On property of least common multiple to be a D-magic number

V.L. Gavrikov
Institute of Ecology and Geography
Siberian Federal University
600041 Krasnoyarsk, pr. Svobodnyi 79
Russian Federation
vgavrikov@sfu-kras.ru

Abstract

Least common multiple (lcm) has been shown to posses the property of D-magic number, that is, its least significant digit 0 does not change when the number is transferred into all other numbering systems with smaller bases. The number $lcm + 1$ preserves this property as well.

Keywords: D-magic number, numbering systems, least common multiple, least significant digit

1 Introduction

Least common multiple (lcm) is a function which was often referred to as having two arguments, i.e. $lcm[x_1, x_2]$ but can be easily reformulated to any number of arguments, $lcm[x_1, x_2, \ldots, x_n]$.

The function has been widely known for being used at formulating of encryption algorithms, both in classical works [1] and in later research on encryption keys [2]. Because of its important applications properties of $lcm[\,]$ are of interest. An identity has been proven [3] that relates $lcm[]$ of binomial coefficients to $lcm[]$ of the sequence of indices of the coefficients. A typical behavior of $lcm[\,]$ of random subsets $\{1, \ldots, \mathrm{n}\}$ [4] has also been studied.

In this work, some properties of divisibility of $lcm[\,]$ function are explored that lead to a sort of invariance of the least significant digit of a number when the number is transferred to a different numbering system.

As usual, when a multidigit integer is transferred to a numbering system its least significant digit (as well as other digits) changes, e.g., $64_{10} = 100_8, 100_{10} = 244_6$. Sometimes however the transfer to another numbering sysytem does not lead to the change in the least significant digit, e.g., $126_{10} = 176_8, 101_{10} = 401_5$.

From these observations let us put a more general question: how can one get the the number that does not change its least significant digit when being transferred to another numbering system?

2 Formulation

Definition 2.1. *For an arbitrary base-L numbering system, D-magic number M is such a numberthat does not change its least significant digit when being transferred to any other base-l numbering system, with $l < L$.*

An integer number M in base-L system may be represented in *decimal* form:

$$M_L = L \cdot n + j, \tag{1}$$

where n is the number of tens in M_L and j is the least significant digit of M_L, with $j < L$.

If l is the base of numbering system then the transfer from M_L to M_l will include calculations of remainders from division by l both $L \cdot n$ and j. Provided these remainders are known a new value for j is received.

If $L \cdot n$ in Eq. (1) is divisible without a remainder by all l, $2 \leq l < L$, and $j < l$ then j will not change when M_L is transferred to any base-l system. There is an infinite quantity of numbers divisible by all $2 \leq l < L$ but the minimal of them is ony one. And this number is least common multiple. In other words, $lcm[\forall l, 2 \leq l < L]$ is a D-magic number in base-L system (as well as in all systems with bases smaller than L). Therefore, *calculation of* $lcm[\,]$ *is the very algorithm to get D-magic numbers.*

3 Illustrations

It is easy to find, e.g., in base-ten system , such a number that wil be divisible without a remainder by $10, 9, 8, 7, 6, 5, 4, 3, 2$. As well known, $lcm[10, 9, 8, 7, 6, 5, 4, 3, 2]$ = 2520 (see sequence A003418 in On-line Encyclopedia of Integer Sequences OEIS `http://oeis.org/A003418`).

A transfer of decimal number 2520 to any numbering system with bases $l < 10$ does not change the least significant digit (in this particular case $j = 0$):

l	M_l
10	252**0**
9	341**0**
8	473**0**
7	1023**0**
6	1540**0**
5	4004**0**
4	21312**0**
3	1011010**0**
2	10011101100**0**

Moreover, in case $j = 1$ (see Eq. 1) this least significant digit will not change as well:

l	M_l
10	252**1**
9	341**1**
8	473**1**
7	1023**1**
6	1540**1**
5	4004**1**
4	21312**1**
3	1011010**1**
2	10011101100**1**

If $j \in \{2, 3, 4, 5, 6, 7, 8\}$ such a property (constance of least significant digit) holds only at $j < l$.

Remark 3.1. Thus $lcm[10, 9, 8, 7, 6, 5, 4, 3, 2]$ equal to 2520 not only is D-magic number itself for base-ten numbering system but also produces a set of D-magic numbers–by adding of least significant digit $j < 10$.

Let us now look at how this approach works at $L \neq 10$.

For base-eight system, $lcm[8, 7, 6, 5, 4, 3, 2] = 840_{10} = 1510_8$. It can be seen that base-eight number 1510 does not change least significant digit when being transferred into numbering systems with bases $7, 6, 5, 4, 3, 2$:

l	M_l
8	151**0**
7	231**0**
6	352**0**
5	1133**0**
4	3102**0**
3	101101**0**
2	110100100**0**

Correspondingly, the base-eight number 1511_8 will also not change least significant digit when transferred into system with bases smaller than 8.

Another example, base-16 numbering system. $lcm[16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2] = 720720_{10} = aff50_{16}$. The transfer of number $aff50_{16}$ into systems with bases smaller than 16 gives:

l	M_l
16	aff5**0**
15	e383**0**
14	14a92**0**
13	1c308**0**
12	2a910**0**
11	45254**0**
10	72072**0**
9	131757**0**
8	257752**0**
7	606114**0**
6	2324040**0**
5	14103034**0**
4	223333110**0**
3	110012112210**0**
2	1010111111101010000**0**

Therefore least common multiple of $2, 3, 4, 5 \ldots L$ is a D-magic number for the numbering system with the base L (maximum of this sequence). A convenient algorithm could be as follows: 1) first, one gets $lcm[2, 3, 4, 5 \ldots L]$ for base-ten system and then 2) transfers it into system with the base L. This procedure leads to the number having 0 as least significant digit.

Adding of unity 1 to the list significant digit 0 brings about another D-magic number. Adding of a digit $j \in \{2, 3, 4, 5 \ldots L - 1\}$ to the least significant digit produces a set of set number that are partly D-magic; when being transferred into base-l systems the least significant digit j of them will not change only when $j < l$.

References

[1] Shannon C.E. 1949. Communication theory of secrecy systems. Bell Labs Technical Journal 28(4): 656–715.

[2] Rivest R.L., Shamir A., Adleman L. 1978. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2): 120–126.

[3] Farhi, B. 2009. An identity involving the least common multiple of binomial coefficients and its application. The American Mathematical Monthly, 116(9): 836–839.

[4] Cilleruelo J., Rué J., Šarka P., Zumalacárregui A. 2014. The least common multiple of random sets of positive integers. Journal of Number Theory, 144: 92–104.