Proc. Camb. Phil. Soc. (1974), **76**, 417
PCPS 76–42
Printed in Great Britain

On the digits of the multiples of an irrational p-adic number

By KURT MAHLER
Canberra

(*Received* 4 *March* 1974)

Let α be an irrational p-adic number, r an arbitrary positive integer. Our aim is to prove that there exists a rational integer X satisfying

$$1 \leqslant X < p^{2p^r}$$

such that every possible sequence of r digits $0, 1, \ldots, p-1$ occurs infinitely often in the canonical p-adic series for $X\alpha$. It is clear that it suffices to prove this result for p-adic *integers*.

In a short paper written after the present one (*Bulletin Australian Mathematical Society* 8 (1973), 191–203) I had proved the analogous result for *real* irrational numbers. The method used in these two papers can easily be extended to finite sets of real and p-adic numbers.

1. Let p be a prime, and let

$$\alpha = \sum_{k=0}^{\infty} a_k p^k$$

be a fixed irrational p-adic integer. Here the coefficients a_k are digits

$$0, 1, 2, \ldots, p-1.$$

If l is any positive integer, put

$$A_l = \sum_{k=1}^{l-1} a_k p^k.$$

Then A_l is a rational integer satisfying

$$|\alpha - A_l|_p \leqslant p^{-l} \quad \text{and} \quad 0 \leqslant A_l \leqslant p^l - 1. \tag{1}$$

Next let x and y be two rational integers not both zero. Since α is irrational,

$$\alpha x - y \neq 0.$$

Assume that the integer l is already so large that

$$|\alpha x - y|_p > p^{-l}. \tag{2}$$

It follows then from

$$A_l X - y = (\alpha x - y) - x(\alpha - A_l)$$

and

$$|x(\alpha - A_l)|_p = |x|_p \, |\alpha - A_l|_p \leqslant p^{-l}$$

that

$$|ax - y|_p > |x(\alpha - A_l)|_p$$

and therefore

$$|A_l x - y|_p = |\alpha x - y|_p > 0. \tag{3}$$

2. Further denote by n and N any two positive integers satisfying

$$1 \leqslant n \leqslant N.$$

If $\quad |\alpha x - y|_p \leqslant p^{-N}$ and hence by (3) also $|A_l x - y|_p \leqslant p^{-N}$,

then there exists to x and y a third rational integer z such that

$$A_l x - y = -p^N z.$$

The two linear forms in x and z,

$$p^{-n}x \quad \text{and} \quad p^{-(N-n)}(A_l x + p^N z)$$

have the determinant

$$\begin{vmatrix} p^{-n} & 0 \\ p^{-(N-n)}A_l & p^n \end{vmatrix} = 1.$$

Therefore, by Minkowski's theorem on linear forms, there exist two rational integers x and z not both zero such that

$$|x| \leqslant p^n \quad \text{and} \quad |A_l x + p^N z| < p^{N-n}.$$

These two inequalities imply, first, that

$$x \neq 0.$$

Secondly, on defining y in terms of x and z by

$$y = A_l x + p^N z,$$

it follows that x and y satisfy the pair of inequalities

$$|y| < p^{N-n} \quad \text{and} \quad |\alpha x - y|_p \leqslant p^{-N}.$$

A second solution of the same pair of inequalities is given by $-x$, $-y$; hence, without loss of generality, it may be assumed that

$$y \geqslant 0.$$

Hence the following result has been proved.

THEOREM 1. *Let α be an irrational p-adic integer, and let n and N be two rational integers satisfying*

$$1 \leqslant n \leqslant N.$$

Then two rational integers x and y exist such that

$$1 \leqslant |x| \leqslant p^n, \quad 0 \leqslant y < p^{N-n}, \quad |\alpha x - y|_p \leqslant p^{-N}.$$

Remark. Assume that n and N have the further property that

$$|\alpha|_p > p^{-(N-n)}.$$

By the lower and upper bounds for $|x|$,

$$|x|_p \geqslant p^{-n}$$

and hence

$$|\alpha x|_p > p^{-N}.$$

Hence in this case the restriction on y in the theorem can be replaced by the stronger one that

$$1 \leqslant y < p^{N-n}.$$

3. In Theorem 1, keep n fixed, but allow N to run over all the integers

$$n, \quad n+1, \quad n+2, \quad \ldots.$$

To each such value of N, there exists a pair of rational integers x_N, y_N satisfying

$$1 \leqslant |x_N| \leqslant p^n, \quad 0 \leqslant y_N < p^{N-n}, \quad |\alpha x_N - y_N|_p \leqslant p^{-N}. \tag{4}$$

Moreover, as soon as N is sufficiently large, y_N is positive. In fact, it is clear that y_N tends to infinity as N increases indefinitely.

