 years ago, or the *absolute primes* according to T. N. Bhargava and P. H. Doyle [6], and A. W. Johnson [7]. The intent of this note is to give a short proof, that does not require too much number crunching, of all known facts concerning absolute primes different from repunits. One implication of our arguments is that, excluding repunits, once we get past 1000 any larger absolute prime must have at least 6×10^{175} *digits*! (So it is hardly surprising that *no* examples are known ...) For the sake of completeness we give all the details needed, including very well known ones.

Analysing the table of primes up to 10^3, we find 21 absolute primes different from repunits:

2, 3, 5, 7, 13, 17, 31, 37, 71, 73, 79, 97, 113, 131, 199, 311, 337, 373, 733, 919, 991.

An easy observation shows that multidigit absolute primes contain only the digits 1, 3, 7 and 9 in their decimal representations. The digits 0, 2, 4, 5, 6, 8 can never appear since by shifting each of these digits to the units place we obtain a multiple of 2 or 5.

Now we can reduce the search considerably by using the following lemmas, in which overlining is used to denote the digits of a number.

Lemma 1. ([6]) An absolute prime does not contain in its decimal representation all four digits 1, 3, 7, 9 simultaneously.

https://doi.org/10.2307/3618302 Published online by Cambridge University Press

Proof. Let N be a number with all four digits indicated in its decimal representation. Shifting them to the four rightmost places we obtain a number

$$N_0 = \overline{c_1c_2\dots c_{n-4}7931} = L \times 10^5 + 7931.$$

Numbers $K_0 = 7931$, $K_1 = 1793$, $K_2 = 9137$, $K_3 = 7913$, $K_4 = 7193$, $K_5 = 1937$, $K_6 = 7139$ have different remainders on dividing by 7; indeed $K_i \equiv i \pmod 7$. The numbers $N_i = L.10^5 + K_i$ for $i = 0, 1, \dots, 6$ also have different remainders on dividing by 7. Hence one of them is a multiple of 7. Since these numbers can be obtained from N by a permutation of digits, N is not an absolute prime. □

Lemma 2. An absolute prime does not contain in its decimal representation three digits a and two digits b simultaneously, provided $a \neq b$.

Proof. Suppose that a number N contains digits a, a, a, b, b in its decimal representation. By a permutation of digits of N we can obtain numbers

$$N_{i,j} = \overline{c_1c_2\dots c_{n-5}aaaaa} + (b - a)(10^i + 10^j),$$

where $4 \geqslant i > j \geqslant 0$. Since the numbers $10^4 + 10^1$, $10^3 + 10^2$, $10^3 + 10^1$, $10^2 + 10^0$, $10^1 + 10^0$, $10^4 + 10^0$, $10^4 + 10^2$ yield 7 different remainders on dividing by 7, (respectively 0, 1, 2, 3, 4, 5 and 6), so do integers $(b-a)(10^i+10^j)$, where $4 \geqslant i > j \geqslant 0$. Hence among the numbers $N_{i,j}$ there exists a number which is a multiple of 7. □

Using these two lemmas and direct calculations by hand (we cannot get rid of them completely) we discover that no 4, 5 or 6 digit absolute primes exist. The details are rather messy, but using Lemmas 1 and 2 and easy divisibility checks modulo 11, 111 and 1111, we can reduce the list of candidates to numbers of the types $\overline{aaab}$, $\overline{abcc}$, $\overline{abccc}$, $\overline{abbcc}$, $\overline{abbbb}$, $\overline{abcccc}$ and $\overline{abbbbb}$. Many of the numbers of these types are divisible by 3, further reducing the search.

For numbers with more than six digits we have another result.

Lemma 3. If $N = \overline{c_1c_2\dots c_{n-6}aaaaab}$ is an absolute prime, $a \neq b$, then $K = \overline{c_1c_2\dots c_{n-6}}$ is divisible by 7.

Proof. By permutation of the right six digits of N we can obtain the numbers $N_i = K.10^6 + a.A_6 + (b - a).10^i$ for $0 \leqslant i \leqslant 5$. Since $(b - a)$ is even and powers 10^i, $0 \leqslant i \leqslant 5$, have different nonzero remainders on dividing by 7:

$$10^0 \equiv 1,\ 10^1 \equiv 3,\ 10^2 \equiv 2,\ 10^3 \equiv 6,\ 10^4 \equiv 4,\ 10^5 \equiv 5 \pmod 7.$$

The integers $(b - a).10^i$ have the same property. If the number $K.10^6 + a.A_6$ had nonzero remainder on dividing by 7, we would find some integer $(b-a).10^i$, which has just the opposite remainder, and obtain that N_i is divisible by 7. Since this is not the case, the number $K.10^6 + a.A_6$ is a multiple of 7. Knowing that $A_6 \equiv 0 \pmod 7$, we conclude that $K.10^6$, and hence K, is divisible by 7. □

We are now in a position to prove that absolute primes have a very specialised form.

