A Right-to-Left Division Algorithm

N.H. Guersenzvaig and G.S. Krimker

Introduction.

In her remarkable paper, published in the April 2003 issue of Crux (see [1, pp. 170–173]), H. Havens (who was a young high school student when she wrote the paper) gives a criterion for divisibility by numbers ending in 9. She also shows that a similar algorithm works for numbers ending in 3 and asked if there are other similar criteria that work in bases different from 10.

Reviewing the existing literature we found that Havens rediscovered part of a general criterion established by N.N. Vorobiov in [2, §4, Th. 24, p. 47] (it appears there is no English version available), and later on, although independently, by J. Whittaker in [3]. We will prove this fact describing precisely Vorobiov's algorithm. Furthermore, we will establish a dual result to that of Vorobiov which can be presented as a division algorithm that proceeds from right to left. In order to appropriately state these facts, we need some terminology.

Let F be a given function of $\mathbb{N}_0$ to $\mathbb{N}_0$, where $\mathbb{N}_0 = \{0, 1, 2, \ldots, \}$. As usual, the composite function $F^m : \mathbb{N}_0 \to \mathbb{N}_0$ is recursively defined by $F^0(n) = n$ and $F^k(n) = F(F^{k-1}(n))$ for $k \geq 1$. Let d be any integer greater than 1. Partly following Vorobiov, we will say (cf. [2, §3, pp. 29–43]) that F is an *algorithm for divisibility by* d if the following three conditions are satisfied:

(A) $F(n)$ is completely determined by n for each $n \in \mathbb{N}_0$.

(B) For each integer $n \geq d$, there exists $k \in \mathbb{N}_0$ such that $F^k(n) < d$.

(C) For each $n \in \mathbb{N}_0$, we have $d \mid n$ if and only if $d \mid F(n)$.

Vorobiov's Algorithm.

For convenience, we will consider an arbitrary base $b \geq 2$. For each positive integer n, we denote by n_0 the rightmost digit of the representation of n in base b. Let us also suppose that d and b are relatively prime (that is, that d_0 and b are relatively prime). [This is equivalent to the existence of integers s and t such that $tb + sd = 1$.] Let t_0 be the least positive solution of the congruence $bx \equiv 1 \pmod{d}$ and let $r_d(n)$ be the remainder on division of n by d. Let $n = (n_k \ldots n_1 n_0)_{(b)} = n_k b^k + \cdots + n_1 b + n_0$ in base b. The algorithm of Vorobiov is based on the following fact:

We have $(n_k \ldots n_2 n_1)_{(b)} b + n_0 = \lfloor n/d \rfloor d + r_d(n)$ from the division algorithm. Hence,

$$(n_k \ldots n_2 n_1)_{(b)} + t_0 n_0 \equiv t_0 r_d(n) \pmod{d}.$$

The left side of this congruence constitutes the recursive part of the algorithm F_V defined by

$$F_V(n) = \begin{cases} \frac{n-n_0}{b} + t_0 n_0 & \text{if } n > (b-1)d, \\ r_d(n) & \text{otherwise.} \end{cases}$$

Now suppose $b = 10$ (which is the case considered by Vorobiov). From [1], we can define Havens' algorithms for cases $d_0 = 9$ and $d_0 = 3$ by

$$F_H(n) = \begin{cases} \frac{n-n_0}{10} + y(d_0) n_0 & \text{if } n \geq d, \\ n & \text{otherwise,} \end{cases}$$

where

$$y(d_0) = \begin{cases} (d+1)/10 & \text{if } d_0 = 9, \\ (3d+1)/10 & \text{if } d_0 = 3. \end{cases}$$

Then note that $F_H(n) = F_V(n)$ for $n > 9d$, because

$$t_0 = \begin{cases} y(d_0) & \text{if } d_0 \in \{3, 9\}, \\ (9d+1)/10 & \text{if } d_0 = 1, \\ (7d+1)/10 & \text{if } d_0 = 7. \end{cases}$$

The Dual to Vorobiov's Algorithm.

