6-1967

# A THEOREM ON REPEATING DECIMALS

William G. Leavitt
*University of Nebraska - Lincoln*

The American Mathematical Monthly, Vol. 74, No. 6 (Jun. - Jul., 1967), pp. 669-673.




# A THEOREM ON REPEATING DECIMALS

W. G. LEAVITT, University of Nebraska

It is well known that a real number is rational if and only if its decimal expansion is a repeating decimal. For example, $2/7 = .285714285714 \cdots$. Many students also know that if $n/m$ is a rational number reduced to lowest terms (that is, $n$ and $m$ relatively prime), then the number of repeated digits (we call this the *length of period*) depends only on $m$. Thus all fractions with denominator 7 have length of period 6. A sharp-eyed student may also notice that when the period (that is, the repeating digits) for 2/7 is split into its two half-periods 285 and 714, then the sum $285+714=999$ is a string of nines. A little experimentation makes it appear likely that this is always true for a fraction with the denominator 7, as well as for fractions with denominators 11, 13, or 17. A natural conjecture is that all primes with even length of period (note that many primes, such as 3 and 31, have odd length of period) will have a similar property. This conjecture is, in fact, true but it is unfortunately not a criterion for primeness, since many composite numbers (such as 77) also have the property. The relevant theorem appears not to be well known, although it was discovered many years ago. (L. E. Dickson [see 1, p. 163] attributes the result to E. Midy, Nantes, 1836). The proof of the theorem is simple and elegant, and since it also provides a nice example of the usefulness of the concept of the order of an element of a group, it deserves to be better known.

In the following, we will develop from the beginning the theory of repeating decimals. This is to provide the necessary machinery for the proof of Midy's theorem, as well as for completeness.

Write $(n, m)$ for the G.C.D. of $n$ and $m$. Assuming $n/m$ is a fraction reduced to lowest terms is thus equivalent to supposing $(n, m)=1$. (Note: we are interested only in positive fractions, so we restrict ourselves to $m>1$ and $n>0$.) Without loss of generality, we may also assume $(10, m)=1$, for if $m$ is divisible by 5 or 2 we could multiply numerator and denominator of $n/m$ by the appropriate power of 2 or 5 to obtain $n/m=10^{-h}n'/m'$ (for some integer $h\geqq 1$), where we still have $(n', m')=1$, and $m'$ is not divisible by either 2 or 5. Since dividing by $10^h$ simply moves the decimal place, it is clear that the repeating digits of $n/m$ are the same as those for $n'/m'$.

Write $n/m=c+h_1/m$ where $0<h_1<m$ and $c\geqq 0$ is an integer. Since $n=cm+h_1$, it is clear that we still have $(h_1, m)=1$. Also, since $c$ may be any integer, the

repeating digits we are after will be those of $h_1/m$. Now we are interested only in the digits obtained upon division by $m$ (not in the position of the decimal point). Thus when in the division process we bring down the first zero, we are actually dividing $10h_1$ by $m$. Let $a_1$ be the first digit in the quotient ($0 \leqq a_1 \leqq 9$) and let $h_2$ be the next remainder, then

$$h_2 = 10h_1 - a_1m.$$

Repeating the division process to obtain the next digit $a_2$ and the next remainder $h_3$,

$$h_3 = 10h_2 - a_2m.$$

Thus in general for any $t \geqq 2$,

$$h_t = 10h_{t-1} - a_{t-1}m. \tag{1}$$

Substituting for $h_{t-1}$ from the preceding relation of (1) yields

$$h_t = 10^2h_{t-2} - (10a_{t-2} + a_{t-1})m,$$

and in general for any $s$ (where $t > s \geqq 1$),

$$h_t = 10^sh_{t-s} - (10^{s-1}a_{t-s} + 10^{s-2}a_{t-s+1} + \cdots + 10a_{t-2} + a_{t-1})m. \tag{2}$$

Note that since $(m, 10h_1) = 1$ it follows from (1) that $m$ and $h_2$ have no common factors, so $(m, 10h_2) = 1$. It is thus clear (inductively) that for all the remainders $h_i$ we have $(m, 10h_i) = 1$. But the total number of integers less than $m$ and prime to $m$ is finite. (Remark that this number is the so-called "Euler $\phi$-function" $\phi(m)$). Accordingly there must exist integers $k$ and $k+r$ such that $h_k = h_{k+r}$. Then from (2)

$$10^rh_k - h_{k+r} = (10^{r-1}a_k + \cdots)m,$$

so that $m$ divides $(10^r - 1)h_k$. But $(m, h_k) = 1$, and so $m$ divides $10^r - 1$ (write this $m \mid 10^r - 1$). Thus $10^r \equiv 1 \pmod{m}$, and we assume that $r$ is the least such integer. Another way of saying this is: $r$ is the order of 10 in the multiplicative group (modulo $m$) of all integers $< m$ and relatively prime to $m$. As we mentioned above, the order of this group is $\phi(m)$, so by the Lagrange theorem, $r \mid \phi(m)$.

