Tromsø Geophysical Observatory Reports

No.3

A property of repetends of fractions $1/m^{2n-1}$ with m prime, equal to 3 modulus 4, and n any positive integer

O.J. Rødseth, S. Wennevold, N.J. Armstrong and R.J.Armstrong

University of Tromsø, 2010

Cover photo: "Conrad Holmboe", Greenland, 1923. In 1922, the precursor of Tromsø Geophysical Observatory, The Geophysical Institute, acquired a 96' steamer to service field stations in the arctic. The boat became trapped in the ice on the eastern seaboard of Greenland in 1923 while unsuccessfully attempting to relieve the personnel there, and, irrevocably damaged by the ice, she limped to Iceland and was scrapped.

Foreword

The series *Tromsø Geophysical Observatory Reports* is primarily intended as a medium for publishing documents within the disciplines of Tromsø Geophysical Observatory: geomagnetism and upper atmosphere physics. However, when Richard Armstrong, a long time colleague of plasma physics at the Department of Physics, was looking for a place to preserve the present little piece of number theory preserved in print, we made an exception from the general rule.

Tromsø Geophysical Observatory Reports

No.3

A property of repetends of fraction $1/m^{2n-1}$ with m prime, equal to 3 modulus 4, and n any positive integer

Ø.J. Rødseth, S. Wennevold, N.J. Armstrong and R.J. Armstrong

University of Tromsø, 2010

A property of repetends of fractions $1/m^{2n-1}$ with m prime, equal to 3 modulus 4, and n any positive integer

Ø. J. Rødseth[1],S. Wennevold[2], N.J. Armstrong[3] and R.J. Armstrong[4]

[1]Dept. of Mathematics, University of Bergen,
[2]Computer Centre, University of Tromsø
[3]Museum of Archeology, Stavanger
[4]Dept. of Physics, University of Tromsø

Abstract

Consider the length of the repeating part (period length) of the digital expansion of 1/m as in Table 1 of Math.Gaz. 87 (November 2003) pp.437-443. When m is prime, and has the form 4t+3, with t a positive integer, we consider the sequence of period lengths as a function of base. We prove that for individual bases xm +u and (x+1)m-u, u<m, the period lengths are a factor 2 different. Here again x and u are positive integers. We show that the same result holds for any odd power of m.

1. Introduction

The study of integer numbers, Z, is of long standing and has, perhaps at first glance surprisingly, interested many of the most distinguished mathematicians in all ages. It is now perhaps therefore a well ploughed field; it is also true that with the advent of ever more powerful computers seemingly intractable problems are being solved and new applications are being discovered. The proving recently of Fermat's last theorem is an indication that classical number theory is still developing with new and exciting frontiers. In parallel the development of new applications is now quite common; indeed some would say that, at long last, this is occurring. With contributions to cryptography, coding theory, the improved acoustic design of concert halls, X-ray astronomy amongst others, [Schroeder, 2009] there is a new drive in the subject which was not present 50 years ago. We can expect many more applications. But it is worth noting that calculations in the general case can become inordinately complicated. Calculations of order as defined below can lead to situations where the P versus NP controversy is involved [*Fortnow*, 2009].

We consider the familiar topic of arithmetical fractions and their representation as decimals [*Green*,1963].We will consider, as has been done by others, for example *Yates* [1982] the representation not just as decimals but in other scales or bases. For example the fraction 1/3 is 0.333333… or 0.3 repeated in the decimal scale. But in the scale of 3 the fraction is just 0.1. Now consider 1/7: in decimal notation it is 0.142857 repeated, but in scale 7 it is just 0.1. In these two cases 3 and 142857 are examples of repetends. The relation of 'fraction' to scale is what we consider in this report. A rational fraction will always have a finite number of digits in its digital representation. But this finite number can be large; for instance 1/19 has in the decimal scale a repetend of 18 digits.

In *Armstrong and Armstrong* [1997] the symmetry obtained in expansions in digital form was shown to be linked to a symmetry of the return plot of the digits. For primes the condition for this to occur was simply that the number of digits in the repeated length was even. This is not always true for a composite divisor.

In *Armstrong and Armstrong* [2003] properties of repetends are related to a cyclic group formed by the least positive residues for a given modulus [*Budden*, 1972], using integer multiplication as the group multiplicative operation. Extension to scales other than 10 was considered . Properties of prime versus scale were studied with some applications.