Theorem 1. Every absolute prime number is either a repunit or can be obtained by a permutation of digits of the number

$$B_n(a, b) = \overline{aaa\dots ab}_{(n)} = aA_n + (b - a)$$

where a and b are different digits from $\{1, 3, 7, 9\}$.

Proof. Let n be the number or digits of N. We can suppose that $n > 6$. By the first two lemmas N does not contain in its decimal representation all four digits from the set indicated simultaneously, and it can contain three such digits only if N is a permutation of digits of the number $\overline{aaa\ldots abc}_{(n)}$. We show that this is impossible. Since N is an absolute prime, the numbers

$$N_1 = \overline{a\ldots acaaaaab}_{(n)}, \qquad N_2 = \overline{a\ldots abaaaaac}_{(n)}$$

are also absolute primes and by Lemma 3 the numbers $\overline{a\ldots ac}_{(n-6)}$ and $\overline{a\ldots ab}_{(n-6)}$ are both divisible by 7. Their difference, whose absolute value is $|b - c|$, is also divisible by 7, and this is a contradiction.

Hence N is either a repunit or contains only two digits. In the latter case we need Lemma 2 once more to deduce that one digit appears only once. □

The prime number 7 played a significant role in the preceding considerations. But other useful primes also exist and we are going to find some of them. Note that for us, the most useful property of 7 was the fact that the powers 10^i, $0 \leqslant i \leqslant 6$, had different nonzero remainders on dividing by 7. In general, by Fermat's Little Theorem for an arbitrary prime $p > 5$, we have $10^{p-1} \equiv 1 \pmod{p}$.

Let $h(p)$ be the least possible positive integer such that $10^{h(p)} \equiv 1 \pmod{p}$. It is obvious that $h(p)$ is a divisor of $p - 1$ and that $10^q \equiv 1 \pmod{p}$ implies $q \equiv 0 \pmod{h(p)}$. It is also easy to see that the powers 10^i, $0 \leqslant i \leqslant p - 1$, have different nonzero remainders on dividing by p as soon as $h(p) = p - 1$. When this is the case, 10 is said to be a primitive root modulo p.

Note that the number 10 is a primitive root modulo primes 17, 19, 23, 29, but 10 is not a primitive root modulo 13 since $10^6 \equiv 1 \pmod{13}$.

Lemma 4. Let A_n be a repunit and $p > 3$ be a prime. Then $A_n \equiv 0 \pmod{p}$ if and only if $n \equiv 0 \pmod{h(p)}$.

Proof. As $10^n = 9A_n + 1$, we have $A_n \equiv 0 \pmod{p}$ if and only if $10^n \equiv 1 \pmod{p}$ and this is equivalent to $n \equiv 0 \pmod{h(p)}$. □

This simple assertion gives us information about divisors of the repunits: in particular, if n is prime and $A_n = p_1p_2\ldots p_s$ is a factorization of A_n into prime factors, then $h(p_1) = h(p_2) = \ldots = h(p_s) = n$. For instance, $A_7 = 239 \times 4649$ and $h(239) = h(4649) = 7$.

Lemma 5. Let $B_n(a, b)$ be an absolute prime. Suppose that 10 is a primitive root modulo a prime number p, such that $(a, p) = 1$. Then n is a multiple of $(p - 1)$ as soon as $n \geqslant p - 1$.

Proof. Assume that $n \geqslant p - 1$. Consider the numbers

$$B_i = aA_{n-p+1}.10^{p-1} + aA_{p-1} + (b - a).10^i, \quad 0 \leqslant i \leqslant p - 2,$$

obtained from $B_n(a, b)$ by a permutation of the last $p - 1$ digits. Since the powers 10^i, $0 \leqslant i \leqslant p - 2$, yield all nonzero remainders on dividing by p, so do $(b - a).10^i$, $0 \leqslant i \leqslant p - 2$, and hence all B_i's can be simultaneously prime only in the case when the number $L = aA_{n-p+1}.10^{p-1} + aA_{p-1}$ is divisible by p. But then, since $(a.10^{p-1}, p) = 1$ and $A_{p-1} \equiv 0 \pmod{p}$, it follows that A_{n-p+1} is divisible by p. Since 10 is a primitive root modulo p then $h(p) = p - 1$, so, by Lemma 4, $n - p + 1$, and hence n, is divisible by $p - 1$. □

We can now prove that no absolute prime has between 7 and 16 digits. The details, although messy, are given in full.