Let s_0 be the smallest positive solution of the congruence $dx \equiv 1 \pmod{b}$ and let $w_b(n)$ be the number of meaningful digits of the representation of n in base b (that is, $w_b(n) = \lfloor \log_b(n) \rfloor + 1$). Our algorithm is based on the following observation:

Writing $\lfloor n/d \rfloor$ in base b, say $\lfloor n/d \rfloor = (a_t \ldots a_2 a_1 a_0)_{(b)}$ with $a_t \neq 0$, we obtain $n - r_d(n) = (a_t \ldots a_2 a_1)_{(b)} bd + a_0 d$ from the division algorithm. Hence,

$$a_0 \equiv s_0(n - r_d(n)) \pmod{b} .$$

Let us now note that, if $d \mid n$, we have

$$\frac{n}{d} = (a_t \ldots a_1 a_0)_{(b)}, \quad a_0 = (s_0 n_0)_0, \quad \text{and} \quad \frac{n - a_0 d}{b} = (a_t \ldots a_2 a_1)_{(b)} d,$$

which tells us that in this case the representation of n/d in base b may be obtained in exactly $w_b(n/d) - 1 = \lfloor \log_b(n/d) \rfloor$ steps.

Consequently, we define $F : \mathbb{N}_0 \to \mathbb{N}_0$ by

$$F(n) = \begin{cases} \frac{n - (s_0 n_0)_0 d}{b} & \text{if } n > (b-1)d, \\ r_d(n) & \text{otherwise.} \end{cases}$$

In order to prove that F is an algorithm for divisibility by d, we will show first that F is well-defined; that is, that $F(n) \in \mathbb{N}_0$ for each $n \in \mathbb{N}_0$. From

the definition of F, it will be enough to prove that $F(n) \in \mathbb{N}$ if $n > (b-1)d$. Indeed, in such a case we have

$$\begin{aligned} 0 &\leq (b-1)d - (s_0 n_0)_0 d < bF(n) = n - (s_0 n_0)_0 d \\ &\equiv n_0 - n_0 s_0 d_0 \equiv 0 \pmod{b}. \end{aligned}$$

Condition (A) clearly follows from the definition of F. On the other hand, condition (B) holds because $F(n) < n$ for $n \geq d$, while condition (C) is satisfied because b and d are relatively prime.

As an example, we have $s_0 = 1$ if and only if $d_0 = 1$. Furthermore, it is easy to check that when $b = 10$ we have

$$s_0 = \begin{cases} d_0 & \text{if } d_0 \in \{1, 9\}, \\ 10 - d_0 & \text{if } d_0 \in \{3, 7\}. \end{cases}$$

Next we establish the connection between F and F_V. To this end we first prove that

$$1 + bd = s_0 d + t_0 b.$$

From $ds_0 \equiv 1 \pmod{b}$, we have $1 = s_0 d - kb$ for some positive integer k. Hence $k < d$, because otherwise we get the contradiction $s_0 d = 1 + kb > db$. Letting $k' = d - k$, we have $0 < d - k' < d$ and $1 + bd = s_0 d + k' b$; whence, k' is the smallest positive solution of $bx \equiv 1 \pmod{d}$; that is, $k' = t_0$.

Now we can prove that $F(n) \leq F_V(n)$ for $n > (b-1)d$, where equality holds if and only if $n_0 = 0$. More precisely, for such $n \in \mathbb{N}$, we have

$$\begin{aligned} F(n) &= \frac{n - n_0}{b} + \frac{n_0 - (s_0 n_0)_0 d}{b} = F_V(n) + \frac{-t_0 n_0 b + n_0 - (s_0 n_0)_0 d}{b} \\ &= F_V(n) + \frac{-n_0(1 + (b - s_0)d) + n_0 - (s_0 n_0)_0 d}{b} \\ &= F_V(n) + \frac{(-n_0 b + s_0 n_0 - (s_0 n_0)_0) d}{b} \\ &= F_V(n) + \left\lfloor -\frac{(b - s_0) n_0}{b} \right\rfloor d. \end{aligned}$$

The following theorem establishes the main properties of F.

