MATHEMATICS Proceedings A 83 (2), June 13, 1980

# On multiplying large periodic integers. I

by J. H. B. Kemperman *

*Dept. of Mathematics, The University of Rochester, Rochester, New York 14627, U.S.A.*

Communicated at the meeting of September 29, 1979

ABSTRACT

Let $z$ be a positive integer which is obtained as the product of several large integers each with a periodic digit behavior. We investigate the periodic behavior for the leading digits of $z$ and for the least significant digits of $z$ and further study the relations between the two periodic behaviors.

## 1. Introduction

Let $g$ be a fixed integer, $g \geqslant 2$, to be used as a number base. Further $x$ will be a positive integer. It can be uniquely represented as

$$x = x_1 + x_2 g + x_3 g^2 + \ldots = (\ldots x_3 x_2 x_1)_g$$

with $x_j$ as a digit, (that is, $x_j \in \{0, 1, \ldots, g-1\}$), and $x_j = 0$ for $j$ large. Let $N = N(x)$ be such that

$$x = (x_N, x_{N-1}, \ldots, x_2, x_1)_g = \sum_{j=1}^{N} x_j g^{j-1} \text{ with } x_N \neq 0.$$

By a *period* of $x$ (to the base $g$) we shall mean an integer with $1 \leqslant T \leqslant N/2$ and such that $x_{j+T} = x_j$ whenever $1 \leqslant j < j+T \leqslant N = N(x)$. The (possibly empty) set of all such periods will be denoted as $\mathscr{T}(x)$. One easily verifies

* This research was supported in part by the National Science Foundation.

that $T_1, T_2 \in \mathscr{T}(x), T_1 < T_2$, imply $T_2 - T_1 \in \mathscr{T}(x)$. Moreover, $T_1 + T_2 \in \mathscr{T}(x)$, provided $T_1 + T_2 \leqslant N/2$.

If $\mathscr{T}(x)$ is non-empty then all the periods $T$ of $x$ are multiples of a common period $T_0$. For, let $T_0$ denote the smallest element in $\mathscr{T}(x)$. One has $hT_0 \in \mathscr{T}(x)$ $(h = 1, 2, \ldots)$ as long as $hT_0 \leqslant N/2$. Let $T$ be an arbitrary period of $x$. If it is not a multiple of $T_0$ then $hT_0 < T < (h+1)T_0$ for some positive integer $h$. Here, $hT_0 < T \leqslant N/2$ thus $hT_0 \in \mathscr{T}(x)$ hence $T' = T - hT_0$ would be a member of $\mathscr{T}(x)$ strictly smaller than $T_0$.

The integer $x$ is said to be periodic (to the base $g$) if it has at least one period $T$. Naturally, this is most interesting when $T$ is quite small relative to $N(x)$. It would follow that $\{x_1, x_2, \ldots, x_N\}$ can be extended to an infinite sequence $\{x_1', x_2', x_3', \ldots\}$ such that $x_{j+T}' = x_j'$ for all $j \geqslant 1$; $(x_j' = x_j$ for $1 \leqslant j \leqslant N)$. This extension is unique and does not depend on the particular period $T$, since it is always a multiple of the minimal period $T_0$.

We will say that $x$ is purely periodic if it possesses a period $T$ which divides $N$. Then also the minimal period $T_0$ of $x$ will be a divisor of $N = N(x)$.

REMARK. The restriction $T \leqslant N/2$ in the definition of period is essential. Let us define a quasi-period of $x$ as any integer $1 \leqslant T < N = N(x)$ such that $x_{j+T} = x_j$ whenever $1 \leqslant j < j + T \leqslant N$. We claim that different quasi-periods may lead to different periodic extensions. Moreover, a quasi-period need not be a multiple of the minimal quasi-period $T_0$, not even when $T_0 \leqslant N/2$ (in which case $x$ is periodic).

For example, $x = (1213121)_{10}$ has $N = 7$, no period, while 4 and 6 are quasi-periods leading to different periodic extensions. Similarly, for $x = (12185121)$ with $N = 8$ and quasi-periods 5 and 7. The integer $x = (112111211)_{10}$ has $N = 9$, a period $T_0 = 4$ and a quasi-period $T = 7$. Similarly, $x = (12112121121)_{10}$ with $N = 11$, $T_0 = 5$ and $T = 8$ (which lead to different periodic extensions).

