Wieferich Primes and Period Lengths for the Expansions of Fractions

GENE GARZA
JEFF YOUNG
University of Montevallo
Montevallo, Al 35115
genesr@prodragon.com

It is well known that some decimal expansions terminate, while others repeat, at least eventually, in patterns, which may be short or lengthy (we shall call this repeating pattern the *period* of the expansion). Here we will extend some known results while exploring expansions of fractions in any base. Our goal will be to find a formula for the length of the period of such expansions. The interested reader is referred to the recent award-winning article by Jones and Pearce, who show how to display such decimal expansions graphically [**3**].

We will consider both the expansions of (the reciprocals of) primes and of composites. It would seem that the easier part of this problem would be that of primes. However, there are difficulties/anomalies among primes that make it hard to find a formula that works in all cases. The most interesting such case is that of Wieferich primes, whose reciprocals are characterized by expansions whose periods are the same length as the periods of their squares. For example, the length of the period of $1/1093$ is 1092 which is the same as that of $1/1093^2$. This, as we shall see, is not normally the case. For someone seeking a simple formula, this is bad news. However, as our table at the end shows, Wieferich primes are quite rare.

Preliminaries Let's review what is meant by the expansion of a fraction and, in particular, the decimal expansion of a fraction. A few examples should suffice. In what follows, a line over digits in a decimal expansion (or expansion in any base b) will denote that those digits repeat infinitely often in that expansion.

$$\begin{aligned}
1/3 &= 0.\overline{3} && \text{(period 1, base 10)}\\
1/3 &= 0.\overline{01} && \text{(period 2, base 2)}\\
1/9 &= 0.\overline{1} && \text{(period 1, base 10)}\\
1/9 &= 0.\overline{000111} && \text{(period 6, base 2)}\\
1/27 &= 0.\overline{037} && \text{(period 3, base 10)}\\
1/27 &= 0.\overline{000010010111101101} && \text{(period 18, base 2)}
\end{aligned}$$

We say that $0.\overline{3} = 0.333\cdots$ is the expansion for $1/3$ in base 10 (decimal), that $0.\overline{01} = 0.010101\cdots$ is the expansion for $1/3$ in base 2, etc. The expansions in bases other than 10 can be obtained by long division after converting to the new base.

PROPOSITION. *The* period *of the expansion of* $1/x$*, in base* b*, is the smallest number, say* p*, for which* $b^p \equiv 1 \pmod{x}$.

That is, the period is the smallest number p such that $x \mid b^p - 1$. (This is basically Th. 4, section 15 from Dudley's book [**2**].)

DEFINITION 1. *By the* period of a number, x*, in base* b*, we shall mean the period of the expansion of* $1/x$ *in base* b.

When considering expansions, it will be our intention to concentrate on just the expansions of reciprocals of integers. This is sufficient since the length of the period of a fraction depends only on the denominator as long as the numerator is relatively prime to the denominator. To see this, consider the following in base ten:

$$\begin{aligned} 1/7 &= 0.\overline{142857} \\ 10/7 &= 1 + 3/7 \quad = 1.\overline{428571} \\ 100/7 &= 14 + 2/7 \quad = 14.\overline{285714} \\ 1000/7 &= 142 + 6/7 \quad = 142.\overline{857142} \\ 10000/7 &= 1428 + 4/7 \quad = 1428.\overline{571428} \\ 100000/7 &= 14285 + 5/7 = 14285.\overline{714285} \end{aligned}$$

Clearly then, the length of the expansion for any proper fraction with denominator 7 is 6. Different numerators simply serve to change the starting digit of the period. For other bases b, we need only note that $b = 10_b$; that is, in base b, b is 10. Thus, for any given base, a reduced proper fraction with denominator x will have a period of the same length as $1/x$.

