Ancient Egyptians and Russian Peasants Foretell the Digital Age

D. N. Seppala-Holtzman

Suppose that you want to multiply two positive integers and that you had never mastered your multiplication tables. You are adept at addition and you can double integers quite well. Your ability to divide by 2, however, is quite spotty. You can handle it, but not when remainders are involved. In these cases, you just ignore remainders and truncate the results. Being able to add, you can utilize the fact that multiplication is nothing more than iterated addition, but this rapidly becomes unwieldy when the numbers become large. Your initial response is despair. Then, you discover two related techniques for multiplication, one used by the ancient Egyptians and the other by Russian peasants. In this article, we shall consider how each of them works, why each of them works, the relationship between the two, and what all of this has to do with the digital age.

ANCIENT EGYPTIAN MULTIPLICATION

First, let us consider the ancient Egyptian method of multiplication. If we wish to multiply positive integers N by M, we select one of the two, say N, and establish two columns, one headed by N and the other by 1. Below each header, we generate columns by doubling the number above it. We stop when we reach the largest power of 2 that does not exceed M. We choose exactly the entries in this column that add up to M and add the corresponding entries in the column headed by N. It is much simpler than it sounds. The following example should illustrate the method.

Suppose we wanted to multiply 25 by 23. We select one of the two, say 25, to head one column and let 1 head the other. See **figure 1**.

From the left-hand column, we select the entries 16, 4, 2, and 1, since these values sum to 23. That is to say, we choose all entries except 8. Crossing out the row that contains 8 in the left column and 200 in the corresponding place in the right column, we add the remaining entries of the right-hand column to obtain our answer: $25 \times 23 = 575$. See **figure 2**.

Naturally, multiplication is commutative, so we would very much hope that this process, despite the fact that it appears asymmetrical, would yield the same answer no matter which numbers were designated N and M. Let's look at **figure 3**. Here, we have crossed out the rows designated by 2 and 4 because $25 = 1 + 8 + 16$. Once again, we get the correct answer, 575. A coincidence? Articles are seldom written about coincidences—unless they are about probability theory. Nevertheless, skeptics are invited (make that *urged*) to try this method out on several pairs of positive integers of their own choosing.

Now that we have a pretty good idea that this process will yield the correct answer, let us examine why it works. The key is to translate M from base ten to base two. Recall how this is done. We begin by finding the highest power of 2 that does not exceed M. We now subtract that power of 2 from M and do the same with what remains after the power of 2 has been subtracted. We continue in this way until we have written M entirely as sums of powers of 2. Thus we see that $23 = 16 + 4 + 2 + 1$. Writing this out in base two we get $(23)_2 = 10111$. This notation means that:

$$23 = (\mathbf{1} \times 16) + (\mathbf{0} \times 8) + (\mathbf{1} \times 4) + (\mathbf{1} \times 2) + (\mathbf{1} \times 1)$$

Looking back at **figure 2**, we see that if we were to assign a 1 to each row that is not crossed out and a 0 to each row that is, we would get 10111 (reading from bottom to top). Similarly, $(25)_2 = 11001$. Assigning 1s and 0s to the rows in **figure 3** as we did above, yields the base-two representation of 25 (reading from bottom to top).

The reason that ancient Egyptian multiplication works should now be evident:

$$\begin{aligned} 23 \times 25 &= (16 + 4 + 2 + 1) \times 25 \\ &= (16 \times 25) + (4 \times 25) + (2 \times 25) + (1 \times 25) \\ &= 400 + 100 + 50 + 25 \\ &= 575 \end{aligned}$$

$$\begin{aligned} 25 \times 23 &= (16 + 8 + 1) \times 23 \\ &= (16 \times 23) + (8 \times 23) + (1 \times 23) \\ &= 368 + 184 + 23 \\ &= 575 \end{aligned}$$

RUSSIAN PEASANT MULTIPLICATION

Now let us now consider a related, slightly less transparent method of multiplication, called Russian peasant multiplication. As before, we begin with two positive integers, N and M, and establish two vertical columns. This time, we head one column by N and the other by M. Let N head the left-hand column and M the right-hand one. Under N, we shall successively double our entries. Under M, we shall repeatedly halve the entries, dropping remainders as we go. We stop when we reach 1 in the right-hand column. Now we cross out each row in which the number in the right-hand column is even and add the remaining entries in the left column. This gives us our result. As above, the apparent asymmetry of the roles of M and N is only superficial.