In this report we both limit and extend the study commenced in the second contribution: we limit ourselves now to primes of form 4t+3, with t integral, thus ignoring 2 and primes of form 4t+1. While on the other hand we extend our study to all odd powers of the primes considered. For these numbers we show that for a given base a modulo (hereafter written 'mod') an odd power of a prime, m, of form 4t+3 the order (period length) of this is one half the order obtained for scale equal to –a mod m. We relate this to the study of Quadratic Residues.

2. Formulation of the Problem

As stated in the introduction this is a continuation of previous articles on the subject of repetends, the expansion of fractions in digital form. We show here a modified Table 1 from [*Armstrong and Armstrong*, 2003], with a particular scaling used there removed. This shows the period lengths of 1/m, m prime in the range 3 to 43. For m equal to 7 we see, for example, that the period length for a=13 is twice that for a=8.

This holds generally and we will now formulate the result of this work (We write the period length for a and m as here defined (the order of a for scale or base m) as $ord_m a$.) as follows:

$ord_m(xm+u) = z\, ord_m((x+1)m-u) = z\, ord_m(xm-u)$ with z=2 or ½.

The last equality follows from Lemma II of *Armstrong and Armstrong* [2003] . Again using this Lemma II we can write the result we shall prove as

$ord_m(u) = z\, ord_m(-u)$, with z=2 or 1/2.

Here m is prime of form 4t+3, and x, t and u are integral.

TABLE 1: Period Lengths, written in decimal notation, of 1/m with m prime for base a. 'X' indicates that the repetend does not exist, i.e. the fraction concerned has a finite digit representation in that scale. An extra column (with extension) shows some period lengths for $m=27=3^3$. The calculations use the remainders for each digit of the repetend.

a\m	3	5	7	11	13	17	19	23	29	31	37	41	43	27	a\m	27
3	X	4	6	5	3	16	18	11	28	30	18	8	42	X	21	X
4	1	2	3	5	6	4	9	11	14	5	18	10	7	9	22	9
5	2	X	6	5	4	16	9	22	14	3	36	20	42	18	23	18
6	X	1	2	10	12	16	9	11	14	6	4	40	3	X	24	X
7	1	4	X	10	12	16	3	22	7	15	9	40	6	9	25	9
8	2	4	1	10	4	8	6	11	28	5	12	20	14	6	26	2
9	X	2	3	5	3	8	9	11	14	15	9	4	21	X	27	X
10	1	X	6	2	6	16	18	22	28	15	3	5	21	3	28	1
11	2	1	3	X	12	16	3	22	28	30	6	40	7	18	29	18
12	X	4	6	1	2	16	6	11	4	30	9	40	42	X	30	X
13	1	4	2	10	X	4	18	11	14	30	36	40	21	9	31	9
14	2	2	X	5	1	16	18	22	28	15	12	8	21	18	32	18
15	X	X	1	5	12	8	18	22	28	10	36	40	21	X	33	X
16	1	1	3	5	3	2	9	11	7	5	9	5	7	9	34	9
17	2	4	6	10	6	X	9	22	4	30	36	40	21	6	35	6
18	X	4	3	10	4	1	2	11	28	15	36	5	42	X	36	X
19	1	2	6	10	12	8	X	22	28	15	36	40	42	3	37	3
20	2	X	2	5	12	16	1	22	7	15	36	20	42	18	38	18

Note that symbols in this work will usually represent positive integers; z here being an exception. The articles by *Armstrong and Armstrong* [1997] and [2003] were limited to irreducible fractions w/m where m is prime; here we relax this restriction for m to include irreducible fractions w/m^{2n+1}, with m prime of form 4t+3, at the conclusion of this work. Φ (s) represents the Euler function, given by

$s\{(1-(1/p))(1-(1/q))(1-(1/r))\ldots.)$

where p,q,r,….are the distinct prime factors of s.

3. Lemma

If m=3 mod 4, $\Phi(m)=2$ mod 4 and (a,m)=1 then 2 divides $ord_m(a)$ just once; for otherwise 4 would divide $\Phi(m)$.

4. Theorem

Let m be a prime of form 4n+3 and (a,m)=1 .

Then $ord_m(a)$ and $ord_m(-a)$ will have different parity and that which is even will be twice the other.

Proof Step 1

Let $r = ord_m(a)$ and $s = ord_m(-a)$ and assume they are both odd.

Then $(-a)^{2r} = 1$ mod m implies s¦ 2r . Since both are odd s¦r.