## The main problem

Let $z$ be a positive integer which has been derived from a few large periodic integers $x^{(m)}$, each with a relatively small period $T_m$, by a short calculation involving the operations of addition, subtraction and multiplication. Then often the sequence of leading digits of $z$ and the sequence of least significant digits of $z$ each have an outspoken periodic behavior. In the present paper we will study this phenomenon and also certain connections between the two periodic behaviors, especially for the case that the $x^{(m)}$ are purely periodic.

As an example, choose $g = 10$, and consider the purely periodic integers

$$x = x(m) = (2121 \ldots 21)_{10} = 21(10^{2m} - 1)/99,$$
$$y = y(n) = (847847 \ldots 847)_{10} = 847(10^{3n} - 1)/999,$$

with $m$ and $n$ large. The first has $N(x) = 2m$ decimal digits and period 2.

The second has $N(y) = 3n$ and period 3. Their product would be equal to

$$z = z(m, n) = x(m)y(n) = (10^{2m} - 1)(10^{3n} - 1)\zeta$$

where

$$\zeta = (\tfrac{21}{99})(\tfrac{847}{999}) = (0.\overline{179846513})_{10}$$

has a purely repeating decimal expansion of period 9 with repeating blocks $\bar{w} = (179846513)$. Letting $k' = \min(2m, 3n) - 2$, the *first* $k'$ significant decimal digits of $z(m, n)$ will show the following periodic pattern:

$$z(m, n) = (179846513179846513179 8 \ldots)_{10}.$$

Next, let us consider the sequence of least significant digits of $z(m, n)$. Working modulo $10^k$, it is obvious that the last $k$ decimal digits of the positive integer $z(m, n)$ are independent of the particular choice of $m$ and $n$ as long as $k \leqslant \min(2m, 3n)$. It turns out that then

$$z = z(m, n) = (1798 \ldots 534868201534868201534 87)_{10}.$$

That is, except for the final digit 7, the tail of the decimal expansion of $z(m, n)$ is also periodic of period 9, this time with blocks (682015348). It is also true that the tail of the decimal expansion of $z - 1$ is purely periodic with period block (820153486). Moreover, it so happens that

$$(179846513)_{10} + (820153486)_{10} = (999999999)_{10}.$$

We will see that this example is not an exception but quite typical instead.

In the Sections 2 and 3 we develop all the necessary tools. These sections are elementary and self-contained, partly expository and parallel to the theory of $g$-adic numbers as treated in [1] and [5]. However, $g$-adic numbers are never mentioned explicitely. The reader may prefer to skim first through the illustrations and running discussion of part II (section 4).

## 2. Arithmetic modulo $g^k$

Let $M$ be a fixed positive integer, $M \geqslant 2$, (usually, $M = g^k$ with $k$ large). If two real numbers $u$ and $v$ differ by a multiple of $M$ then we write $u \equiv v \pmod{M}$. For instance, $-1 \equiv (999 \ldots 99)_{10} \pmod{10^k}$, where the latter integer has at least $k$ digits 9.

Let $R_M$ denote the (commutative) ring of integers modulo $M$. An element $x \in R_M$ is called a zero-divisor if $xy = 0$ for some $y \in R_M$ with $y \neq 0$. If $x$ corresponds to the integer $u$ this means that $(u, M) \geqslant 2$.

Let $S_M$ denote the set of all $x \in R_M$ which are not zero-divisors; (they correspond to the integers $u$ with $(u, M) = 1$). If $x, y \in S_M$ then also $xy \in S_M$.

Two pairs $(r_1, s_1)$ and $(r_2, s_2)$ in $R_M \times S_M$ will be said to be *equivalent* if $r_1 s_2 = r_2 s_1$; we will write $(r_1, s_1) \sim (r_2, s_2)$. One easily verifies that this is an equivalence relation. Let $[r/s]$ denote the equivalence class which contains the pair $(r, s) \in R_M \times S_M$. Thus $[r_1/s_1] = [r_2/s_2]$ if and only if

$r_1 s_2 = r_2 s_1$. One easily verifies that a well-defined commutative ring is obtained by defining $[r_1/s_1].[r_2/s_2] = [r_1 r_2/s_1 s_2]$ and $[r_1/s_1] + [r_2/s_2] = [r_1 s_2 + r_2 s_1/s_1 s_2]$, (with $r_i = R_M$ and $s_i \in S_M$).