Now consider the decimal expansions for 3, 6, 15, and 30:

$$\begin{aligned} 1/3 &= 0.\overline{3} \\ 1/6 &= 0.1\overline{6} \\ 1/15 &= 0.0\overline{6} \\ 1/30 &= 0.0\overline{3} \end{aligned}$$

These expansions suggest that factors of the base in the denominators do not affect the length of the period, but only delay its beginning. This is easily seen in the following example:

$$\begin{aligned} 1/7 &= 0.\overline{142857} \\ 1/35 &= 2/(10 \cdot 7) = .0\overline{285741} \\ 1/14 &= 5/(10 \cdot 7) = 0.0\overline{714285} \end{aligned}$$

Thus, when looking for the length of the period for an expansion it is enough to factor out all numbers from the denominator that divide the base, and determine the length of the period for the remaining number.

Periods of composites It seems natural to ask about the periods of composites whose factors may or may not be repeated and whose factors include none of the factors of the base. Some of these questions have been answered, and it is our purpose to consider these questions and to provide some additional answers.

First of all, it is well known that the expansion of a composite whose prime factors are not repeated and are not factors of the base has a period length that is just the lcm (least common multiple) of the periods of the individual factors [**2**]. For example, the period of 77 in base 10 is 6, since the period of 7 is 6, the period of 11 is 2, and lcm(6, 2) = 6. Similarly, the period of $341 = 11 \cdot 31$ is 30, since the period of 11 is 2 and the period of 31 is 15.

The "lcm rule" makes such problems quite manageable. It remains to consider powers of single primes. A few examples would again be useful. In base 10,

$$\begin{aligned} 1/7 &= 0.\overline{142857} && \text{(period 6)} \\ 1/7^2 &= 0.\overline{020408163265306122448979591836734693877551} && \text{(period 42)} \\ 1/7^3 &= 0.\overline{0029155\cdots} && \text{(period 294).} \end{aligned}$$

In base 2,

$$\begin{aligned} 1/7 &= 0.\overline{001} && \text{(period 3)} \\ 1/7^2 &= 0.\overline{000001010011100101111} && \text{(period 21)} \\ 1/7^3 &= 0.\overline{000000001\cdots} && \text{(period 147).} \end{aligned}$$

Careful observation leads one to conjecture that the period for, say x^n, when x is prime, is just the period of x multiplied by x^{n-1}. The unfortunate difficulty with attempting to prove this *power rule* conjecture is that it is not true! Counterexamples are abundant; just look at $1/3$, $1/9$, and 127 in base 10. The periods for the expansions of these numbers are 1, 1, and 3, respectively.

However, there is something special about 9 in base 10, which will eventually lead us to refine our conjecture. Actually, for any base b there is something special about the expansion of $1/(b-1)$. One can see this by considering the following geometric series in base b:

$$\frac{1}{b-1} = \frac{1}{b} + \frac{1}{b^2} + \frac{1}{b^3} + \cdots$$

In "decimal point" notation for base b, the expansion for $b-1$ is nothing more than $.111\cdots$. Because of this, any factor of $b-1$ has a period of length 1 in base b.

To illustrate, let $b-1$ be the product of, say, x and y (which are both less than b, and therefore are just "digits" in base b), and consider the expansion in base b of $1/x$. It is not too hard to see that it is nothing more than $.yyy\cdots$. For example in base 11, $1/2 = .555\cdots$ and $1/5 = .222\cdots$. This may be verified by observing that $1/2$ is nothing more than $1/2 = 5/11 + 5/11^2 + 5/11^3\cdots$. Likewise, $1/5 = 2/11 + 2/11^2 + 211^3\cdots$.

In base $b = 10$ the only factors of $b-1$ are 3 and 9. Here, we note that $10^1 \equiv 1 \pmod 3$ and that $10^1 \equiv 1 \pmod{3^2}$.

Period one primes For a particular base b, factors of $b-1$, which we call *period one primes*, provide counterexamples to our conjectured power rule formula. However, in any given base, period one primes will obviously be scarce so we simply eliminate all period one primes from consideration. In base 10, 3 is easily verified as the only period one prime. Of course, base 2 has no period one primes.

