Parabola Volume 52, Issue 3 (2016)

Cryptarithmetics: A primer

Miklos N. Szilagyi [1]

The word "crypt-arithmetic" was first used by M. Vatriquant, under the pseudonym Minos, in the May 1931 issue of *Sphinx*, a Belgian magazine of recreational mathematics. He wrote "Cryptographers [...] put figures in places of letters. By way of reprisal, we put letters in place of figures." A cryptarithmetic puzzle is a simple mathematical operation in which letters or other symbols have replaced the digits and we are challenged to find the original numbers.

Many people believe that such puzzles were started thousands of years ago in ancient China and India but I have not seen a single proof of this.

In modern times, the first proven example appeared in the *American Agriculturist Magazine* in 1864. Later, H. E. Dudeney created the well-known puzzle

$$\begin{array}{cccccc} & & S & E & N & D \\ + & & M & O & R & E \\ \hline & M & O & N & E & Y \end{array}$$

published in the July 1924 issue of the *Strand Magazine*. In one of his books, *Puzzles and Curious Problems*, published posthumously in 1931 (he died in 1930), many more such puzzles are listed. The next substantial instance was the *Sphinx Magazine* mentioned above, where some of the puzzles proposed there are quite difficult to solve. For example, M. Pigeolet published most of his puzzles there between 1931 and 1939 (a collection of these can be found at http://cryptarithms.awardspace.us/collection.html). Virtually any book about recreational mathematics contains cryptarithmetic puzzles (Hunter 1983, Hunter and Madachy 1975, Kraitchik 1942). A number of books specifically devoted to them have also been published (Brooke 1963, Kahan 1978, van der Elsen 1998).

We assume the following elementary constraints in these puzzles:

1. No number begins with a zero.

2. Each symbol represents a digit only.

3. Two or more symbols may represent the same digit.

An elementary knowledge of number theory and modular arithmetic does not hurt. In 1955, J.A.H. Hunter introduced the word "alphametic" to designate cryptarithms whose letters form meaningful words or phrases (see for example the Dudeney puzzle given above). A. Wayne invented a special case of that in 1945, the so-called *doubly*

[1] Department of Electrical and Computering Engineering, University of Arizona

true cryptarithm. These are made up of number words that also form a valid sum, for example,

$$
\begin{array}{rccccc}
 & & & O & N & E \\
+ & & & T & W & O \\
+ & & F & I & V & E \\
\hline
 & E & I & G & H & T
\end{array}
$$

Let us try to solve the following addition (Dudley 1977–78):

$$
\begin{array}{rcccccc}
 & S & T & A & B & L & E \\
+ & & T & A & B & L & E \\
+ & & & A & B & L & E \\
\hline
 & A & T & B & E & S & T
\end{array}
$$

A straightforward approach is to represent the addition in the form of a system of algebraic equations:

$$3\mathrm{E} = \mathrm{T} + 10c_1 \,, \tag{1a}$$
$$c_1 + 3\mathrm{L} = \mathrm{S} + 10c_2 \,, \tag{1b}$$
$$c_2 + 3\mathrm{B} = \mathrm{E} + 10c_3 \,, \tag{1c}$$
$$c_3 + 3\mathrm{A} = \mathrm{B} + 10c_4 \,, \tag{1d}$$
$$c_4 + \mathrm{T} = 10c_5 \,, \tag{1e}$$
$$c_5 + \mathrm{S} = \mathrm{A} \,. \tag{1f}$$

We have 11 unknown quantities but only 6 equations. Fortunately, these are Diophantine equations; i.e., all unknown quantities are non-negative integers. In addition, the unknown letters can only represent 10 different digits (0, 1, 2, 3, 4, 5, 6, 7, 8 and 9) and the values of the remainders (c_1, c_2, c_3, c_4 and c_5) can only be 0, 1 or 2.

We start with Equation (1e). The value of c_5 can only be 0 or 1. If $c_5 = 0$, then T and c_4 must also be zero, which is impossible because TABLE cannot start with 0. Therefore, $c_5 = 1$ which leads to $c_4 = 1$, $\mathrm{T} = 9$, $\mathrm{E} = 3$, $c_1 = 0$, and $\mathrm{A} = \mathrm{S} + 1$.