If the $r_i \in R_M$ and $s_i \in S_M$ are represented by integers $u_i$ and $v_i$, respectively, then the relation $[r_1/s_1] = [r_2/s_2]$, (that is, $(r_1, s_1) \sim (r_2, s_2)$), will be expressed as

$$(2.1) \qquad u_1/v_1 \equiv u_2/v_2 \ [\mathrm{mod}\ M].$$

Let us stress that (2.1) does *not* assert that $u_1/v_1 \equiv u_2/v_2 \pmod M$ but only that $u_1 v_2 \equiv u_2 v_1 \pmod M$. For instance, $3/7 \equiv 9/1$ [mod 10]. However, if $x$ and $y$ are *integers* then the relations $x/1 \equiv y/1$ [mod $M$] and $x \equiv y \pmod M$ are identical.

Let $s \in S_M$ be fixed. Then the map $x \to xs$ of $R_M$ into itself is injective. Since $R_M$ is finite, this map is also onto. Hence, for each $r \in R_M$, there exists a unique $x \in R_M$ with $xs = r$, equivalently, $[r/s] = [x/1]$. Identifying $[x/1]$ with $x$, we see that the above ring of equivalence classes is nothing but $R_M$ itself. Our treatment (which is well-known, see [3] p. 67) shows that in $R_M$ one may freely divide by elements $s \in S_M$. Moreover, relative to multiplication, addition, subtraction by elements in $R_M$ or division by elements in $S_M$, the resulting quotients $r/s$ can be handled just as in ordinary grade school arithmetic.

## 3. The sequence of least significant digits

In the sequel, $k$ will be a fixed positive integer and $g$ a fixed base. Consider a nonnegative integer $z$ which is given in the form

$$(3.1) \qquad z = F(x^{(1)}, \ldots, x^{(M)}),$$

where $F$ denotes a polynomial with integer coefficients. Further, $x^{(m)}$ denotes a nonnegative integer such that the sequence of its last $k$ digits (to the base $g$) is a periodic sequence of period $T_m$, $(m = 1, \ldots, M)$, (where $T_m \leqslant k/2$). In other words,

$$(3.2) \qquad x^{(m)} = (\ldots \bar{w}^{(m)} \bar{w}^{(m)} \bar{w}^{(m)} \ldots \bar{w}^{(m)})_g \pmod{g^k},$$

with $\bar{w}^{(m)} = (w_1^{(m)}, \ldots, w_{T_m}^{(m)})$ as a given block of $T_m$ digits $w_j^{(m)}$, $(m = 1, \ldots, M)$. Among other things, we are interested in the problem of determining the periodic behavior of the sequence of last $k$ digits of the resulting integer $z$.

Consider a nonnegative integer $x$ having the following behavior:

$$(3.3) \qquad x \equiv (\ldots \bar{w}\, \bar{w}\, \bar{w}\, \bar{w}\, \bar{u})_g \pmod{g^k}.$$

Here,

$$\bar{w} = (w_1, w_2, \ldots, w_T) \text{ and } \bar{u} = (u_1, u_2, \ldots, u_h)$$

denote blocks of $T \geqslant 1$ digits $w_j$ and $h \geqslant 0$ digits $u_j$, respectively. If $h = 0$ then $\bar{u}$ stands for the empty block. Thus, the sequence of the $k$ least significant digits of $x$ ends as follows:

$$\dots w_{T-1}w_Tw_1w_2 \dots w_Tw_1w_2 \dots w_Tu_1u_2 \dots, u_h.$$

To the blocks $\bar{u}$ and $\bar{w}$ we will associate the integers

$$(3.4)\qquad \begin{cases} u=(u_1, u_2, \dots, u_h)_g=u_1g^{h-1}+u_2g^{h-2}+\dots+u_h; \\ w=(w_1, w_2, \dots, w_T)_g=w_1g^{T-1}+w_2g^{T-2}+\dots+w_T, \end{cases}$$