If we eliminate all period one primes and reconsider our conjecture, we are once again doomed—but for a different reason. As we shall see shortly, there are certain exceptions that occur, perhaps in all bases. So, what can we say with confidence? Well, it is certainly true, as we shall prove for any prime x and any base b, that $b^{px^{n-1}} \equiv 1 \pmod{x^n}$, where p is the period of x in base b.

Of course, this does not mean that px^{n-1} is actually the length of the period for the expansion of $1/x^n$. It is well known [2] that the period of x^n must divide $b^{px^{n-1}} - 1$, but we do not know that px^{n-1} is the smallest such number. What might happen in this case? In our earlier efforts to prove the power rule, the difficulty always occurred at the same point. It seemed unlikely at first that some x^2 might divide $b^p - 1$, where p is the period of x, since this would imply that the period of x^2 is the same as the period of x. This brings us to the *Wieferich primes*.

Wieferich primes A *Wieferich prime in base b* is a prime number, x that satisfies the congruence

$$b^{x-1} \equiv 1 \pmod{x^2}.$$

(In some discussions, the base b is limited to be 2.) Are they common? Do they exist in all bases? The answers to these questions are not all known. However, it is known [**5**] that Wieferich primes exist for many different bases, and we offer a table of Wieferich primes at the end of this Note.

In base 2, for example, 1093 and 3511 are Wieferich primes. This means that not only is $2^{1092} \equiv 1 \pmod{1093}$ and $2^{3510} \equiv 1 \pmod{3511}$ (which follows by Fermat's Little Theorm [**2**]), but also that $2^{1092} \equiv 1 \pmod{1093^2}$ and $2^{3510} \equiv 1 \pmod{3511^2}$. Crandall, Dilcher, and Pomerance [**1**] showed in 1997 that the only base-2 Wieferich primes below $4 \cdot 10^{12}$ are 1093 and 3511.

Actually, we will characterize Wieferich primes slightly differently. Of course, since $x - 1$ must be divisible by the period p, we change this definition to primes characterized by $b^p \equiv 1 \pmod{x^2}$. (In light of the upcoming corollary with $mq = x - 1$ and $n = 2$, we see that the new definition is equivalent to the previous one.) We note that if $b^p \equiv 1 \pmod{x^n}$ where n is anything higher than 2, then it is also true that $b^p \equiv 1 \pmod{x^2}$. Thus, for our purposes, if $b^p \equiv 1 \pmod{x^3}$ then x is a Wieferich prime for base b. We shall also refer to Wieferich primes as "primes with square periods" to emphasize the exceptional cases where the periods of the expansions for $1/x$ are the same as the periods of the expansions for their squares, $1/x^2$.

There are, of course, period one numbers with not only square periods, but cube periods and even higher. To see this, consider $9^1 \equiv 1 \pmod 2$, $9^1 \equiv 1 \pmod{2^2}$, $9^1 \equiv 1 \pmod{2^3}$. Here the period for each of 2, 2^2 and 2^3 is 1 in base 9. Two better examples might be $3^{10} \equiv 1 \pmod{11^2}$ and $7^4 \equiv 1 \pmod{5^2}$, where $3^{10} \equiv 1 \pmod{11}$ and $7^4 \equiv 1 \pmod 5$. It is thus apparent that if one is to compute, by way of some formula, the period for an expansion in any base, then those rare numbers with square periods must be considered and discounted. Indeed, we shall derive such a formula for the length of the period of a number whenever period one numbers and numbers with square periods are discarded. We will call this formula by the obvious name, the *power rule*.

The power rule Before stating our main theorem we need the following lemmas and corollaries:

LEMMA 1. *Suppose* $a_i \equiv 1 \pmod x$ *for each* a_i, $i = 1, \ldots, m$, *where* $m > 0$. *Then* $\sum a_i \equiv 0 \pmod x$ *if and only if* $m \equiv 0 \pmod x$.

