INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 5 (2005), #A19

DECIMAL EXPANSION OF 1/P AND SUBGROUP SUMS

Ankit Gupta
Department of Mathematics and Statistics, Indian Institute of Technology, Kanpur, U.P. 208016, India
ankitg@iitk.ac.in

B. Sury
Stat-Math Unit, Indian Statistical Institute, Bangalore, 560 059, India
sury@isibang.ac.in

Received: 10/30/04, Revised: 7/1/05, Accepted: 8/9/05, Published: 8/10/05

Abstract

It is well-known and elementary to show that for any prime $p \neq 2, 5$, the decimal expansion of $1/p$ is periodic with period dividing $p-1$. In fact, the period is $p-1$ if and only if 10 is a primitive root (mod p). In 1836, Midy proved that if $1/p$ has even period $2d$, then writing

$$\frac{1}{p} = 0.(UV)(UV)\cdots\cdots$$

where U, V are blocks of d digits each, one has $U + V = 10^d - 1$ (that is, it is a block of d 9s). In January 2004, Brian Ginsberg, a student from Yale University generalized Midy's theorem to decimal expansions with period $3d$. His proof is elementary. The purpose of this note is to solve the problem in complete generality. This involves some interesting questions about the cyclic group of order $p-1$.

1. Sums in $(\mathbf{Z}/p\mathbf{Z})^*$

We start with a simple fact that will be useful for us.

Lemma 1. *Let $p > 2$ be a prime and $l > 1$ be a divisor of $p-1$. Let $G(p,l) \subset \{1, 2, \cdots, p-1\}$ be the representatives of the unique subgroup of order l in the group $(\mathbf{Z}/p\mathbf{Z})^*$. Then, the sum $s(p,l) := \sum_{g \in G(p,l)} g = rp$ for some natural number r.*

Proof. If G is a nontrivial subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$ and $x \neq e$ in G, then,

$$x \sum_{g \in G} g = \sum_{h \in G} h$$

so that $\sum_{g \in G} g \equiv 0 \pmod{p}$. □

The connection of Lemma 1 with the decimal expansion of $1/p$ is seen from Theorem 1 below.

Theorem 1. *Let $p > 5$ be a prime and suppose $l > 1$ is a natural number such that the decimal expansion of $1/p$ is periodic, of period ld. Write*

$$\frac{1}{p} = 0.(U_1U_2\cdots U_l)(U_1U_2\cdots U_l)\cdots\cdots$$

where each U_i consists of d digits. Then, one has

$$U_1 + U_2 + \cdots + U_l = r(10^d - 1)$$

where $s(p,l) = rp$.

This immediately gives a (different) proof of Midy's and Ginsberg's theorems.

Corollary 1. *For a prime $p \neq 2, 5$, and with notations as above, we have $s(p,2) = s(p,3) = p$. In particular, Midy's theorem and Ginsberg's theorem follow.*

Proof. Note that $G(p,2) = \{1, p-1\}$ and $G(p,3) = \{1, x, y\}$ for some $x, y < p-1$. Since $1 + x + y \equiv 0 \pmod p$ and is less than $1 + 2(p-1)$, it follows that $1 + x + y = p$. □

Proof of Theorem 1. Note that since 10 has order $ld \pmod p$, the elements of $G(p,l)$ are the images of $10^{id}; 1 \leq i \leq l$ modulo p. Thus, if r_i is the fractional part $\{10^{id}/p\}$, then,

$$\sum_{i=1}^{l} r_i = r.$$

Now,

$$\frac{1}{p} = 0.(U_1U_2\cdots U_l)(U_1U_2\cdots U_l)\cdots\cdots$$

$$\frac{10^d}{p} = U_1.(U_2U_3\cdots U_lU_1)(U_2U_3\cdots U_lU_1)\cdots\cdots$$

$$\frac{10^{2d}}{p} = U_1U_2.(U_3U_4\cdots U_1U_2)(U_3U_4\cdots U_1U_2)\cdots\cdots$$

$$\vdots$$

$$\frac{10^{(l-1)d}}{p} = U_1U_2\cdots U_{l-1}.(U_lU_1\cdots U_{l-1})(U_lU_1\cdots U_{l-1})\cdots\cdots$$