Avoiding repetitions, we obtain the following table of possible values for L, S, c_2 and A from Equation (1b):

L	S	c_2	A
2	6	0	7
7	1	2	2
8	4	2	5

Equation (1d) yields $\mathrm{B} = 3\mathrm{A} + c_3 - 10$ that immediately excludes the first two rows of the table. Now, B equals with 6 or 7, respectively for $c_3 = 1$ or 2. The remaining Equation (1c) resolves this uncertainty by defining $\mathrm{B} = (10c_3 + 1)/3$. As 11 is not divisible by 3, the result is then $\mathrm{B} = (10 \times 2 + 1)/3 = 7$ and this concludes the solution. The final result is:

$$
\begin{array}{rcccccc}
 & 4 & 9 & 5 & 7 & 8 & 3 \\
+ & & 9 & 5 & 7 & 8 & 3 \\
+ & & & 5 & 7 & 8 & 3 \\
\hline
 & 5 & 9 & 7 & 3 & 4 & 9
\end{array}
$$

This solution is elementary but this is not generally the case for solving such problems; the number of addenda is not limited. To my knowledge, the world record for cryptarithms is a monster consisting of the addition of 42 numbers. Solving cryptarithmetic problems requires basic understanding of arithmetic but also ingenuity, sound logical reasoning and perseverance. Some cryptarithms – especially those created by computer programs – are quite complex and have multiple solutions. There are no specific rules or routines for the solution of such puzzles. Try to solve this one for example:

$$\begin{array}{cccccc} & & \mathrm{S} & \mathrm{E} & \mathrm{N} & \mathrm{D} \\ + & & \mathrm{M} & \mathrm{O} & \mathrm{R} & \mathrm{E} \\ + & & \mathrm{G} & \mathrm{O} & \mathrm{L} & \mathrm{D} \\ \hline & \mathrm{M} & \mathrm{O} & \mathrm{N} & \mathrm{E} & \mathrm{Y} \end{array}$$

It has 28 different solutions and you would have to spend many hours to find them all, at least without use of a computer.

In the case of *multiplications* additional information is available:

Rule 1. If $\ldots\mathrm{G} \times \mathrm{R} = \ldots\mathrm{R}$, then

- $\mathrm{R} = 2, 4$ or 8 means that $\mathrm{G} = 1$ or 6;
- $\mathrm{R} = 5$ means that $\mathrm{G} = 1, 3, 7$ or 9;
- $\mathrm{G} = 1$ might be a partial solution for any value of R (except 0 or 1).

Rule 2. Similarly, if $\ldots\mathrm{A} \times \mathrm{K} = \ldots A$, then

- $\mathrm{A} = 2, 4$ or 8 means that $\mathrm{K} = 1$ or 6;
- $\mathrm{A} = 5$ means that $\mathrm{K} = 1, 3, 7$ or 9;
- $\mathrm{A} = 0$ means that K can be anything except 0.

Rule 3. If $\ldots\mathrm{C} \times \mathrm{C} = \ldots\mathrm{H}$, then

- $\mathrm{H} = 1$ means that $\mathrm{C} = 9$;
- $\mathrm{H} = 4$ means that $\mathrm{C} = 2$ or 8;
- $\mathrm{H} = 6$ means that $\mathrm{C} = 4$;
- $\mathrm{H} = 9$ means that $\mathrm{C} = 3$ or 7.

Rule 4. If $\ldots\mathrm{B} \times \mathrm{B} = \ldots\mathrm{B}$, then B can only be $1, 5$ or 6.

Let us solve the following puzzle (Brooke 1963):

$$\begin{array}{ccccc} & & \mathrm{A} & \mathrm{B} & \mathrm{C} \\ \times & & & \mathrm{D} & \mathrm{E} \\ \hline & & \mathrm{F} & \mathrm{E} & \mathrm{C} \\ + & \mathrm{D} & \mathrm{E} & \mathrm{C} & \\ \hline & \mathrm{H} & \mathrm{G} & \mathrm{B} & \mathrm{C} \end{array}$$