Theorem 1. Let b and d be arbitrary relatively prime integers greater than 1. Let n be any integer, $n \geq d$, and let $m = \min\{k \in \mathbb{N}_0 : F^k(n) \leq (b-1)d\}$. For $k = 0, 1, \ldots, m$, we define

$$q_k = \begin{cases} (s_0 (F^k(n))_0)_0 & \text{if } 0 \leq k < m, \\ \lfloor F^m(n)/d \rfloor & \text{if } k = m. \end{cases}$$

(a) i) The numbers $q = (q_m \ldots q_1 q_0)_{(b)} = q_m b^m + \cdots + q_1 b + q_0$ and $r = F^{m+1}(n)$ are the unique integers that satisfy

$$n = qd + rb^m \quad \text{and} \quad 0 \leq r < d. \tag{1}$$

ii) $d \mid n \iff r = 0 \iff q = \frac{n}{d}$.

iii) If d is a prime number, then

$$r \equiv \pm r_d(n) \pmod{d} \iff b^m \equiv \pm 1 \pmod{d} .$$

(b) i) $w_b(n) - w_b(d) - 1 \le w_b(\lfloor n/d \rfloor) - 1 \le m$
$\le w_b(\lfloor n/d \rfloor) \le w_b(n) - w_b(d) + 1.$

ii) $m = w_b(\lfloor n/d \rfloor) - 1$ if and only if $F^k(n)/b^{m-k} \ge d$ for some $k \in \{0, \ldots, m\}$.

iii) Suppose $b > 2$. Then

$$m = w_b(\lfloor n/d \rfloor) - 1 \iff F^m(n) \ge d \text{ or } a \ne b-1 ,$$

where a denotes the left-most non-zero digit of the representation of $\lfloor n/d \rfloor$ in base b.

iv) $w_b(\lfloor n/d \rfloor) = w_b(n) - w_b(d) + 1$ if and only if we have either $m = w_b(n) - w_b(d) + 1$ or both $m = w_b(n) - w_b(d)$ and $F^k(n)/b^{m-k} \ge d$ for some $k \in \{0, 1, \ldots, m\}$.

Proof: (a) i) In case $m = 0$, we have $n \le (b-1)d$. Thus, $q = q_0 = \lfloor n/d \rfloor$ and $r = F(n) = r_d(n)$; whence, $n = qd + rb^0$. Next suppose $m \ge 1$. It follows easily by induction that

$$n = (q_{k-1}b^{k-1} + \cdots + q_0)d + F^k(n)b^k , \quad k = 1, \ldots, m. \tag{2}$$

Therefore, (1) holds because

$$\begin{aligned} r = F(F^m(n)) &= r_d(F^m(n)) = F^m(n) - q_m d \\ &= \frac{n - (q_m b^m + \cdots + q_0)d}{b^m} . \end{aligned}$$

In order to prove the uniqueness of q and r, we suppose that (1) is satisfied by integers q' and r' as well as. Because d and b are relatively prime and $(q - q')d = (r' - r)b^m$, it follows that $d \mid (r' - r)$. Hence, $r' = r$ (because $|r' - r| < d$) and $q = q'$.

ii) This follows at once from (1), because b and d are relatively prime.

iii) From (1), we get $r = r_d(t_0^m n)$, where t_0 denotes the smallest positive solution of $bx \equiv 1 \pmod{d}$. Then it is easy to see that our assertion is a particular case of the following result:

$$r \equiv \pm r_d(n) \pmod{d} \iff r(b^m \mp 1) \equiv 0 \pmod{d} .$$

(b) i) The extreme inequalities are well-known and follow at once from

$$b^{w_b(n)-w_b(d)-1} = \frac{b^{w_b(n)-1}}{b^{w_b(d)}} < \frac{n}{d} < \frac{b^{w_b(n)}}{b^{w_b(d)-1}} = b^{w_b(n)-w_b(d)+1} .$$

On the other hand, the central inequalities are immediate consequences of

$$(b-1)b^{m-1} \;<\; \left(\frac{F^{m-1}(n)}{d}\right) b^{m-1} \;\leq\; \frac{n}{d} \;<\; (q_m \ldots q_0)_{(b)} + b^m \,. \qquad (3)$$

ii) ($\Rightarrow$) This is clear, since $w_b(\lfloor n/d \rfloor) = m+1$ implies that $n/d \geq b^m$.