The proof is left as an exercise for the reader.

COROLLARY. *If* $b^{mq} \equiv 1 \pmod{x^n}$ *for* $n \geq 1$ *where* q *is a multiple of the period of* x, *but* m *is not a multiple of* x, *then* $b^q \equiv 1 \pmod{x^n}$.

Proof. To see this we will rewrite $(b^{mq} - 1)$ as $(b^q)^m - 1$ and write q as dp where d is an integer. Then we factor $b^{mq} - 1 = b^{pmd} - 1$ as $(b^{pd} - 1)(b^{pd(m-1)} + b^{pd(m-2)} + \cdots + 1) = (b^q - 1)(b^{pd(m-1)} + b^{pd(m-2)} + \cdots + 1)$. Applying Lemma 1 to the second factor, which has m terms, each of which is congruent to 1 $(\mathrm{mod}\, x)$ (since p is the period of x), we see that x^n must divide $(b^q - 1)$ so that $b^q \equiv 1 \pmod{x^n}$. ∎

LEMMA 2. *If* x *is an odd prime,* $k > 1$, *and* $b^{px^{(k-1)}} \equiv 1 \pmod{x^{k+1}}$ *where* p *is the period of* x *in base* b, *then* $b^{px^{(k-2)}} \equiv 1 \pmod{x^k}$. (Note that x is selected to be odd, since 2 is period one for all odd bases. Otherwise, $7^2 \equiv 1 \pmod{2^4}$ while 7^1 is not 1 $(\mathrm{mod}\, 2^3)$ would be an obvious exception.)

Proof. Since p is the period of x, we have $b^p \equiv 1 \pmod x$ and we can write b^p as $(1 + nx)$ for some integer n. By the Binomial Theorem,

(1) $(b^p)^{x^{(k-1)}} \equiv 1 + nx^k \pmod{x^{k+1}}$ and

(2) $(b^p)^{x^{(k-2)}} \equiv 1 + nx^{k-1} \pmod{x^k}$.

But, by our hypothesis, $b^{px^{(k-1)}} \equiv 1 \pmod{x^{k+1}}$. This, along with (1) implies that $x \mid n$. The conclusion that $b^{px^{(k-2)}} \equiv 1 \pmod{x^k}$ then follows from (2) and the proof is complete. ∎

The idea behind Lemma 2 is that under certain conditions factors of x can be cancelled from congruences. Now we are prepared to state and prove our main result:

POWER RULE THEOREM. *If x is an odd prime, $N = x^n$, $n > 1$, and x is not a period one prime nor a Wieferich prime for base b, that is, not a prime with a square period, then the period of N is px^{n-1} where p is the period of x.*

Proof. We need to show two things:

I. $x^n \mid b^{px^{(n-1)}} - 1$.

II. If $x^n \mid b^Q - 1$, then $Q \geq px^{n-1}$.

I. This follows immediately from the binomial theorem since $b^p = 1 \pmod{x}$.

II. We must show for $n \geq 2$ that if $x^n \mid b^Q - 1$, then $Q \geq px^{n-1}$ for since we already know that it is true for $n = 1$. Assume not, that is, assume $Q < px^{n-1}$.

Once again, we know that Q must be a multiple of p, the period of x, since $x^n \mid b^Q - 1$ implies $x \mid b^Q - 1$. So let $Q = mp$. There are two cases to consider.

First, let's consider the case where m is a multiple of x. We write $m = rx^t$ where $1 \leq t < n - 1$ and r is not a multiple of x, so that $Q = rx^t p$. Here we have $x^n \mid b^{rx^t p} - 1$. By the Corollary, we can cancel the r so that $x^n \mid b^{px^t} - 1$. By Lemma 2, we can cancel one x from both sides of the expression to obtain $x^{n-1} \mid b^{px^{t-1}} - 1$. This we may repeat until we have $x^{n-t} \mid b^p - 1$ since under our assumptions $n - t \geq 2$. But this means that x is a Wieferich prime contrary to our hypotheses, so we conclude that m is not a multiple of x.