We illustrate this method with the same two choices of M and N, namely, 23 and 25. We shall let each integer play each role to demonstrate commutativity. See **figure 4**. Naturally, these two sets of summands should look familiar: They are precisely the same terms that gave us the answer of 575 in the previous method. But why should crossing out the even terms in the right-hand column produce the very same terms that the ancient Egyptian method gave us?

1	N
1	25
2	50
4	100
8	200
16	400

Fig. 1 Scheme for Egyptian multiplication of 25 by 23

1	N
1	25
2	50
4	100
~~8~~	~~200~~
+ 16	400
$M = 23$	$575 = M \times N$

Fig. 2 Since 1 + 2 + 4 + 16 = 23, include only those rows.

1	N
1	23
~~2~~	~~46~~
~~4~~	~~92~~
8	184
+ 16	368
$M = 25$	$575 = M \times N$

Fig. 3 Commutativity holds in this method of multiplication.

N	M		N	M
23	25		25	23
~~46~~	~~12~~		50	11
~~92~~	~~6~~		100	5
184	3		~~200~~	~~2~~
+ 368	1		+ 400	1
575			575	

Fig. 4 Scheme for Russian peasant method for multiplying 23 by 25

N	M	M_2		N	M	M_2
23	25	11001		25	23	10111
~~46~~	~~12~~	1100		50	11	1011
~~92~~	~~6~~	110		100	5	101
184	3	11		~~200~~	~~2~~	10
+ 368	1	1		+ 400	1	1
	575				575	

Fig. 5 Scheme with binary representations included

THE CONNECTION BETWEEN THE TWO METHODS

We now show how Russian peasant multiplication is related to the ancient Egyptian method and, in the process, validate it. Before we proceed, let us introduce some notation that will expedite the exposition. For any positive real number, M, we denote by $[M]$ *the greatest integer not exceeding* M. If M happens to be an integer, then $M = [M]$. If M is not an integer, $[M]$ is just M with its fractional part excised. We call this excision *truncation*. Thus, $[23] = 23$ and $[23.792] = 23$. Note that dividing M by 2 and dropping the possible remainder can now be denoted by $[M/2]$.

Now let us begin our exploration of the Russian peasant algorithm by examining what happens to the binary representation of a number when it is divided by 2 and its remainder, if there is one, is dropped. Consider the following examples:

$$(23)_2 = 10111 \quad [23/2]_2 = (11)_2 = 1011$$
$$(22)_2 = 10110 \quad [22/2]_2 = (11)_2 = 1011$$
$$(28)_2 = 11100 \quad [28/2]_2 = (14)_2 = 1110$$

You will notice that in each of these examples, halving and truncating a number has the effect of chopping off the right-most digit in its binary representation. Thus, the process of halving and truncating turns 10111 into 1011. The right-most "1" is dropped. Likewise, 10110 becomes 1011 under this process, and the right-most "0" is dropped.

Is this true in general, and if it is, what does it have to do with Russian peasant multiplication? The answers are, respectively, "yes" and "everything." First, the "yes."

THEOREM. Let S be a positive integer and let T be the result of halving and truncating S. Thus, $T = [S/2]$. Then, the binary representation of T is precisely the binary representation of S with the right-most digit chopped off.

PROOF. Let us consider two cases.