Lemma 6. The numbers $B_n(a, b), 7 \leqslant n \leqslant 16$, are not absolutely prime.

*Proof.** Direct calculations here seem to be unavoidable. These calculations show that, by a permutation of digits, the numbers $B_n(a, b)$ can be converted into a multiple of 3, 17 or 19. The one exception $B_{14}(7, 9)$ can be converted into a multiple of 23.

(i) If $a = 1, 3$ or 9 then we can use Lemma 5. Note that 10 is a primitive root modulo 7 and $(a, 7) = 1$. Hence n is a multiple of $7 - 1 = 6$ for $n \geqslant 6$. Thus for $7 \leqslant n \leqslant 16$ the only possibility is $n = 12$. We check $B_{12}(a, b)$ by direct calculation (including the cases where $a = 7$).

Any permutation, N, of $B_{12}(a, b)$ takes the form

$$N = aA_{12} + (b - a).10^i \text{ where } 0 \leqslant i \leqslant 11.$$

Since $A_{12} \equiv 0 \pmod 3$ and $10^i \equiv 1 \pmod 3$ then

$$N \equiv 0 \pmod p \text{ if and only if } b \equiv a \pmod 3.$$

This disposes of the cases where $(a, b) = (1, 7), (7, 1), (3, 9)$ and $(9, 3)$.

We note that $A_{12} \equiv 9 \pmod{17}$ and $A_{12} \equiv 7 \pmod{19}$. The powers of 10 modulo 17 and 19 are given in Table 1.

TABLE 1

i	0	1	2	3	4	5	6	7	8	9	10
$10^i \pmod{17}$	1	10	15	14	4	6	9	5	16	7	2
$10^i \pmod{19}$	1	10	5	12	6	3	11	15	17	18	9

i	11	12	13	14	15	16	17	18
$10^i \pmod{17}$	3	13	11	8	12	1	10	15
$10^i \pmod{19}$	14	7	13	16	8	4	2	1

For each remaining choice of (a, b) we can select i such that

$$N = aA_{12} + (b - a).10^i \equiv 0 \pmod{17}$$

$$\text{or} \quad N = aA_{12} + (b - a).10^i \equiv 0 \pmod{19}.$$

For example if $a = 7, b = 3$ then $b - a = -4$, $7A_{12} \equiv 12 \pmod{17}$ and $7A_{12} \equiv 11 \pmod{19}$ so we need

$$12 - 4.10^i \equiv 0 \pmod{17} \tag{1}$$

$$\text{or} \quad 11 - 4.10^i \equiv 0 \pmod{19}. \tag{2}$$

We can use $10^{11} \equiv 3 \pmod{17}$, to satisfy (1) or $10^8 \equiv 17 \pmod{19}$ to satisfy (2), i.e. $17 | 377777777777$ and $19 | 777377777777$. Table 2 summarises the values of i needed to obtain composite permutations of $B_{12}(a, b)$.

TABLE 2

$a \backslash b$	1	3	7	9
1	*	(4)	*	(0)
3	(7)	*	(5)	*
7	*	(11)	*	[2]
9	[7]	*	[5]	*

$N = aA_{12} + (b - a).10^i \equiv 0$

where i has the value shown in the table

* $N \equiv 0 \pmod 3$

(4) Value of i for $N \equiv 0 \pmod{17}$

[5] Value of i for $N \equiv 0 \pmod{19}$

* It has not been possible to contact Dmitry Mavlo to obtain his agreement to the insertion of details in this proof, which were supplied by the editor.

For example, $B_{12}(9, 7) = 999999999997$ has the entry [5] showing that $9A_{12} + (7 - 9).10^5 = 999999799999 \equiv 0 \pmod{19}$.

(ii) If $a = 7$ we need to check permutations of $B_n(7, b)$ for $b = 1, 3$ and 9 and $7 \leqslant n \leqslant 16$. Such numbers take the form

$$N = 7A_n + (b - 7).10^i \qquad \text{where } 0 \leqslant i \leqslant n - 1.$$

Now $\quad 9A_n = 10^n - 1 \quad$ implies that

$$A_n \equiv 18A_n \equiv 2(10^n - 1) \pmod{17}$$

so $$7A_n \equiv -3(10^{n+1} - 1) \pmod{17}.$$

Also $$A_n \equiv 17 \times 9A_n \equiv 17(10^n - 1) \pmod{19}$$

so $$7A_n \equiv 5(10^{n+1} - 1) \pmod{19}.$$

Table 3 shows the values of $7A_n$ for $7 \leqslant n \leqslant 16$.