($u=0$ if $h=0$). Note that $0 \leqslant u < g^h$ and $0 \leqslant w < g^T$. Further $w$ and $\bar{w}$ determine each other if $T$ is known, similarly for $u$ and $\bar{u}$ when $h$ is known. It follows from (3.3) and (3.4) that

$$x \equiv u+w(1+g^T+g^{2T}+\dots+g^{(j-1)T})g^h \pmod{g^k},$$

provided the positive integer $j$ satisfies $jT+h \geqslant k$. Hence,

$$(g^T-1)x \equiv (g^T-1)u+w(g^{jT}-1)g^h \equiv (g^T-1)u-wg^h \pmod{g^k}.$$

Consequently, using the notations of Section 2 with $M=g^k$, we have the central relation

$$(3.5)\qquad x \equiv \xi \ [\mathrm{mod}\ g^k], \text{ where } \xi=u-wg^h/(g^T-1).$$

Conversely, (3.5) with $u$ and $w$ of the form (3.4) (where $u_j, w_j \in \{0, 1, \dots, g-1\}$) implies for $x$ the regular behavior (3.3).

Consider the special case $h=0$. Then

$$x \equiv (\dots \bar{w}\,\bar{w}\,\bar{w}\,\bar{w})_g \pmod{g^k},$$

that is, the last $k$ digits of $x$ form a periodic sequence of period $T$ (provided $k \geqslant 2T$). And in this case (3.5) simplifies to

$$(3.6)\qquad x \equiv -w/(g^T-1) \ [\mathrm{mod}\ g^k].$$

In particular, for $m=1, \dots, M$, (3.2) is equivalent to

$$(3.7)\qquad x^{(m)} \equiv \xi^{(m)} \ [\mathrm{mod}\ g^k], \text{ where } \xi^{(m)}=-w_m/(g^{T_m}-1),$$

with

$$w_m=(w_1^{(m)}, w_2^{(m)}, \dots, w_{T_m}^{(m)})_g, \text{ thus, } w_m \in \{0, 1, \dots, g^{T_m-1}\}.$$

It follows from (3.1), (3.7) and the remarks in Section 2 that the given nonnegative integer $z$ satisfies

$$(3.8)\qquad z \equiv \zeta \ [\mathrm{mod}\ g^k],$$

where $\zeta$ is the rational number defined by

$$(3.9)\qquad \zeta=F(\xi^{(1)}, \xi^{(2)}, \dots, \xi^{(M)}).$$

It is an easy matter to compute the number $\zeta$. It remains to determine the resulting behavior of the sequence of the $k$ least significant digits of $z$.

Observe that $\zeta$ can be written as

$$(3.10)\qquad \zeta=r/s \quad \text{with } s \geqslant 1,\ (g, s)=1,$$

($r$ and $s$ integers; we do not require that $(r, s)=1$). Every prime factor of $s$ must be a prime factor of $g^{T_m}-1$, for some $m \in \{1, 2, \ldots, M\}$. Moreover, the rational number $\zeta$ is independent of $k$.

The theory of $g$-adic numbers (see [5] pp. 14–17) implies that any rational number $\zeta$ of the type (3.10) can be brought into the form

(3.11) $\quad \zeta = u - wg^h/(g^T - 1)$.

Here, $T \geq 1$, $h \geq 0$, $u$ and $w$ are integers (independent of $k$), while

(3.12) $\quad u \in \{0, 1, \ldots, g^h - 1\}$; $w \in \{0, 1, \ldots, g^T - 1\}$.

In view of the criterion (3.5), it follows that (3.8) is equivalent to

(3.13) $\quad z \equiv (\ldots \bar{w}\,\bar{w}\,\bar{w}\,\bar{w}\,\bar{u})_g \pmod{g^k}$,

with $\bar{w}$ as the block of digits associated to $w$ and $T$, $\bar{u}$ as the block of digits associated to $u$ and $h$. That is,

$$\bar{w} = (w_1, w_2, \ldots, w_T); \quad \bar{u} = (u_1, u_2, \ldots, u_h),$$

with the $u_j$ and $w_j$ as digits such that (3.4) holds. This reduces the problem to a calculation of the decomposition (3.11), (3.12).