Thus, we have $U_1U_2\cdots U_i = [10^{id}/p]$ for all $i < l$. Hence, the sum of the numbers to the left of the decimal points on the right-hand sides of the above equations is $\sum_{i=1}^{l-1}[10^{id}/p]$. Therefore, the sum of the decimals on the right-hand side of the above equations is $\sum_{i=0}^{l-1}\{10^{id}/p\} = r$. But this sum of decimals is clearly $\frac{U_1+U_2+\cdots+U_l}{10^d-1}$. This proves that $U_1 + \cdots + U_l = r(10^d - 1)$. □

In view of this Theorem 1, when one looks for generalizations of Midy's theorem etc., it is sufficient to consider the more general problem of determining the value of $s(p,l)$ for various primes p and divisors l of $p-1$. Note that the latter problem is more general because the former one addresses only the cases when l divides the order of 10 (mod p). The computation of $s(p,l)$ for any prime p and any divisor l of $p-1$ is equivalent to the computation of the sum $U_1 + \cdots + U_l$ where $1/p$ is expressed in base b for a primitive root b (mod p). In particular, the question arises as to whether $s(p,l)$ equals p for any $l > 3$ at all? We shall now show that there are some cases when it does and some cases when it does not.

2. Mersenne, Sophie Germain, and Dirichlet

Mersenne primes are prime numbers of the form $2^n - 1$, in which case n must also be a prime. We then have two primes p, n with p much larger than n. Another class of primes is the set of those primes q for which $2q+1$ is also prime. They came up in the proof of the first case of Fermat's last theorem due to Sophie Germain for such primes q. In contrast with the Mersenne primes, here the two primes $q, 2q+1$ are comparable in size. Neither of these classes of primes is known to be infinite. The behaviour of $s(p,l)$ is different for these two classes as we show now.

Lemma 2. *Let $p = 2^l - 1$ be a (Mersenne) prime. Then, $s(p,l) = p$.*

Proof. Clearly, $2^l = 1$ in $(\mathbf{Z}/p\mathbf{Z})^*$. Therefore, 2 has order l in this group. This implies that $G(p,l) = \{1, 2, 2^2, \cdots, 2^{l-1}\}$. Hence $s(p,l) = 2^l - 1 = p$. □

Lemma 3. *Let $l > 3$ be a (Sophie Germain) prime so that $p = 2l + 1$ is also prime. Then, $s(p,l) > p$.*

Proof. Evidently, $s(p,l) \geq 1 + 2 + 3 + \cdots + (l-1) = l(l-1)/2 > 2l + 1$ if $l > 5$. For $l = 5$, it is directly checked that $s(11,5) = 1 + 3 + 4 + 5 + 9 = 22$. □

The question as to whether either of the cases $s(p,l) = p$ and $s(p,l) > p$ can occur infinitely often seems to be difficult to answer. The next result we prove below indicates that if p is comparable in size to l, then $s(p,l) > p$ for large l. Let us note that the hypothesis of this proposition is conjecturally satisfied for large enough l in the following sense. First, by Dirichlet's theorem on primes in progression, given any l, there is a prime p so that $p \equiv 1 \pmod{l}$. The prime number theorem gives the lower bound for the smallest such p to be at least of the order $l \ \log l$ ([R], p.282). Wagstaff noted in 1979 ([R], p.283) that, for heuristic reasons, the smallest such prime is of the order of $l(\log l)^2$ for large l except for a set of density zero. Kumar Murty showed in his Bachelor's thesis ([R], p.281) of 1977 that except for a set of positive integers l not belonging to a sequence of density zero, for each $\epsilon > 0$, the least $p \equiv 1 \pmod{l}$ satisfies $p < l^{2+\epsilon}$. The pair correlation conjecture – a deep conjecture of analytic number theory about the zeroes of the Riemann zeta function – would imply that for any large l, there is a prime $p \equiv 1 \pmod{l}$ such that $p < l^{1+\epsilon}$. The smallest exponent k such that $p < Cl^k$ for some C and all large enough l, is known as Linnik's constant; the best unconditional result in analytic number theory available at present is due to Heath-Brown ([H]) and gives us $k \leq 5.5$. Even the existence of Linnik's constant is a very deep theorem due to Linnik.