For all N the integer x_N assumes only the finitely many values

$$\mp 1, \quad \mp 2, \quad \ldots, \quad \mp p^n.$$

It follows that there exists an infinite sequence $\{N_k\}$ of values of N satisfying

$$N_1 < N_2 < N_3 < \ldots$$

such that

$$x_{N_1} = x_{N_2} = x_{N_3} = \ldots = x_0 \quad \text{say},$$

retains a constant value independent of N_k, while

$$y_{N_k} \geqslant 1 \quad \text{for all } k.$$

Hence, for the N in $\{N_k\}$, (4) takes the stronger form

$$1 \leqslant |x_0| \leqslant p^n, \quad 1 \leqslant y_{N_k} < p^{N_k-n}, \quad |\alpha x_0 - y_{N_k}|_p \leqslant p^{-N_k} \tag{5}$$

for all k. The constant product αx_0 is again an irrational p-adic integer, say, with the series

$$\alpha x_0 = \sum_{h=0}^{\infty} b_h p^h,$$

where the b_h are digits $0, 1, 2, \ldots, p-1$. Write similarly the positive integers y_{N_k} as p-adic series

$$y_{N_k} = \sum_{h=0}^{\infty} c_{hk} p^h \quad (k = 1, 2, 3, \ldots),$$

where also the c_{hk} are digits.

Then, from the upper bound for y_{N_k},

$$c_{hk} = 0 \quad \text{if} \quad h \geqslant N_k - n,$$

while the upper estimate for $|\alpha x_0 - y_{N_k}|_p$ implies that

$$c_{hk} = b_h \quad \text{for} \quad h = 0, 1, 2, \ldots, N_k - 1.$$

From these two sets of equations we deduce immediately that for all $k \geqslant 1$

$$b_h = 0 \quad \text{for} \quad N_k - n \leqslant h \leqslant N_k - 1,$$

and hence we arrive at the following result.

THEOREM 2. *Let α be an irrational p-adic integer, and let n be any positive integer. Then there exists a rational integer x_0 satisfying*

$$1 \leqslant |x_0| \leqslant p^n,$$

with the property that in the p-adic series

$$\alpha x_0 = \sum_{h=0}^{\infty} b_h p^h$$

there are infinitely many sequences of n consecutive digits b_h all equal to zero.

4. Denote by m a positive integer and by

$$g_0, g_1, \ldots, g_{m-1}$$

an arbitrary ordered sequence of m digits $0, 1, 2, \ldots, p-1$, and put

$$g = g_0 + g_1 p + \ldots + g_{m-1} p^{m-1},$$

so that evidently $$0 \leqslant g \leqslant p^m - 1.$$

In Theorem 2, choose $n \geqslant m$ and take for k any positive integer. This means that in the p-adic series

$$\alpha x_0 = \sum_{h=0}^{\infty} b_h p^h$$

all digits b_h with suffices in the interval

$$N_k - n \leqslant h \leqslant N_k - 1$$

are zero. On the other hand, by the irrationality of αx_0, infinitely many of the coefficients b_h with $h \geqslant N_k$ are distinct from zero. Assume, to fix the ideas, that N_k^* is the smallest suffix such that both

$$N_k^* \geqslant N_k \quad \text{and} \quad b_{N_k^*} \neq 0.$$

We can write αx_0 as $$\alpha x_0 = \Sigma_k^0 + \Sigma_k^1 p^{N_k^*} + \Sigma_k^2 p^{N_k^*+m},$$

where

$$\Sigma_k^0 = \sum_{h=0}^{N_k-n-1} b_h p^h, \quad \Sigma_k^1 = \sum_{h=N_k^*}^{N_k^*+m-1} b_h p^{h-N_k^*}, \quad \Sigma_k^2 = \sum_{h=N_k^*+m}^{\infty} b_h p^{h-N_k^*-m}.$$

Here Σ_k^0 is a non-negative rational integer; Σ_k^1 is by $b_{N_k^*} \neq 0$ a positive integer which is relatively prime to p; and Σ_k^2 is a p-adic integer.

