2014 Hawaii University International Conferences
Science, Technology, Engineering, Math & Education
June 16, 17, & 18 2014
Ala Moana Hotel, Honolulu, Hawaii

The Array of Remainders

Mohandespour, Fereydun
Purdue University at Fort Wayne
Department of Mathematics / IPFW / LTL

THE ARRAY OF REMAINDERS

Remainders of successive division by a given divisor are organized in a particular order and placed in a matrix. The matrix thus formed will bear thought-provoking properties and useful applications in *number theory* which will be revealed in length below:

Throughout this paper, $\acute{N}$ will represent the set of natural numbers (1, 2, 3, …) and $\hat{W}$ will stand for the set of whole numbers (0, 1, 2, 3, …).

DEFINITION: Let **d** be a positive integer other than $2^u.5^v$, $k.2^{u+1}$, $k.5^{v+1}$ (u, v, k ε $\hat{W}$). Let **N** be a natural number (N < d). Let $R_1, R_2, \ldots, R_n$ be successive remainders of N/d such that $N \equiv R_1 \pmod d$, $10R_1 \equiv R_2 \pmod d$, … $10R_{n-1} \equiv R_n \pmod d$, $(0 < R_n < d)$. Then, we define "x" to be the Remainder Generating Coefficient (R.G.C) if x is the smallest positive integer to satisfy the following system of congruencies:

$$A \left\{ \begin{array}{lll} x\,N & \equiv R_1 & (\text{mod d}) \\ x\,R_1 & \equiv R_2 & (\text{mod d}) \\ x\,R_2 & \equiv R_3 & (\text{mod d}) \\ \bullet\bullet\bullet & & (\text{mod d}) \\ x\,R_{n-1} & \equiv R_n & (\text{mod d}) \end{array} \right.$$

DERIVATION OF R.G.C: Although x can be found by solving A, it is more convenient to use the formula: $x = (kd + 1) / 10$, $k \,\varepsilon\, \acute{N}, k < 10$.
Please note that k must be chosen such that $10 \mid (kd + 1)$. This can be accomplished by the following assignment:

$$B \left\{ \begin{array}{ll} k = 9 & \text{when } d = \ldots 1 \\ k = 3 & \text{when } d = \ldots 3 \\ k = 7 & \text{when } d = \ldots 7 \\ k = 1 & \text{when } d = \ldots 9 \end{array} \right.$$

The proof is omitted here for the sake of brevity.

EXAMPLE 1: Find k and x for when a) d = 7, b) d = 16 and c) d = 19
SOLUTION:

a) $d = 7 \Rightarrow k = 7$ (from table B)
$x = (kd + 1)/10 = (49 + 1)/10 = 5.$

b) d = 16 does not satisfy the definition of d.

c) $d = 19 \Rightarrow k = 1$ (from table B)
$x = (kd + 1)/10 = (19 + 1) / 10 = 2$

EXAMPLE 2: Derive the *array of remainders* for when $d = 7$

SOLUTION:
Since no beginning point is given, let us begin with $R_1 = 1$ (this is when $N = 1$). In example 1, we found $x = 5$ when $d = 7$. Thus, the successive remainders for $d = 7$ are: $R_2 \equiv 5(1) = 5$. $R_3 \equiv 5(5) \pmod 7 = 4$. $R_4 \equiv 5(4) \pmod 7 = 6$. $R_5 \equiv 5(6) \pmod 7 = 2$ & $R_6 \equiv 5(2) \pmod 7 = 3$.
Hence the entire *remainder matrix* for divisor 7 is: $\{1, 5, 4, 6, 2, 3\}$

PROPOSITION 1: If $d = 09, 19, 29, \ldots, n9$ then R.G.C $= 1, 2, 3, \ldots, n + 1$

PROOF: From the derivation of R.G.C, we have:

$k = 1$ when $d = 9, 19, 29, \ldots, n9$. Then

$$
\begin{aligned}
\text{R.G.C} &= (kd + 1) / 10 \\
&= (1d + 1) / 10 \\
&= (9 + 1, 19 + 1, 29 + 1, \ldots n9 + 1) / 10 \\
&= [10, 20, 30, 10(n + 1)] / 10 \\
\text{R.G.C} &= 1, 2, 3, \ldots, n + 1
\end{aligned}
$$

PROPOSITION 2: $x =$ R.G.C is always smaller than d ($d > 1$)

PROOF: x can be largest when $k = 9$.
In $x = (kd + 1)/10$ let $k = 9$, then
$x = (9d + 1) / 10$ or $x = 0.9d + 0.1$. Clearly, $x < d$, $\forall\, d > 1$.

PROPOSITON 3: x and d are relatively prime.
PROOF is omitted for the sake of brevity. We accept that $(x, d) = 1$

DEFINITION: We define "C", a positive integer to be the complement of R if $R + C = d$

PROPOSITION 4: The successive remainders of a given **d** are complements of one another in PAIRS either in the same column or in adjacent columns.

PROOF is omitted for the sake of brevity, however, we expound with an example:

EXAMPLE 3: Find the complement pairs when $d = 7$.