Second and finally, we consider what happens when m is not a multiple of x. In this case we have $x^n \mid b^{mp} - 1$. Once again using the Corollary, we can cancel m so that $x^n \mid b^p - 1$. Since $n \geq 2$, we conclude that x must be a Wieferich prime, which once again violates our hypothesis. This completes the proof of the Power Rule Theorem. ∎

Conclusion Together with the lcm rule, the power rule provides a formula for the period of the expansion for the reciprocal of any composite—as long as no factors of the composite are to be excluded such as Wieferich primes or period one numbers. This formula may be evaluated easily as long as the periods for the individual prime factors are known. Predicting the periods for an arbitrary prime is, however, still elusive. A table of Wieferich primes is provided to demonstrate their scarcity in bases up to 25 for numbers up to 2^{18}. (Period one numbers that qualify as Wieferich primes, such as 2 in base 9, have been removed from the table.) This table contains two particularly interesting entries: $18^6 \equiv 1 \pmod{7^2}$ and $19^6 \equiv 1 \pmod{7^2}$. The interesting part is that the following congruences are also valid: $18^6 \equiv 1 \pmod{7^3}$ and $19^6 \equiv 1 \pmod{7^3}$. This shows that there exist non period-one Wieferich primes with cube periods—in this case, for bases 18 and 19. For other bases this is still an open question [**5**]. Not quite so obvious from the table is the fact that $18^3 \equiv 1 \pmod{7^2}$ and $18^3 \equiv 1 \pmod{7^3}$. This answers, negatively, the question [**5**] whether Wieferich primes, x, must have periods of maximal length, that is, $x - 1$. Another such example is: $3^{10} \equiv 1 \pmod{11^2}$ and $3^5 \equiv 1 \pmod{11^2}$.

TABLE 1: Table of Wieferich primes up to 2^{18} for bases up to 25.

base	Wieferich primes	base	Wieferich primes
2	1093, 3511	14	29, 353
3	11	15	29131
4	1093, 3511	16	1093, 3511
5	20771, 40487	17	3, 46021, 48947
6	66161	18	5, 7, 37, 331, 33923
7	5	19	7, 13, 43, 137
8	3, 1093, 3511	20	281, 46457
9	11	21	None
10	487	22	13, 673
11	71	23	13
12	2693, 123653	24	5, 25633
13	863	25	20771, 40487

Open Questions To repeat, it is known that Wieferich primes satisfying the congruence, $b^p \equiv 1 \pmod{x^2}$, exist and are rare, but it is not known if any Wieferich primes, other than period one primes, satisfy the congruence $b^p \equiv 1 \pmod{x^n}$, $n > 2$ except for bases 18 and 19. Also, it is not known if there are Wieferich primes for each base; or even if the set of such primes is infinite (discounting period one primes, once again).

CONJECTURE. Wieferich primes exist for all bases and, furthermore, the following relationship holds in any base, b, for infinitely many primes, x, and for any value of n: $b^{x-1} \equiv 1 \pmod{x^n}$.

Acknowledgment. The authors would like to express their appreciation to the reviewers for many suggestions and improvements.

REFERENCES

1. Richard Crandall, Karl Dilcher, and Carl Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66** (1997), 433–449.
2. Underwood Dudley, *Elementary Number Theory*, W. H. Freeman and Company, San Francisco, 1969.
3. Rafe Jones and Jan Pearce, A postmodern view of fractions and the reciprocals of Fermat primes, this MAGAZINE **73**:2 (2000), 83–96.
4. William Levitt, Repeating decimals, *College Math. J.* **15** (1984), 299–308.
5. P. Ribenboim, *The Book of Prime Number Records*, 2nd ed., Springer, New York, 1989.