Since Σ_k^1 is prime to p, there exists a rational integer x_1 such that

$$1 \leqslant x_1 \leqslant p^m - 1 \quad \text{and} \quad x_1 \Sigma_k^1 \equiv g \pmod{p^m}.$$

Put now $$X_k = x_0 x_1;$$

this integer depends on k and satisfies

$$1 \leqslant |X_k| < p^{m+n}.$$

Evidently $$\alpha X_k = x_1 \Sigma_k^0 + x_1 \Sigma_k^1 p^{N_k^*} + x_1 \Sigma_k^2 p^{N_k^*+m}.$$

Here the first term has the form

$$x_1 \Sigma_k^0 = \sum_{h=0}^{N_k-1} d_h p^h,$$

where the d_h are certain digits; this follows from the upper bound for x_1. Thus $x_1 \Sigma_k^0$ contains only terms $d_h p^h$ with suffices

$$h \leqslant N_k - 1 < N_k^*,$$

and hence it cannot affect the digits of the next product $x_1 \Sigma_k^1 p^{N_k^*}$. For similar reasons, the first m digits of $x_1 \Sigma_k^1 p^{N_k^*}$ do not depend on contributions from the third sum $x_1 \Sigma_k^2 p^{N_k^*+m}$. Therefore, by the congruence

$$x_1 \Sigma_k^1 \equiv g \pmod{p^m},$$

these first m digits are exactly $g_0, g_1, \ldots, g_{m-1}$ in this order.

The result so proved holds for every choice of the integer

$$k = 1, 2, 3, \ldots,$$

and it is clear from the irrationality of $x_0 \alpha$ that the integer N_k^* tends to infinity at the same time as k. On the other hand, the integer X_k satisfies for every k the same inequality

$$1 \leqslant |X_k| < p^{m+n}.$$

It follows then that there is an infinite sequence

$$k_1, k_2, k_3, \ldots$$

of distinct suffices k tending to infinity for which X_k retains a fixed value, X say. Hence the construction just given leads to the following result.

THEOREM 3. *Let α be an irrational p-adic integer, and let m and n be two rational integers satisfying*

$$1 \leqslant m \leqslant n.$$

Let further

$$G = \{g_0, g_1, \ldots, g_{m-1}\}$$

be an arbitrary ordered sequence of m digits. Then there exists a positive integer X depending only on α, m, and n, but not on G, such that the sequence of digits f_h in

$$\alpha X = \sum_{h=0}^{\infty} f_h p^h$$

contains infinitely often the sequence G. Moreover, $1 \leqslant |X| < p^{m+n}$.

5. The result just proved will now be applied in a special case which, in fact, leads to a generalization.

Denote by r any positive integer. There are exactly

$$p^r$$

possible distinct ordered sequences of r digits $0, 1, 2, \ldots, p-1$. By writing these p^r sequences one after the other, say in lexicographic order, we obtain a new ordered sequence

$$E = \{e_1, e_2, \ldots, e_R\}, \quad \text{where} \quad R = rp^r,$$

of digits in which every ordered sequence of r digits is contained as a part. (In fact, it is possible to find sequences E of this kind which are much shorter.)

Next put

$$m = n = R = rp^r$$

and apply Theorem 3. This gives a rational integer X satisfying

$$1 \leqslant |X| < p^{m+n} = p^{2rp^r}$$

such that the ordered sequence E occurs infinitely often among the sequence of digits c_h of

$$\alpha X = \sum_{h=0}^{\infty} c_h p^h.$$

In other words, every possible sequence of r digits occurs infinitely often among the digits of $X\alpha$.

If $X\alpha$ has this property, so has $-X\alpha$. For let c_s be the first digit of X which does not vanish. Then evidently

$$-\alpha X = (p-c_s)p^s + \sum_{h=s+1}^{\infty} (p-c_h-1)p^s,$$

also contains every possible sequence of r digits, naturally not in general in the same order as in E. Thus we arrive at the following final result.

THEOREM 4. *Let*

$$\alpha = \sum_{h=0}^{\infty} a_h p^h$$

be any irrational p-adic integer and r any positive integer. Then there exists a positive integer X less than p^{2rp^r} such that every possible sequence of r digits occurs infinitely often among the digits of αX.