ILLUSTRATION. As an example, consider the illustration used in Section 1. That is, take $g=10$ and $z$ as the product $z=xy$ of the periodic positive integers $x=(2121 \ldots 21)_{10}$ and $y=(847847 \ldots 847)_{10}$ having $2m \geq k$ and $3n \geq k$ decimal digits, respectively. Thus, $z$ is of the form (3.1) with $M=2$; $F(x, y)=xy$; $T_1=2$, $\bar{w}^{(1)}=(2, 1)$, thus, $\xi^{(1)}=-21/99$; further, $T_2=3$, $\bar{w}^{(2)}=(8, 4, 7)$, thus, $\xi^{(2)}=-847/999$.

Consequently, $z=xy$ satisfies (3.8) with $\zeta=(\frac{21}{99})(\frac{847}{999})$. Moreover,

$$\zeta = 7 - 10(.\overline{682015348})_{10} = 7 - 10w/(10^9 - 1),$$

where $w$ is the 9-digit integer $w=(682015348)_{10}$. Therefore, (3.11) holds with $T=9$, $h=1$ and $u=7$. This in turn is equivalent to

$$z \equiv (\ldots \bar{w}\,\bar{w}\,\bar{w}\,\bar{w}\,7)_{10} \pmod{10^k},$$

with $\bar{w}$ as the 9-digit block $\bar{w}=(682015348)$.

Let us turn to the problem of determining the decomposition (3.11), (3.12). The treatment below includes a proof that this decomposition is always possible and has many interesting byproducts.

We start with a rational number $\zeta$ of the canonical form (3.10), (possibly calculated from (3.7) and (3.9)). Further $z$ will denote a nonnegative integer satisfying (3.8).

If $s=1$ then everything is trivial. For, then $\zeta$ itself is an integer and (3.8) simply says that $z \equiv \zeta \pmod{g^k}$. If $\zeta \geq 0$ then (3.11) holds with $u=\zeta$; $w=0$; $T \geq 1$ arbitrary and $h \geq 0$ so large that $\zeta < g^h$. If $\zeta < 0$ then (3.11) holds with $h \geq 0$ such that $|\zeta| \leq g^h$; $u=g^h+\zeta$; $w=g^T-1$ and $T \geq 1$ arbitrary.

For convenience, we will assume $s \geqslant 2$ from now on. By $T$ we shall denote the smallest integer $T \geqslant 1$ with $g^T \equiv 1 \pmod{s}$. One has $1 \leqslant T \leqslant \phi(s) \leqslant s-1$, with $\phi$ as the Euler $\phi$-function.

It suffices to construct a representation of the form

$$(3.14) \quad \zeta = r/s = u - g^h(R/s),$$

where $h$ is a nonnegative integer, while $u$ and $R$ satisfy

$$(3.15) \quad u \in \{0, 1, \ldots, g^h - 1\}; \; R \in \{0, 1, \ldots, s\};$$

($u = 0$ when $h = 0$).

For, suppose one has a decomposition as in (3.14), (3.15). Let $\lambda$ be the positive integer such that $g^T - 1 = \lambda s$. Then

$$R/s = w/(g^T - 1) \text{ with } w = \lambda s.$$

Since $0 \leqslant R/s \leqslant 1$, one has that $w \in \{0, 1, \ldots, g^T - 1\}$. Consequently, (3.14), (3.15) imply that $\zeta$ has the required representation (3.11), (3.12). And the latter implies in turn the important property (3.13) for $z$.

REMARK. Let $\bar{w} = (w_1, \ldots, w_T)$ denote the block associated to $w$ and $T$, (see (3.4)). Then one has the expansion

$$(3.16) \quad R/s = w/(g^T - 1) = (.\bar{w}\,\bar{w}\,\bar{w} \ldots)_g = g^{-h}(u - \zeta);$$

(here, the period $T$ is minimal when $(R, s) = 1$, see [2] p. 111). Comparing (3.13) and (3.16), it is obvious that the sequence of the last $k$ digits of $z$ is closely related to the usual expansion to the base $g$ of the rational number $\zeta$ associated to $z$. For a special case this was also observed by Knuth [4] p. 180, 497.