Writing, as we have indicated, the decimal expansion of $h_1/m$ as $.a_1a_2 \cdots$, we can prove:

THEOREM 1. *If $r$ is the order of 10 modulo $m$, then $a_{r+i} = a_i$ for all $i \geqq 1$. Conversely, if there exist positive integers $k$ and $u$ such that $a_{u+i} = a_i$ for all $i \geqq k$, then $r \mid u$.*

*Proof.* From (2) we have $h_{r+i} \equiv 10^rh_i \pmod{m}$, and since $10^r \equiv 1 \pmod{m}$, it follows that $h_{r+i} \equiv h_i \pmod{m}$. But all remainders $h_i < m$, so this implies $h_{r+i} = h_i$. Then from (1)

$$0 = h_{r+i+1} - h_{i+1} = (a_{r+i} - a_i)m,$$

whence

$$a_{r+i} = a_i. \tag{3}$$

Conversely, suppose $a_{u+i}=a_i$ for all $i \geqq k$. If we take $w$ large enough so that $wr \geqq k$, then this says that $a_{u+wr+i}=a_{wr+i}$ for all $i \geqq 1$, so by (3), $a_{u+i}=a_i$. Now let $d=(u, r)$ and take advantage of the fact that there exist integers $s$ and $t$ such that $su+tr=d$. We know that either $s$ or $t$ must be positive, so suppose $s>0$ (same proof if $t>0$). Then $a_{su+i}=a_i$ and by using (3), $a_{su+tr+i}=a_i$. Thus $a_{d+i}=a_i$. Once again, using (1), it is clear that

$$10(h_{d+i} - h_i) = h_{d+i+1} - h_{i+1}, \tag{4}$$

and $10(h_{d+i+1}-h_{i+1})=h_{d+i+2}-h_{i+2}$. Multiplying (4) by 10 and adding, yields

$$10^2(h_{d+i} - h_i) = h_{d+i+2} - h_{i+2}.$$

Thus (inductively), for any $q \geqq 1$,

$$10^q(h_{d+i} - h_i) = h_{d+i+q} - h_{i+q}.$$

But since all $h_i<m$, the right hand side (in absolute value) is less than $m$. If we choose $q$ large enough so that $10^q>m$, this relation could be true only if $h_{d+i}=h_i$. As in the discussion of above, this implies $10^d \equiv 1 \pmod{m}$. But $r$ is the order of 10 modulo $m$ and so from group theory we know that $r \mid d$. Since $d=(u, r)$, it follows that $r=d$ and so $r \mid u$.

From this theorem it is clear that the digits repeat if and only if we moved ahead $r$ digits (or some multiple of $r$ digits). That is to say, all fractions $h_1/m$ have periods of length precisely $r$, where $r$ is the order of 10 modulo $m$.

Note that when $m$ is prime, $\phi(m)=m-1$. Thus when $m$ is prime, $r \mid m-1$.

We now discuss the case of even period $r$.

LEMMA 1. *If there exists a positive integer $v$ such that $10^v \equiv -1 \pmod{m}$, then $r$ is even, where $r$ is the order of 10 modulo $m$.*

*Proof.* Since $10^{2v} \equiv 1 \pmod{m}$ and $r$ is the period of 10 modulo $m$, we know that $r \mid 2v$. If $r$ were odd then $r \mid v$ and thus $10^v \equiv 1 \pmod{m}$. But from $10^v \equiv -1 \pmod{m}$ we would then get $0 \equiv 2 \pmod{m}$, which is impossible (since we are assuming $(m, 10)=1$).

LEMMA 2. *If $m$ is prime and $r$ is even, then $10^{r/2} \equiv -1 \pmod{m}$.*

*Proof.* Write $r=2w$, then since $10^r \equiv 1 \pmod{m}$ we have $(10^w-1)(10^w+1) \equiv 0 \pmod{m}$. Since $m$ is prime it must divide one or the other of the terms on the left-hand side. But $r$ is the order of 10 and so $10^w \not\equiv 1 \pmod{m}$. Thus $m$ can only divide the second of the two factors, that is $10^w \equiv -1 \pmod{m}$.

We will continue to assume that $r=2w$ and that the period is $a_1 \cdots a_w a_{w+1} \cdots a_{2w}$. Let $c$ and $d$ be the two half-periods, so that $c=a_1 \cdots a_w$ and $d=a_{w+1} \cdots a_{2w}$ (or writing in terms of powers of 10, $c=a_1 10^{w-1}+a_2 10^{w-2} + \cdots + a_w$ and $d=a_{w+1}10^{w-1}+a_{w+2}10^{w-2}+ \cdots + a_{2w}$).