($\Leftarrow$) Suppose $k \in \{0, 1, \ldots, m\}$ and $F^k(n)/b^{m-k} \geq d$. Hence, from (2), we get $n/d = (q_{k-1} \ldots q_1 q_0)_{(b)} + b^k F^k(n)/d \geq b^m$. Thus, $w_b(\lfloor n/d \rfloor) - 1 \geq m$. Then, from i), we have $w_b(\lfloor n/d \rfloor) - 1 = m$.

iii) ($\Rightarrow$) Suppose $w_b(\lfloor n/d \rfloor) = m+1$ and $F^m(n) < d$. Then $a \neq b-1$, because otherwise, from $a > 1$ and (3), we have the contradiction

$$\lfloor n/d \rfloor \;<\; (q_{m-1} \ldots q_1 q_0)_{(b)} + b^m \,.$$

($\Leftarrow$) Case $F^m(n) \geq d$ follows directly from ii). Then, in case $a \neq b-1$, we have $w_b(\lfloor n/d \rfloor) - 1 = m$, because otherwise from $a < b-1$ and (3), we obtain the contradiction

$$\lfloor n/d \rfloor \;>\; (b-1)b^{m-1} \,.$$

iv) ($\Leftarrow$) This follows directly from i) and ii).

($\Rightarrow$) Suppose that $w_b(\lfloor n/d \rfloor) = w_b(n) - w_b(d) + 1$ and that $m \neq w_b(n) - w_b(d) + 1$. Note that $m \neq w_b(n) - w_b(d) - 1$, because otherwise we have the contradiction $w_b(\lfloor n/d \rfloor) = m+2$. Thus, from i), we have $m = w_b(n) - w_b(d)$. From ii), it only remains to prove that $m = w_b(\lfloor n/d \rfloor)$. But this equality holds, because otherwise we have $m = w_b(\lfloor n/d \rfloor) - 1$; whence, we obtain the contradiction $w_b(\lfloor n/d \rfloor) = w_b(n) - w_b(d)$. ∎

Miscellaneous remarks.

(I) For each $k \in \{1, \ldots, m\}$, the numbers

$Q_k = (q_{k-1} \ldots q_1 q_0)_{(b)} = q_{k-1}b^{k-1} + \cdots + q_1 b + q_0$ and $F_k = F^k(n)$

are the unique integers which satisfy

$$n = Q_k d + F_k b^k \quad \text{and} \quad 0 \leq Q_k < b^k \,.$$

(II) Suppose $n = (n_k \ldots n_1 n_0)_{(b)}$ in base b. The following very well-known facts follow at once from (1) and the fact that d and b are relatively prime:

$$b \equiv 1 \pmod{d} \implies \left[d \mid n \iff d \mid (n_0 + n_1 + \cdots + n_k)\right]$$

$$b \equiv -1 \pmod{d} \implies \left[d \mid n \iff d \mid (n_0 - n_1 + \cdots + (-1)^k n_k)\right] .$$

(III) Let $\overline{q} = b^m - (q_{m-1} \ldots q_0)_{(b)} = (\overline{q}_{m-1} \ldots \overline{q}_0)_{(b)}$, where the base b digits $\overline{q}_k$, for $k = 0, \ldots, m-1$, are defined by

$$\overline{q}_k = \begin{cases} 0 & \text{if } (q_k \ldots q_0)_{(b)} = 0, \\ b - q_k & \text{if } q_k \neq 0 \text{ and } (q_{k-1} \ldots q_0)_{(b)} = 0, \\ b - 1 - q_k & \text{otherwise.} \end{cases}$$

Now from (2) (with $k = m$), it follows that

$$m \;=\; w_b(\lfloor n/d \rfloor) - 1 \Longleftrightarrow F^m(n) \geq (\overline{q}/b^m)d\,.$$

(IV) Statement iv) of (b) is logically equivalent to $w_b(\lfloor n/d \rfloor) = w_b(n) - w_b(d)$ if and only if $m = w_b(n) - w_b(d) - 1$ or both $m = w_b(n) - w_b(d)$ and $F^k(n)/b^{m-k} < d$ for $k = 0, 1, \ldots, m$.