It remains to show that $\zeta$ has a representation (3.14), (3.15). Particularly simple is the case that

$$(3.17) \quad -1 \leqslant \zeta \leqslant 0, \text{ that is, } -s \leqslant r \leqslant 0.$$

For, then (3.14), (3.15) hold with $h = 0$, $u = 0$ and $R = -r$. Moreover (3.13) and (3.16) imply

$$(3.18) \quad z \equiv (\ldots \bar{w}\,\bar{w}\,\bar{w}\,\bar{w})_g \pmod{g^k},$$

where $\bar{w}$ is the *same* block (of length $T$) as in the expansion

$$(3.19) \quad -\zeta = -r/s = (.\bar{w}\,\bar{w}\,\bar{w}\,\bar{w} \ldots)_g.$$

Next, we like to reduce the general case to the special case (3.17). For this purpose, let us introduce integers $v_j$ and $R_j$ such that

$$(3.20) \quad r/s = v_j - g^j(R_j/s) \text{ and } v_j \in \{0, 1, \ldots, g^j - 1\},$$

($j = 0, 1, 2, \ldots$). In particular,

$$(3.21) \quad v_j s \equiv r \pmod{g^j} \text{ and } v_j \in \{0, 1, \ldots, g^j - 1\}.$$

Since (3.21) has precisely one solution $v_j$ and $R_j$ is determined by $R_j=(v_js-r)/g^j$, we see that, for each $j\geqslant 0$, there is a unique such pair $v_j$, $R_j$. For instance, $v_0=0$ and $R_0=-r$.

One is ready if there exists an index $j$ with $0\leqslant R_j\leqslant s$. For, then (3.20) implies that (3.14) and (3.15) hold with $h=j$, $u=v_j$ and $R=R_j$. Moreover, from the remarks following (3.15), $0\leqslant R_j\leqslant s$ would imply that

$$(3.22)\qquad z\equiv(\ldots\bar{w}^{(j)}\bar{w}^{(j)}\bar{w}^{(j)}\bar{v}^{(j)})_g \pmod{g^k},$$

with $\bar{w}^{(j)}$ as the block of $T$ digits associated to the integer $w^{(j)}\in\{0,1,\ldots,g^T-1\}$ defined by

$$(3.23)\qquad R_j/s=w^{(j)}/(g^T-1)=(.\bar{w}^{(j)}\bar{w}^{(j)}\bar{w}^{(j)}\ldots)_g.$$

Further $\bar{v}^{(j)}$ denotes the block of $j$ digits corresponding to $v_j\in\{0,1,\ldots,g^j-1\}$.

It will be convenient to introduce a fixed integer $f$ such that

$$fg\equiv 1 \pmod{s}.$$

Let $a_j$ denote the integer defined by $(fg)^j=1+a_js$. Then $r/s=-a_jr+g^j(f^jr/s)$, showing that the first condition (3.20) holds with $v_j=-a_jr+b_jg^j$ and $R_j=-f^jr+b_js$, whatever the value $b_j$. By an appropriate choice of the integer $b_j$, one can also satisfy the second condition (3.20). In fact, one has the explicit formulae

$$(3.24)\qquad v_j=\{-a_jr/g^j\}g^j=\{(r/sg^j)(1-(fg)^j)\}g^j=\{(-\zeta)(f^j-g^{-j})\}g^j,$$

with $\{y\}=y-[y]$ as the non-integral part of $y$. Similarly,

$$b_j=-[-a_jrg^{-j}]=-[(-\zeta)(f^j-g^{-j})]$$

and

$$(3.25)\qquad R_j/s=(-\zeta)f^j-[(-\zeta)f^j+\varepsilon_j],\ \text{where } \varepsilon_j=\zeta g^{-j}.$$

It is easily seen that, for $t$ as an integer, $0\leqslant t/s-[t/s+\varepsilon]\leqslant 1$ as soon as $-1/s\leqslant\varepsilon<1/s$. Choosing $t=-rf^j$, we see from (3.25) that $0\leqslant R_j\leqslant s$ holds as soon as $-1/s\leqslant(r/s)g^{-j}<1/s$ which is true for $g^j>|r|$.