Now let r=qs, and so $(-1)^r =(- a)^r =(-a)^{qs} =1$ implying r to be even, a contradiction.

Step 2

From Step 1 we know that one order is even, and we can then choose b from a and –a such that $ord_m(b) =2t$.

From the Lemma t is odd. Let u= $ord_m(-b)$.

Now $(b^t - 1)(b^t + 1) = (b^{2t} -1) \equiv 0$ mod m.

Note $b^t =1$ mod m would imply $ord_m(b) = t$, i.e. not 2t.

So $(b)^t = -1 \pmod m$ and since t is odd, $(-b)^t = 1$. Therefore $u|t$.

From $b^{2u} = (-b)^{2u} = 1 \bmod m$ yields $2t¦\ 2u$ i.e. $t¦u$.

So t=u giving $ord_m(-b)$ as odd and equal to (1/2) $ord_m(b)$,

as was to be proved.

5. Corollary

The theorem also holds if m is an odd power of an odd prime.

Let $h=m^{(2n+1)}$ where m is an odd prime .

Since $1^{2n} = 3^{2n} = 1 \bmod 4$ we see that h=m mod 4.

With m prime $\Phi(h) = \Phi(m^{2n+1}) = m^{2n}(m-1)$.

Therefore if h=3 mod 4 (or equivalently m=3 mod 4) then

ord(h)=2 mod 4.

Thus replacing m by h in the theorem we have that the conditions of the Lemma are fulfilled and the Theorem will still hold.The right most column in Table 1 is an example of this result with m=3 and n=1.

6. Note 1: Relation of the result to Quadratic Residues (QR)[*Yates,1982*].

We show that the b value of the Theorem which is of odd order is a QR modulus m and that the converse is also true.

We prove first that an element, b, which is of odd order is a QR.

For then $b^{2n+1}=1$. We assume all numbers are mod m.

So $b=b^{2n+2}=b^{2(n+1)}$ and therefore b by definition is QR, for (n+1) is an integer and b^{n+1} is also an integer.

Now we show that a QR element implies that it is of odd order.

Take $b=x^2$, with ord(x)=t and ord(b)=s. We assume again that numbers are mod m.

Assume s=2h, an even number, to demonstrate that this leads to a contradiction.

We have $1=b^s=x^{4h}$; consequently $t ¦ 4h$

But 4 does not divide t since it is of the form 4k+3.

So $t ¦ h$, leading to $1=x^h=b^{s/4}$.

This would mean that the order of b was less than or equal to s/4, which is a contradiction.

We have then shown the equivalence of odd order with the property of being a QR.

7. Note 2: If b is of odd order, q, then q is also the order of b^w, with w= 2^v, for all v, with v assumed as usual to be a positive integer .

The proof is straightforward, closely paralleling the procedure followed in the theorem. Many examples of this result are evident in Table 1.

Acknowledgement R.A. is grateful to Prof. D. MacHale for cogent comments on the presentation of this work.

References

1. Armstrong, N.J. and Armstrong, R.J., An observation concerning repetends, *Math.Gaz.* 81(March 1997) 101-104.
2. Armstrong , N.J. and Armstrong, , R.J. Some properties of repetends, *Math.Gaz.* 87(November 2003) 437- 443.
3. Budden, F.J., The Fascination of Groups, Cambridge University Press, Cambridge, 1972.

4. Fortnow, L., The Status of the P versus NP Problem, *Comm. Of the ACM*, 52 (2009) 78-86
5. R.E.Green, Recurring Decimals, *Math.Gaz.* 48(March 1963) 25-33
6. Schroeder,M.R., Number Theory in Science and Communication, Springer,Berlin, 2009 (5th edition).
7. Yates, S., Repunits and Repetends, published privately by the author, Delray Beach, Fla.,USA, 1982.

Tromsø Geophysical Observatory Reports

No. 1. Chris M. Hall & Bjørn Ove Husøy: Altitude calibration of the Tromsø Medium Frequency Radar. 2004

No. 2. Truls Lynne Hansen & Per Pippin Aspaas: Maximillian Hell's geomagnetic observations in Norway 1769. 2005

No.3. Ø.J. Rødseth, S. Wennerwold, N.J. Armstrong and R.J. Armstrong: A property of fractions $1/m^{2n+1}$ with m prime equal to modulus 4, and n any positive integer. 2010

Tromsø Geophysical Observatory
University of Tromsø
N-9037 Tromsø
Norway
ISSN: 1504-1174