Our equations are now the following,

$$\mathrm{E} + \mathrm{C} = \mathrm{B} + 10c_1\,, \tag{2a}$$

$$c_1 + \mathrm{E} + \mathrm{F} = \mathrm{G} + 10\,, \tag{2b}$$

$$1 + \mathrm{D} = \mathrm{H}\,, \tag{2c}$$

$$\mathrm{ABC} \times \mathrm{E} = \mathrm{FEC}\,, \tag{2d}$$

$$\mathrm{ABC} \times \mathrm{D} = \mathrm{DEC}\,, \tag{2e}$$

It is clear from Equations (2d) and (2e) that neither D nor E can be equal to 1. Then it follows from **Rule 2** and Equation (2c) that $\mathrm{C} = 5$, E is equal to 3, 7 or 9, and D is equal to 3 or 7. Avoiding repetitions, we obtain the following table of the possible values for D, H, E, B, c_1, F and G from Equations (2a) and (2b):

D	H	E	B	c_1
3	4	7	2	1
7	8	9	4	1

Equation (2b) immediately eliminates the second row because otherwise, $c_1 + \mathrm{E} = 10$ and so $\mathrm{F} = \mathrm{G}$. In the first row F can take the values 5, 6, 8 or 9. Equation (2b) leads to the elimination of 5, 6 and 9. Therefore, $\mathrm{F} = 8$ and $\mathrm{G} = 6$. We find $\mathrm{A} = 1$ from both Equation (2d) and Equation (2e). The solution is

$$\begin{array}{rrrrr} & & 1 & 2 & 5 \\ \times & & & 3 & 7 \\ \hline & & 8 & 7 & 5 \\ + & 3 & 7 & 5 & \\ \hline & 4 & 6 & 2 & 5 \end{array}$$

The solution of the cryptarithmetics with long divisions is usually relatively easy because of the large number of multiplications and subtractions given in the problem statement. The reader finds one such puzzle in the Problem Section of this issue.

In some cases, there are redundancies in the problem statement that can be utilised in creating *skeleton* cryptarithmetics (arithmetical restorations) in which some unknown characters are denoted by lowercase letters, periods or asterisks. They may represent any digit. The solutions of such puzzles are usually not very easy. Here is an example of a long division where no symbols or digits are given at all (Corrigan, well before

1930):

$$
\begin{array}{ccccccccccccc}
 & & & * & * & * & * & . & * & * & * & * & \\ \cline{4-12}
* & * & \multicolumn{1}{c|}{*} & * & * & * & * & * & * & & & & \\
 & & & * & * & * & & & & & & & \\ \cline{4-6}
 & & & & & * & * & * & & & & & \\
 & & & & & * & * & * & & & & & \\ \cline{6-8}
 & & & & & & * & * & * & & & & \\
 & & & & & & * & * & * & & & & \\ \cline{7-9}
 & & & & & & & * & * & * & & & \\
 & & & & & & & * & * & * & & & \\ \cline{8-10}
 & & & & & & & & & * & * & * & * \\
 & & & & & & & & & * & * & * & * \\ \cline{10-13}
\end{array}
$$

Does it look hopeless? Not really, if we do not forget about the decimal point. Inspecting this skeleton, we immediately see where zeros must be:

$$
\begin{array}{ccccccccccccc}
 & & & * & 0 & * & * & . & * & 0 & 0 & * & \\ \cline{4-12}
* & * & \multicolumn{1}{c|}{*} & * & * & * & * & * & * & & & & \\
 & & & * & * & * & & & & & & & \\ \cline{4-6}
 & & & & & * & * & * & & & & & \\
 & & & & & * & * & * & & & & & \\ \cline{6-8}
 & & & & & & * & * & * & & & & \\
 & & & & & & * & * & * & & & & \\ \cline{7-9}
 & & & & & & & * & * & 0 & & & \\
 & & & & & & & * & * & * & & & \\ \cline{8-10}
 & & & & & & & & & * & 0 & 0 & 0 \\
 & & & & & & & & & * & 0 & 0 & 0 \\ \cline{10-13}
\end{array}
$$

This information is enough to solve the puzzle and the solution is

$$
\begin{array}{cccccccccccc}
 & & & 1 & 0 & 1 & 1 & . & 1 & 0 & 0 & 8 \\ \cline{4-12}
6 & 2 & \multicolumn{1}{c|}{5} & 6 & 3 & 1 & 9 & 3 & 8 & & & \\
\end{array}.
$$