We can now prove Midy's theorem in a very simple way.

THEOREM 2. *If* $r=2w$ *and* $10^w \equiv -1 \pmod{m}$, *then* $c+d=10^w-1=99\cdots 9$.

*Proof.* From (2) we have $h_{w+1}=10^w h_1-cm$, $h_{2w+1}=10^w h_{w+1}-dm$. But $r=2w$ is the period, so $h_{2w+1}=h_1$ and thus

$$(h_1 + h_{w+1})(10^w - 1) = (c + d)m. \tag{5}$$

But by hypothesis $10^w-1\equiv -2 \pmod{m}$, so $10^w-1$ and $m$ are relatively prime. From (5) we therefore have that $m \mid h_1+h_{w+1}$. But each $h_i<m$ so $h_1+h_{w+1}<2m$. It can therefore be divisible by $m$ only if it equals $m$, that is, $h_1+h_{w+1}=m$. Hence $c+d=10^w-1$.

Notice that, once again, this theorem depends only on the denominator $m$ of the fraction. Let us say that an integer $m$ which satisfies Theorem 2 has the *nines-property*. From Lemma 2, it immediately follows that:

COROLLARY 1. *Every prime with even period has the nines-property.*

However, it is also true, as the following corollary shows, that there are many composite numbers with the nines-property.

COROLLARY 2. *If* $m \mid (10^p+1)$ *where* $p$ *is prime, then* $m$ *has the nines-property.*

*Proof.* By hypothesis, $10^p \equiv -1 \pmod{m}$ and so $10^{2p} \equiv 1 \pmod{m}$. Since $r$ is the order of 10 modulo $m$, it follows that $r \mid 2p$. If $r \mid 2$ then $m \mid 99$. But we always have $10^p \equiv 1 \pmod 3$ and so $10^p \not\equiv -1 \pmod 3$. Since $10^p \equiv -1 \pmod{m}$, it follows that $m$ and 3 are relatively prime. Thus in this case we could only have $m=11$, and it is easily verified directly that $m=11$ satisfies Theorem 2.

The remaining cases are $r=p$, which (as we saw in the proof of Lemma 1) contradicts $10^p \equiv -1 \pmod{m}$ or $r=2p$. In the latter case, Theorem 2 is evidently satisfied.

From this corollary, it follows that there are many composite nines-numbers. For example $10^3+1=7\cdot 11\cdot 13$ so that in addition to primes 7, 11, and 13 we also have composites 77, 91, and 143 (as well as 1001 itself) as nines-numbers.

COROLLARY 3. *If* $m$ *is prime and* $10^{(m-1)/2} \equiv -1 \pmod{m}$ *then* $m$ *is a nines-number.*

*Proof.* By Lemma 1, $r$ is even and so by Corollary 1, $m$ is a nines-number.

This corollary, together with the theory of quadratic residues, shows that any prime of form $40k \pm 7, \pm 11$, $\pm 17$, or $\pm 19$ is a nines-number. (For a discussion of quadratic residues see, for example, [2, Chapter 5]. The condition $10^{(m-1)/2} \equiv -1 \pmod{m}$ is the so-called Euler criterion that 10 should be a quadratic nonresidue of the prime $m$ [2, p. 46]. A determination of the form given for the primes for which 10 is a quadratic non-residue is found, as an example, in [2, p. 74].)

On the other hand, there are many primes $m$ with odd periods. If, for example, $(m-1)/2$ is odd and $10^{(m-1)/2} \equiv 1 \pmod{m}$, then clearly $r$ is odd, since it

must divide $(m-1)/2$. Again from the theory of quadratic residues, this class will contain all primes of form $40k+3$, $-13$, $-9$, or $-1$.

Note that Corollary 3 does not give all prime nines-numbers. One such prime which escapes Corollary 3 is 13.

Another familiar class of numbers, the Fermat numbers $m=2^{2^n}+1$, are covered by the following:

COROLLARY 4. *Every prime Fermat number* $>5$ *is a nines-number.*

*Proof.* This can be established directly, or one can use a simple induction to show that when $n \geqq 2$, $2^{2^n} \equiv 16 \pmod{40}$. The result is thus a special case of the remark following Corollary 3. This class is, of course, somewhat restricted since the only Fermat primes known which are $>5$ are given by $n=2$, 3, or 4.

This paper was presented at the May, 1965 meeting of the Nebraska Section of the Mathematical Association of America.

**References**

1. L. E. Dickson, History of the Theory of Numbers, vol. I, Chelsea, New York, 1952.
2. W. J. Leveque, Topics in Number Theory, vol. I, Addison-Wesley, Reading, Mass., 1956.