This completes the proof of the existence of a representation (3.14), (3.15). In the sequel, $h$ will be defined by

$$(3.26)\qquad h=h_{\min}=\min\{j:j\geqslant 0,\ 0\leqslant R_j\leqslant s\}.$$

We have shown that $h$ is finite (and our estimates show that $h\leqslant 1+[\log_g|r|]$). Moreover, (3.14), (3.15) holds with $u=v_h$ and $R=R_h$, while (3.22), (3.23) hold with $j=h$.

ALGORITHM. For actual calculations (of $h$, $u=v_h$ and $R_h$), the following recursive scheme is to be preferred above (3.24), (3.25).

From the definition (3.21) of $v_j$ there exist unique digits

$$(3.27)\qquad z_i\in\{0,1,\ldots,g-1\},\quad (i=1,2,\ldots),$$

such that

(3.28) $v_j = z_1 + z_2 g + \ldots + z_j g^{j-1}$ for all $j \geqslant 0$,

$(v_0 = 0)$. Moreover, from (3.20) applied to two consecutive values $j$,

(3.29) $(gR_{j+1} - R_j)/s = (v_{j+1} - v_j)/s, \quad (j > 0)$,

therefore, (3.28) implies that

(3.30) $R_{j+1} = (R_j + z_{j+1}s)/g, \quad (j > 0)$.

Recall that $R_0 = -r$. Given $R_j$, the digit $z_{j+1} \in \{0, 1, \ldots, g-1\}$ is *uniquely determined* by the requirement that $R_j + z_{j+1}s$ be divisible by $g$. Afterwards, one calculates $R_{j+1}$ from (3.30), then $z_{j+2}$ and so on.

If both $R_j$ and $s$ are expressed to the base $g$, then in calculating $z_{j+1}$ one only needs to pay attention to the very last digits $\varrho_j$ and $\sigma$ of $R_j$ and $s$, and further to the sign of $R_j$. Let $e$ be the unique digit such that $e\sigma \equiv -1 \pmod{g}$, that is $es \equiv -1 \pmod{g}$. Then $z_{j+1} \equiv eR_j \pmod{g}$. If $R_j > 0$ this is the same as $z_{j+1} \equiv e\varrho_j \pmod{g}$.

As a concrete example, if $g = 10$ and $\zeta = -87/13$ then we get the following calculation, (where $\sigma = 3$ and $e = 3$).

| | | | |
|---|---|---|---|
| 87 | $R_0 = 87$ | $\varrho_0 = 7$ | $z_1 = 1$ |
| 13 | | | |
| 10 | $R_1 = 10$ | $\varrho_1 = 0$ | $z_2 = 0$ |
| 00 | | | |
| 1 | $R_2 = 1$ | $\varrho_2 = 1$ | $z_3 = 3$ |
| 39 | | | |
| 4 | $R_3 = 4$ | $\varrho_3 = 4$ | $z_4 = 2$ |
| 26 | | | |
| 3 | $R_4 = 3$ | $\varrho_4 = 3$ | $z_5 = 9$ |
| 117 | | | |
| 12 | $R_5 = 12$ | $\varrho_5 = 2$ | $z_6 = 6$ |
| 78 | | | |
| 9 | $R_6 = 9$ | $\varrho_6 = 9$ | $z_7 = 7$ |
| 91 | | | |
| 10 | $R_7 = 10$ | $\varrho_7 = 0$ | $z_8 = 0$ |

Already after one step it is true that $0 < R_j < 13$. The first digit is $z_1 = 1$. From there on, the digits recur in blocks $(\underline{032967})$ of length 6. This is naturally related to the fact that $R_1/s = 10/13 = (.\overline{769230})_{10}$, see (3.38).

COMMENTS. Observe from (3.30) and $0 \leqslant z_{j+1} \leqslant g-1$ that

(3.31) $0 \leqslant R_j \leqslant s$ implies $0 \leqslant R_{j+1} \leqslant s$.

Hence, from (3.26),

(3.32) $0 \leq R_j \leq s$ for all $j \geq h$, while $R_j \notin [0, s]$ for all $j < h$.

Further note, from (3.28) and (3.30), that

(3.33) $\zeta = r/s = z_1 + z_2 g + \ldots + z_j g^{j-1} - g^j(R_j/s)$.