Case 1: Let S be even. Clearly, in this case, the right-most binary digit of S is 0. Suppose that $S = 2^a + 2^b + 2^c + \cdots + 2^k$ where $a > b > \ldots > k$ and $a, b, c, \ldots, k$ are natural numbers. Then the binary representation of S will have 1s in positions $(a + 1)$, $(b + 1)$, $(c + 1)$, $\ldots$, $(k + 1)$ and 0s everywhere else. (Recall that the coefficient of 2^0 is in the units, or first, place, the coefficient of 2^1 is in the second place, and so on.) Now, since S is even, k must be larger than 0. Dividing S by 2 will yield $S/2 = 2^{a-1} + 2^{b-1} + 2^{c-1} + \cdots + 2^{k-1}$. Moreover, as S is even, there is no remainder to drop, so truncation has no effect. It follows that the binary representation of $[S/2]$ will have 1s in positions $a, b, c, \ldots, k$ and 0s everywhere else. Thus, all of the 1s will be shifted one position to the right and the right-most 0 will be dropped. This proves the result in the case that S is even.

Case 2: Let S be odd. Let us write S as $(S - 1) + 1$. Then $[S/2] = [(1/2)((S - 1) + 1)] = [(S - 1)/2 + (1/2)] = (S - 1)/2$, since $S - 1$ is obviously even. Now, by Case 1, all the 1s will be shifted one position to the right and the right-most 1 will be dropped. This proves the result in the case that S is odd.

It may prove helpful to reexamine the three examples given before the theorem (**figs. 2–4**) as an aid to understanding the general case. In particular, the examples of 23 and 22 illustrate the relationship between the odd and even cases in the proof. In particular, we note that, when S is odd,

$$[S/2] = [(S - 1)/2] \\ = (S - 1)/2.$$

Now, back to our Russian peasants. Let us reexamine **figure 4**, but with one additional piece of information. Let us include the binary representations of the numbers in the columns headed by M in a new column: M_2. See **figure 5**.

Several observations are in order. First, note how the binary representations in the M_2 columns illustrate the theorem. The right-most digit is dropped in each successive row. As a result of this, observe that, reading from the bottom upward, the right-most digit of the number in the M_2 column is precisely the binary representation of the number M. In the left-hand case, $M = 25$ and $25_2 = 11001$. Reading from the bottom up, the right-most digits are 1, 1, 0, 0, and 1. In other words, reading upward, the first, second, and fifth rows correspond to the three 1s in $25_2 = 11001$, in the first, second, and fifth positions, reading from left to right. Thus, the 1s in the binary representation of M select which rows in the column headed by N contribute to $M \times N$.

Similarly, in the right-hand column in **figure 5**, $23_2 = 10111$. Reading from the bottom up, the first, third, fourth, and fifth rows contribute to the product, $N \times M$.

Ancient Egyptian				Russian Peasant	
1	N			N	M
1	25	1		25	23
2	50	1		50	11
4	100	1		100	5
~~8~~	~~200~~	0		~~200~~	~~2~~
+16	400	1	↑ $(23)_2$	+400	1
$575 = M \times N$				$M \times N = 575$	

Fig. 6 The two methods viewed side by side

Thus, exactly as with the ancient Egyptian method, we get

$$\begin{aligned} 25 \times 23 &= (16 + 8 + 1) \times 23 \\ &= (16 \times 23) + (8 \times 23) + (1 \times 23) \\ &= 368 + 184 + 23 \\ &= 575 \end{aligned}$$

and

$$\begin{aligned} 23 \times 25 &= (16 + 4 + 2 + 1) \times 25 \\ &= (16 \times 25) + (4 \times 25) + (2 \times 25) + (1 \times 25) \\ &= 400 + 100 + 50 + 25 \\ &= 575. \end{aligned}$$

In other words, the grounds for crossing out a row in the ancient Egyptian and Russian peasant methods correspond precisely. As such, the exact same terms in the column headed by N (the doubling column) contribute to and add up to the same answer. Thus, these two methods of multiplication are now seen to be equivalent to one another. Let us view the two methods, side by side, with $M = 23$ and $N = 25$. See **figure 6**.

So there we have it: These two rather primitive-looking algorithms are valid, equivalent, and, at their core, powered by properties of the base-two number system. In the case of the ancient Egyptian algorithm, we had to provide the base-two representation of M ourselves by selecting the rows that added up to M. In the Russian peasant algorithm, the process of halving and truncating provided this representation for us. In both cases, the driving force is the base-two number system, the very same force behind today's digital age.