TABLE 3

n	7	8	9	10	11	10	13	14	15	16
$7A_n \pmod{17}$	6	16	14	11	15	4	13	1	0	3
$7A_n \pmod{19}$	4	9	2	8	11	3	16	15	5	0

Table 4 shows values of i for which

$$N = 7A_n + (b - 7).10^i \equiv 0 \pmod{17, 19 \text{ or } 23}.$$

TABLE 3

b	$b-7$	n	7	8	9	10	11	12	13	14	15	16
1	−6	$i =$	(0)	(3)	*	(8)	[2]	*	(7)	(11)	*	(6)
3	−4	$i =$	*	(4)	[1]	*	[8]	(0)	*	(9)	[4]	*
9	2	$i =$	*	(6)	1	*	(0)	(2)	*	◇9	[12]	*

Key: (3) $N \equiv 0 \pmod{17}$ ◇9 $N \equiv 0 \pmod{23}$

[1] $N \equiv 0 \pmod{19}$ * $N \equiv 0 \pmod{3}$

For example, if $b = 3$ and $n = 9$, we need to solve

$$N = 7A_9 + (3 - 7).10^i \equiv 0 \pmod{17, 19 \text{ or } 23}.$$

Noting that $7A_9 \equiv 2 \pmod{19}$ and $-4 \times 10^1 \equiv -2 \pmod{19}$ we have

$$N = 7A_9 + (3 - 7).10^1 \equiv 0 \pmod{19}$$

as shown by the entry [1] in the table. So 19 divides 777777737.

Theorem 2. Let N be an absolute prime, different from repunits, that contains $n > 3$ digits in its decimal representation. Then n is a multiple of 11088.

https://doi.org/10.2307/3618302 Published online by Cambridge University Press

Proof. According to the previous lemma we assume that $n > 16$. Since 10 is a primitive root modulo 17, Lemma 5 yields that n divides 16 and hence $n \geqslant 32$. We can repeat this argument three times, using primes 19, 23, 29, to obtain that n is a multiple of 18, 22 and 28 respectively. Hence n divides LCM(16, 18, 22, 28) = 11088. □

Richert [5] used in addition the primes 47, 59, 61, 97, 167, 179, 253, 383, 503, 863, 887, 983 to show that the number n of digits of the absolute prime number $B_n(a, b)$ is divisible by 321 653 308 662 329 838 581 993 760. He also mentioned that by using the tables of primes and their primitive roots up to 10^5, it is possible to show that $n > 6 \times 10^{175}$.

Finally we discuss which pairs (a, b) can appear in a decimal representation of the absolute prime $B_n(a, b)$ with $n > 3$ (if it exists at all!).

Theorem 3. If for $n > 3$ the number $B_n(a, b)$ is an absolute prime, then $(a,b) \neq (9, 7), (9, 1), (1, 7), (7, 1), (3, 9), (9, 3)$.

Proof. Write down the following equality:

$$9A_n - 2.10^r = 10^n - 1 - 2.10^r = 10^n + 1 - 2(10^r + 1).$$

We know from Theorem 2 that n must be even. Write $n = u.2^m$, where u is odd. Then for $r = 2^m$ the number $10^n + 1$ is divisible by $10^r + 1$, and the number $9A_n - 2.10^r$ is composite. But this number can be obtained by a permutation of digits of $B_n(9, 7)$.

Furthermore

$$B_n(9, 1) = 9A_n - 8.10^0 = 10^n - 9 = \left(10^{n/2} - 3\right)\left(10^{n/2} + 3\right),$$

and this number is also composite.

Finally, using Theorem 2, we see that n is divisible by 11088, and so is divisible by 3. Therefore the sums of the digits of $B_n(1, 7)$ and $B_n(7, 1)$ are also divisible by 3. Hence these numbers are composite as well as $B_n(9, 3)$ and $B_n(3, 9)$. □

References

1. M. Gardner, Mathematical games, *Scientific American* (June 1964) p. 118.
2. H. S. Williams, Some primes with interesting digits patterns, *Math. Comp.*, **32** (1978) pp. 1306-1310.
3. S. Yates, *Repunits and repetends*, Star Publ. Co., Boynton Beach, Florida, (1982).
4. P. Ribenboim, *The little book of big primes,* Springer-Verlag (1991) pp. 172-173.
5. H.-E. Richert, Om permutable primtall, *Norsk Matematiske Tiddskrift*, **33** (1951) pp. 50-54.
6. T. N. Bhargava and P. H. Doyle, On the existence of absolute primes, *Mathematics Magazine*, **47** (1974) p. 233.
7. A. W. Johnson, Absolute primes, *Mathematics Magazine*, **50** (1977) pp. 100-103.

DMITRY MAVLO
125195, Moscow, Fyestivalnaya 25-64, Russia

https://doi.org/10.2307/3618302 Published online by Cambridge University Press