From (3.30), if one $R_j$ is divisible by $s$ then all are. Since $\zeta = r/s = -R_0/s$, this happens precisely when $\zeta$ is an integer. In that case, one must have for all $j \geq h$ that either $R_j = 0$ or $R_j = s$. It is clear from (3.33) that, for $\zeta$ as a nonnegative integer, one must have $R_j = 0$ and $z_{j+1} = 0$ for all $j \geq h$. Similarly, if $\zeta$ is a negative integer then $R_j = s$ and $z_{j+1} = g - 1$ for all $j \geq h$, (where $h$ depends on $\zeta$).

On the other hand, if $\zeta$ is not an integer then $R_j = 0$ and $R_j = s$ are impossible, showing that $0 < R_j < s$ for all $j \geq h$. Further, from (3.20) and (3.22), $g^j R_j \equiv -r \pmod{s}$, thus, $R_j \equiv -f^j r \pmod{s}$. Since $g^T \equiv 1 \pmod{s}$ one has $f^T \equiv 1 \pmod{s}$, hence, $R_{j+T} \equiv R_j \pmod{s}$. Consequently, (even if $\zeta$ is an integer), one has

(3.34) $R_{j+T} = R_j$ and thus $z_{j+T+1} = z_{j+1}$ for all $j \geq h$.

On the other hand, $z_{h+T} \neq z_h$ (if $h \geq 1$). This follows for instance from (3.30) applied for $j = h-1$ and $j = h+T-1$, where $R_h = R_{h+T}$ but $R_{h-1} \neq R_{h+T-1}$, (since the second belongs to $[0, s]$ and the first does not).

The fraction $-R_j/s$ in (3.33) is equivalent [mod $g^k$] to an integer (see Section 2). Hence, it follows from (3.8) and (3.38) that

(3.35) $z \equiv z_1 + z_2 g + \ldots + z_j g^{j-1} \pmod{g^j}$ whenever $0 < j \leq k$.

One may conclude from (3.35) that the digits $z_1, z_2, \ldots, z_k$ which we computed from the algorithm (3.30) (with $R_{j+1}$ an integer) are precisely the $k$ least significant digits in the representation of the integer $z$ to the base $g$. This justifies the notation $z_i$ for the digits in (3.28).

Another way of proving (3.35) is to note, using (3.32), that (3.22) is valid for all $j \geq h$. Here,

(3.36) $\bar{v}^{(j)} = (z_j, z_{j-1}, \ldots, z_1)$

is the block of the $j$ digits of the integer $v_j$ (with $0 \leq v_j < g^j$; see (3.28)). Afterwards, comparing (3.22) and (3.35), it also follows that the block $\bar{w}^{(j)}$ in (3.22), (3.23) must be of the form

(3.37) $\bar{w}^{(j)} = (z_{j+T}, z_{j+T-1}, \ldots, z_{j+1})$.

And (3.23) becomes

$$(3.38) \quad \begin{cases} R_j/s = (.\bar{w}^{(j)}\bar{w}^{(j)}\bar{w}^{(j)} \ldots)_g = (.\overline{z_{j+T}z_{j+T-1} \ldots z_{j+1}})_g = \\ = (.z_{j+T}z_{j+T-1} \ldots z_{j+1}z_{j+T}z_{j+T-1}z_{j+1}z_{j+T} \ldots)_g, \end{cases}$$

provided $j \geq h$.

Thus, starting from $R_j/s$ with $j \geqslant h$, the usual long division algorithm yields in succession the digits $z_{j+T}, z_{j+T-1}, \ldots, z_{j+1}, z_{j+T}, z_{j+T-1}, \ldots$. In particular,

$$gr_i = z_{j+T-1}s + r_{i+1}; \quad 0 < r_{i+1} < s, \text{ for } i = 0, 1, \ldots, T-1,$$

where $r_0 = R_j$; (naturally, $r_i = R_{j+T-i}$ for $i \leqslant T$).

Instead, the algorithm (3.30) starting from $R_j$ (with $j \geqslant h$) yields in succession the digits $z_{j+1}, z_{j+2}, \ldots, z_{j+T}, z_{j+T+1} = z_{j+1}, z_{j+2}, \ldots$, thus, the same digits but in opposite order.

*(To be continued)*