(V) In base b^k one simply replaces m by $[m/k]$, r by $\tau_d\left(rb^{\tau_k(m)}\right)$, and q by $q + \lfloor rb^{\tau_k(m)}/d \rfloor$.

(VI) Algorithm F and Theorem 1 also make sense, mutatis mutandis, for elements in an arbitrary euclidean domain (for example, for polynomials in one indeterminate with coefficients in an arbitrary field).

Finally, we give an example of each one of the four possible cases of the algorithm F.

Example 1. We consider $b = 10$, $n = 9999989$ and $d = 1001$. Thus, $s_0 = 1$. The algorithm proceeds from the right to the left as follows:

k	$F^k(n)$	q_k	$q_k d$
0	9999989	9	9009
	-9009		
1	999098	8	8008
	-8008		
2	99109	9	9009
	-9009		
3	9010	0	0
	-0		
$4 = m$	$901 = r$	$0989 = q$	

Then $9999989 = 989 \cdot 1001 + 901 \cdot 10^4$ and (since $m = w_{10}(n) - w_{10}(d) + 1$) we have $w_{10}(\lfloor n/d \rfloor) = w_{10}(n) - w_{10}(d) + 1 = 4$.

Example 2. Let $n = 101011$ and $d = 101$ in base $b = 2$. Obviously $s_0 = 1$.

k	$F^k(n)$	q_k	$q_k d$
0	101011	1	101
	-101		
1	10011	1	101
	-101		
2	0111	1	101
	-101		
$3 = m$	$001 = r$	$111 = q$	

Then $101011 = 111 \cdot 101 + 1 \cdot 10^3$ and (since $m = w_2(n) - w_2(d)$ and $n/2^m \geq d$) we have $w_2(\lfloor n/d \rfloor) = w_2(n) - w_2(d) + 1 = 4$.

Example 3. Let $n = 100111$ and $d = 101$ in base $b = 2$. Thus $s_0 = 1$.

k	$F^k(n)$	q_k	$q_k d$
0	100111	1	101
	-101		
1	10001	1	101
	-101		
2	0110	0	0
	-0		
$3 = m$	$011 = r$	$011 = q$	

Then $100111 = 011 \cdot 101 + 11 \cdot 10^3$ and $w_2(\lfloor n/d \rfloor) = w_2(n) - w_2(d) = 3$ (because $m = w_2(n) - w_2(d)$ and $F^k(n)/2^{m-k} < d$ for $k = 0, 1, 2, 3$).

Example 4. We consider $b = 10$, $n = 15354363$ and $d = 97$. Hence, $s_0 = 3$.

k	$F^k(n)$	q_k	$q_k d$
0	15354363	9	873
	-873		
1	1535349	7	679
	-679		
2	153467	1	97
	-97		
3	15337	1	97
	-97		
4	1524	2	194
	-194		
$5 = m$	$d \le 133 \le (b-1)d$	1	97
	97		
	$36 = r$	$121179 = q$	

It follows that $15354363 = 121179 \cdot 97 + 36 \cdot 10^5$, and we obtain $w_{10}(\lfloor n/d \rfloor) = w_{10}(n) - w_{10}(d) = 6$ (because $m = w_{10}(n) - w_{10}(d) - 1$).

Acknowledgement. The authors would like to express their appreciation to the referee for helpful suggestions.

References.

[1] Havens, H., Divisibility by numbers ending in nine, *Crux Mathematicorum with Mathematical Mayhem* 29 (2003), 170–173.

[2] Vorobiov, N.N., *Criterios de divisibilidad*, Mir, Moscow, 1975.

[3] Whittaker, J., A New Divisibility Criterion, *The College Math. Journal*, Vol. 16, No. 4 (1985), 268–276.

Natalio H. Guersenzvaig
Universidad CAECE
Buenos Aires
Argentina
nguersenz@fibertel.com.ar

Gustavo S. Krimker
Universidad CAECE
Buenos Aires
Argentina
guskrimker@fullzero.com.ar