Proposition 1. *For any prime $p \geq 11$ and any prime divisor l of $p-1$ such that $p < l^2/2$, one has $s(p,l) > p$.*

Proof. For any $p \equiv 1 \pmod{l}$, let the unique subgroup of order l of $(\mathbf{Z}/p\mathbf{Z})^*$ be generated by x. If $G(p,l) = \{1, x_1, \cdots, x_{l-1}\}$ with x_i the residue of x^i, then at least one of x_i and x_{l-i} is greater than $\sqrt{p}$, for each $1 \leq i < l$. The reason is as follows. If both x_i, x_{l-i} are at most $\sqrt{p}$, then we have a contradiction since $1 \equiv x_i x_{l-i} \pmod{p}$. Therefore, at least half of the x_i's for $i \geq 1$ are more than $\sqrt{p}$. Thus, the largest $(l-1)/2$ of them are bigger than the numbers $\sqrt{p}, \sqrt{p}+1, \cdots, \sqrt{p}+(l-3)/2$. The others (including 1) are bigger than or equal to the numbers $1, 2, \cdots, (l+1)/2$. Hence

$$s(p,l) > \sum_{i=1}^{(l+1)/2} i + \frac{\sqrt{p}(l-1)}{2} + \sum_{j=1}^{(l-3)/2} j = \frac{l^2+3}{4} + \frac{\sqrt{p}(l-1)}{2}.$$

Since $\sqrt{p} < l/\sqrt{2}$, we can see that $s(p,l) > p$. This completes the proof. □

Given a prime p and any divisor n of $p-1$, it is possible to give an expression for the natural number $\frac{s(p,n)}{p}$. We do this below using an element b of order $n \pmod{p}$ (knowing b is essentially equivalent to knowing a primitive root $a \pmod{p}$ because one may take $b = a^{(p-1)/n}$). In the formula below, we write $\log_b$ to denote the logarithm to the base b. In other words, $[\log_b(d)] = r$ if $b^r \leq d < b^{r+1}$.

Proposition 2. *Let p be a prime, $n|(p-1)$, and $b < p$ be an element of order n in $(\mathbf{Z}/p\mathbf{Z})^*$. Then, we have*

$$\frac{s(p,n)}{p} = \frac{b^n - 1}{p(b-1)} - (n-1)[\frac{b^{n-1}}{p}] + \sum_{i=1}^{[\frac{b^{n-1}}{p}]} [\log_b(ip)].$$

For example, take $p = 11, n = 5, b = 4$. Then, $s(p,n) = 1+4+5+9+3 = 22$. Since $[\log_4(11i)]$ equals 1 for $i = 1$, equals 2 for $2 \leq i \leq 5$ and, equals 3 for $6 \leq i \leq 23$, the expression on the right side of the proposition gives $31 - 92 + (1+8+54) = 2$. Another class of examples easily seen from the above is that of Mersenne primes $p = 2^n - 1$. Then, $b = 2$ and the sum is empty and one evidently has $\frac{s(p,n)}{p} = 1$.

Proof. We separate the powers $1, b, b^2, \ldots, b^{n-1}$ into the various ranges $((i-1)p, ip)$ for $1 \leq i \leq [\frac{b^{n-1}}{p}]$. Now, the largest r for which the power b^r is in the range $(0,p)$, equals $[\log_b p]$. Counting in this manner, we have $b^{r_i+1}, b^{r_i+2}, \ldots, b^{r_{i+1}}$ in the range $(ip, (i+1)p)$ where $r_i = [\log_b(ip)]$. These powers contribute $\sum_{j=r_i+1}^{r_{i+1}} (b_j - ip)$ to the sum $s(p,n)$. If t

is the largest number for which $r_t < n-1$, then the interval $(tp,(t+1)p)$ contains the powers $b^{r_t+1},\cdots,b^{n-1}$. Hence, we get

$$s(p,n)=\sum_{j=0}^{n-1} b^j - \sum_{i=1}^{t-1}(r_{i+1}-r_i)ip-(n-1-r_t)tp,$$

which simplifies to the expression

$$s(p,n)=\frac{b^n-1}{b-1}-p(n-1)[\frac{b^{n-1}}{p}]+\sum_{i=1}^{[\frac{b^{n-1}}{p}]} p[\log_b(ip)].$$

This completes the proof. □

We end with the following question which is interesting because finding a primitive root (mod p) is far from easy.

Question. *Given any prime p and any divisor $n>1$ of $p-1$, give an expression for the natural number $s(p,n)/p$ in terms of p and n alone.*

Acknowledgement. We would like to thank the referee for a careful reading of the paper and for suggestions to improve the language.

References

[G] Brian D. Ginsberg, 'Midy's (nearly) secret theorem - an extension after 165 years', *College Math. Journal* **35** (2004), 26-30.

[H] D.R.Heath-Brown, 'Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression', *Proc. Lond. Math. Soc.* **64** (1992), 265-338.

[R] P. Ribenboim, The new book of prime number records, 3rd ed., Springer, 1996.