SOLUTION: In example 2, we found the remainder set $= \{1, 5, 4, 6, 2, 3\}$ when $d = 7$.

For clarity, let us divide the members into two columns:
$$
\left\{
\begin{array}{lll}
1 & 6 & \text{where } 1 + 6 = 7 \\
5 & 2 & \text{where } 5 + 2 = 7 \\
4 & 3 & \text{where } 4 + 3 = 7
\end{array}
\right.
$$

Next, we will see why R & C of d were both located in the same column.*

COROLLARY 1: Let **p** denote the number of distinct remainders generated by R.G.C of **d**. Then **p** is even if remainders and their complements are located in the same column.

PROOF: From PROPOSITION 4 we know that complements appear in pairs; and that there exits a complement for every remainder. Hence, **p** must be even.

PROPOSITION 5: If **p** is even then C_n of R_n (the complement of R in column n) is the member $p/2 + 1$ in column n, where **p** is the number of distinct remainders as defined in COROLLARY 1.

PROOF is trivial, however, it is omitted for the sake of brevity.

PROPOSITION 6: In an array of remainders, if $p = k$ ($k \varepsilon \acute{N}$) in one column, then $p = k$ in every column where **p** introduced in COROLLARY 1 is the *period* of **d**.

PROOF is omitted for the sake of brevity.

PROPOSITION 7: The period of an array of remainders generated by R.G.C is: $p = (d - 1) / n$, where n is the number of columns in the matrix and $n \mid (d - 1)$.

PROOF: By PROPOSITION 6, p is the same in every column of the matrix and there are n columns. Since there are $d - 1$ remainders then $(n)(p) = d - 1$, hence, $p = (d - 1) / n$.

COROLLARY 2: If an array of remainders consists of one column only, then the period **p** is maximum.

PROOF: In $p = (d - 1) / n$, let $n = 1$, then $p = d - 1$, a maximum value.

NOTE-1: **p** will be even since this occurs only when **d** is a prime number.
NOTE-2: The converse is not necessarily true –that is, not all primes yield max periods.

PROPOSITION 8: If $p = d - 1$, then R and C share the same column.

PROOF: By COROLLARY 2, R consists of only one column. The R values are:
1, 2, 3, …, $d - 3$, $d - 2$, and $d - 1$ and there are equal pairs. Clearly,
$1 + (d - 1) = d$
$2 + (d - 2) = d$
$3 + (d - 3) = d$
•••

* Total number of columns of an array is determined by each pattern of d. The same divisor may (or may not) generate different patters of mantissa for different dividends.

We are now prepared to proceed with the last proposition in this paper: The topic of when $p = d - 1$ became the center of research for many years. At first it appeared as if **d** posing as a prime number would generate the maximum period. Although this is a necessary condition, however not sufficient. There are exceptions such as $d = 71$ and $d = 13$.

While the true answer (for when **p** is max) was found long time ago, PROPOSITION 9 below offers an improved solution which will alleviate labor by 50%.

PROPOSITION 9: Let **p** be the period of d, d a prime number. Then **p** is maximum if: $10^{\varphi(d)/2} \equiv C_{max} \pmod{d}$ where φ is the Euler Phi function and $C_{max} = d - 1$

PROOF: First, we will use the recommend solution in Number Theory, then we will accelerate the process:

$p = d - 1$ if $10^{\varphi(d)} \equiv 1 \pmod{d}$ [1] ← current solution (1)

By PROPOSITION 8, if $p = d - 1$, then every remainder will have a complement in column 1. In particular, the complement of the first remainder is $C_{max} = d - 1$, hence, by PROPOSITION 5, we can check for the first occurrence of C_{max} located at $p/2 + 1$. Accordingly, we can substitute $\varphi(d) / 2$ for $\varphi(d)$ to generate half of the remainders only. Then we will substitute C_{max} for 1 (the occurrence of the first complement). Thus:

$P = d - 1$ if $10^{\varphi(d)/2} \equiv C_{max} \pmod{d}$ ← accelerated solution (2)

EXAMPLE 4: Verify that divisor 7 has a maximum period of 6.

SOLUTION:

$10^{\varphi(d)/2} \equiv C_{max} \pmod{d}$
$\varphi(d)/2 = (d - 1)/2 = (7 - 1)/2 = 3$
$C_{max} = d - 1 = 7 - 1 = 6.$

$\boxed{10^3 \equiv 6 \pmod{7}}$ √

In conclusion, let us consider two applications. The applications will take a careful look at PROPOSITIONS 5, 7 and 9 which are the key to a series of fundamental problems in theory of numbers.

* Please note both formulae (1) & (2) give the *necessary* condition and not the *sufficient* condition for p max. For example, consider $d = 11$ where $10^{10} \equiv 1 \pmod{11}$, but manual examination shows $p = 2$.

EXAMPLE 5: Period for d = 13 is 6. Period for d = 31 is 15. The complements of d = 13 are the same remainders in column 1 in descending order. However, the complements of d = 31 are entirely new remainders found in column 2. Why?