Ball and Coxeter (1974) give some basic principles that can be used to decipher skeleton puzzles. Cryptarithmetics can be combined with other number puzzles such as Sudoku to create "cryptic Sudoku". You can find a potpourri of other strange combinations like chessmetics, checkermetics, musicmetics, arithmogryphs, alphametic squares, alphametic poems and literature, alphametics consisting of prime numbers only, equation puzzles, etc. These are each interesting but their common problem is that almost all of them are generated by smart computer programs and can only be solved by other computer programs. This is not what we expect from a mathematical puzzle. The great masters of cryptarithmetics (Dudeney, Hunter, Madachy and others) created their puzzles using only paper and pencil and solved them without any artificial help.

The brute-force solution of a cryptarithmetic puzzle (in base 10) requires $10! = 3,628,800$ possible assignments of digits to letters. It is a manageable effort but there exist many computer programs that can solve such puzzles in much shorter time. On the web you can find a number of online solvers such as, for e.g.,

Naoyuki Tamura's "Cryptarithmetic Puzzle Solver"
bach.istc.kobe-u.ac.jp/llp/crypt.html

Truman Collins' "Alphametic Puzzle Solver"
www.tkcs-collins.com/truman/alphamet/alpha_solve.shtml

Robert Israel's "The Alphametic Applet"
geocities.com/rbisrael/metic/metic.html

When generalised to *arbitrary bases*, the problem of determining if a cryptarithm has a solution is NP-complete (Eppstein, 1987). Different strategies for solving cryptarithmetic problems were studied by Newell and Simon (1972).

Creation of cryptarithmetics is fun; let me show how I do it. I start with two words that I want to add. For example, Bill and Monica. To make the solution easy, I have to find a sum that contains most of the letters of the two addenda. In addition, it must tell me something about these two. This is a challenge even for a native speaker but English is my third language! Nevertheless, I was able to find about a dozen meaningful words. One of them even made sense; I was exceptionally lucky because the solution is unique and quite easy, and here it is:[2]

$$\begin{array}{rcccccc} & & & B & I & L & L \\ + & M & O & N & I & C & A \\ \hline & C & A & R & N & A & L \end{array}$$

References

[1] W.W.R. Ball and H.S.M. Coxeter, *Mathematical Recreations and Essays*, Dover, New York, 1974.

[2] M. Brooke, *One Hundred & Fifty Puzzles in Crypt-Arithmetic*, Dover, New York, 1963.

[3] A. Corrigan in: H. E. Dudeney, *536 Curious Problems & Puzzles*, Barnes & Noble, New York, 1995.

[4] H. E. Dudeney in: *Strand Magazine* **68** (1994), pp. 97 and 214.

[5] U. Dudley, *Journal of Recreational Mathematics* **10** (3) (1977–1978), p. 205, Problem #637.

[2][Editor's note: This problem refers to the so-called *Monica Lewinski scandal* which in 1998 focussed on USA President William Clinton's untruthful denial about his extramarital affair a few year prior with his then 22-year old intern Monica Lewinski. This scandal held and still holds great public fascination in USA. This, sadly, has led to almost two decades of nationwide bullying of Monica Lewinsky, who however has used this to become a successful anti-cyberbullying advocate.]

[6] D. Eppstein, On the NP–completeness of cryptarithms, *SIGACT News* **18** (3) (1987), 38–40.

[7] J.A.H. Hunter, *Entertaining Mathematical Teasers*, Dover, New York, 1983.

[8] J.A.H. Hunter and J. S. Madachy, *Mathematical Diversions*, Dover, New York, 1975.

[9] J.A.H. Hunter in: *Toronto – The Globe and Mail*, p. 27, 27 October 1955.

[10] S. Kahan, *Have Some Sums To Solve: The Complete Arithmetics Book*, Baywood Publishing, 1978.

[11] M. Kraitchik, *Mathematical Recreations*, W.W. Norton, New York, 1942.

[12] A. Newell and H.A. Simon, *Human Problem Solving*, Prentice–Hall, Englewood Cliffs, NJ, 1972.

[13] J. van der Elsen, *Alphametics*, Maastricht, 1998.