SOLUTION: Let us construct the matrix of remainders for each divisor:

d = 13		d = 31	
R	C	R	C
1	12	1	30
3	10	2	29
4	9	4	27
9	4	5	26
10	3	7	24
12	1	8	25
		9	22
2	11	10	21
5	8	14	17
6	7	16	15
7	6	18	13
8	5	19	12
11	2	20	11
		25	6
		28	3

Note that complements of 13 are inclusive and complements of 31 are exclusive. Although both divisors 13 and 31 are prime numbers, neither has a maximum period.

First, we use PROP. 9 to verify that the period in each case is NOT maximum:

$10^{\varphi(d)/2} \equiv C_{max} \pmod{d}$

$13 \rightarrow 10^6 \not\equiv 12 \pmod{13}$ √

$31 \rightarrow 10^{15} \not\equiv 30 \pmod{31}$ √

Second, we use PROP. 7 to verify the periods given for d = 13 & d = 31 are accurate:

$p = (d - 1) / n$

$13 \rightarrow (13 - 1) / 2 = 6$

$31 \rightarrow (31 - 1) / 2 = 15$

Last, we apply Euler φ function to PROP. 9 to obtain the half-remainder number:
$\varphi(13) / 2 = 12 / 2 = 6$, an even number $\Rightarrow 2 \mid 6$ $\Rightarrow$ two *dependent* columns for R & C
$\varphi(31) / 2 = 30 / 2 = 15$, an odd number $\Rightarrow 2 \nmid 15 \Rightarrow$ two *independent* columns for R & C

QED.

EXAMPLE 6: If **d** = 11, 101, 1001,…, $1\overbrace{0\ldots.0}^{\text{n times}}1$, then show p = 2, 4, 6, …, 2n

SOLUTION: First, we notice that **d** is a positive integer having no factors of 2 and 5, thus the properties can be applied to find **p** for every **d**.

Next, we manually find the period and remainders for one of the given divisors. The manual check is mainly for confirmation of data already provided. 11 seems to be the most convenient divisor to explore where we find 5 columns each with a period of 2:

(R, C) → (1, 10), (2, 9), (3, 8), (4, 7), (5, 6). It can be seen R + C = 11 in every column.

We use PROPOSITION 5 to confirm a period of 2 for d = 11 as follows:
$p = (d - 1) / n = (11 - 1) / 5 \Rightarrow p = 2$, where n is the # of columns.

Finally, we seek a general solution for the entire set:

By Prop. 5, if there is a complement for each remainder then p = 2 times C-count.
So now we need to calculate the number of complements for each given d.
Total number of complements can be easily determined here: they are the number of zeroes embedded in each given **d** because 11 = (10 + 1), 101 = (100 + 1), etc. Thus,

$C = \log(10^1, 10^2, 10^3, \ldots 10^n)$, then,
$P = 2(1, 2, 3, \ldots, n)$ or
$P = 2, 4, 6, \ldots, 2n$

DISCUSSION:
Calculating p for d = 11 and d = 101 is a trivial matter because by Prop. 7:

$p = (d - 1) / n$ where p is period, d is devisor and n is the # of columns in the matrix
$p = (11 - 1) / 5 \Rightarrow p = 2$ ∴when d = 11, there are 5 columns each with a period of 2
$p = (101 - 1) / 25 \Rightarrow p = 4$ ∴when d = 101, there are 25 columns each with a period of 4

It is not trivial when d = 1001 however. The above formula does NOT fit:

$6 = (1001 - 1) / n \Rightarrow n = 1000 / 6$ which is impossible. Prop. 5 states either period is maximum or there must be equal number of remainders and complements per matrix.

The logic we used in Example 6, correctly determines p = 6 when d = 1001, but the formula derived in Prop. 7 will not work in this case: why?

The short answer is because 1001 is not a prime number. The long answer is, "Wait, there is more to come on the presentation day…"

The short answer is because 1001 is not a prime number. The long answer is

EPILOGUE

The Division Algorithm (D = dQ + R) has been quite humble for its contributions to the field of mathematics at large. It has been the building block for math and science –if not directly then at least as a pedagogical tool.

One of those "esoteric" contributions is in computer science when a beginner student is asked to write a pseudo-code to emulate R (the remainder) assuming the function did not exist in any syntactical language. The student must intimately understand the division algorithm in order to accomplish this task.

Still other applications of division algorithm are found in number theory and geometric series. Number theory has long been fascinated by **d** (the divisor) while geometric series have busily explored **Q** (the quotient).

The dividend **(D)** is often taken for granted. Theory of limits would be assimilated faster if a student understood the difference between 1/0 and 0/0 while attending grade school. Thanks to calculus, the student would ultimately learn the distinction in a section devoted to "asymptotic behavior" of rational functions [2].

My mission in publishing *The Array of Remainders* has been to link the four components of the division algorithm together (as a common map): to show how new properties and applications can be developed once we fully realize the marvel of D = dQ + R.

* * *

[1] Eynden, Charles Vanden, Number Theory, An Introduction to Proof, 1970, P 216

[2] Rogawski, Jon, Calculus, Early Transcendentals, Second Edition, 2012, pp. 241-244