Journal of Advances in Applied Mathematics, Vol. 4, No. 2, April 2019
https://dx.doi.org/10.22606/jaam.2019.42004

Number of Digits in Two Integers and Their Multiplication

Xingbo WANG

Department of Mechatronic Engineering, Foshan University, Foshan, China
Guangdong Engineering Center of Information Security for Intelligent Manufacturing System, Foshan, China
State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi, China
Email: dr.xbang@qq.com; xbwang@fosu.edu.cn

Abstract. This paper first proves a formula that discloses the relationship between the number of digits in multiplication and its two divisors, then proves that the two divisors are of the equal length if the divisor-ratio generated from the bigger divisor divided by the small one is smaller than 10. Hence the paper shows that, all the RSA numbers must have two divisors of the equal length.

Keywords: Number of digits, multiplication, divisor, RSA number.

1 Introduction

Analysing the arithmetic calculations, 1035918371=32717×31663, 170442776634553 =228479×745988807 and 1123877887715932507=299155897×3756830131, one can see that, the semiprimes, 1035918371, 170442776634553 and 1123877887715932507 are decimal integer with 10, 15 and 19 decimal digits respectively, and the number of the digits in the 6 divisors of the 3 semiprimes are (5,5), (6,9) and (9,10) respectively. Coincidentally, 10=5+5, 15=6+9 and 19=9+10. Are these really coincidental? Look at more examples list in Table 1.

Table 1. Number of digits in semiprimes and their divisors

m=p×q	digit(m), digit(p), digit(q)
16637=131×127	5, 3, 3
2129189=2003×1063	7, 4, 4
4538873=2237×2029	7, 4, 4
8772041=3299×2659	7, 4, 4
1035918371=32717×31663	10, 5, 5
2512642129=51071×49199	10, 5, 5
5783560579=81017×71387	10, 5, 5
9048212729=99871×90599	10, 5, 5
80735174503=311393×259271	11, 6, 6
211041144109=511279×412771	12, 6, 6
170442776634553=228479×745988807	15, 6, 9
1808898276844231=2424833×745988807	16, 7, 9
35249679931198483=59138501×596052983	17, 8, 9
37522676526028537=193707721×193707697	17, 9, 9
556499304645216091=745988813×745988807	18, 9, 9
1123877887715932507=299155897×3756830131	19, 9, 10
1129367102454866881=25869889×43655660929	19, 8, 11
1902408569846737793=745988807×2550183799	19, 9, 10
10188337563435517819=70901851×143696355169	20, 8, 12
24928816998094684879=347912923×71652460573	20, 9, 11

Apart from the examples in Table 1, analyzing the RSA numbers [1] yields the following Table 2.

Table 2. Number of digits in RSA numbers and their divisors

No.	RSA numbers	D_{RSA}	D_p	D_q
1	RSA100	100	50	50
2	RSA110	110	55	55
3	RSA120	120	60	60
4	RSA129	129	64	66
5	RSA130	130	65	65
6	RSA140	140	70	70
7	RSA150	150	75	75
8	RSA155	155	78	78
9	RSA160	160	80	80
10	RSA170	170	85	85
11	RSA180	180	90	90
12	RSA190	190	95	95
13	RSA200	200	100	100
14	RSA210	210	105	105
15	RSA220	220	110	110
16	RSA576	174	87	87
17	RSA640	193	97	97
18	RSA704	212	106	106
19	RSA768	232	116	116
20	RSA230	230	115	115

Obviously, it seems to have the following formula

$$D_m = D_p + D_q \quad \text{or} \quad D_m = D_p + D_q - 1 \tag{1}$$

where D_p, D_q and D_m mean number of digits in divisor p, divisor q and their multiplication $m = p \times q$ respectively.

Now comes a question, is the formula (1) true? And under what condition it is true if it is true? This paper answers the questions.

2 Preliminaries

The floor function of real number x is denoted by symbol $\lfloor x \rfloor$ that satisfies $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$; the fraction part of x is denoted by symbol $\{x\}$ that satisfies $x = \lfloor x \rfloor + \{x\}$. Symbol D_n is the decimal digits of positive integer n. In this whole article, $A \Rightarrow B$ means conclusion B can be derived from condition A; $A \Leftrightarrow B$ means B holds if and only if A holds. Symbol $A \oplus B$ means A or B holds.

Lemma 1. (See in [2]) A positive integer n with base b has $\lfloor \log_b n \rfloor + 1$ digits.

Lemma 2. (See in [3]) Let x and y be real numbers; then

(**P1**) $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$

(**P2**) $\lfloor x \rfloor - \lfloor y \rfloor - 1 \le \lfloor x - y \rfloor \le \lfloor x \rfloor - \lfloor y \rfloor < \lfloor x \rfloor - \lfloor y \rfloor + 1$

(**P3**) $\lfloor 2x \rfloor + \lfloor 2y \rfloor \ge \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor$

(**P13**) $x \le y \Rightarrow \lfloor x \rfloor \le \lfloor y \rfloor$

(**P20**) $\lfloor \sqrt{x} \rfloor = \lfloor \sqrt{\lfloor x \rfloor} \rfloor$ with $x \ge 0$

(**P21**) $\lfloor \log_b x \rfloor = \lfloor \log_b \lfloor x \rfloor \rfloor$ with $x > 0$

Lemma 3. (See in [4]) Let α and x be positive real numbers; then it holds

$$\alpha \lfloor x \rfloor - 1 < \lfloor \alpha x \rfloor < \alpha(\lfloor x \rfloor + 1)$$

Particularly, if α is a positive integer, say $\alpha = n$, then it yields

$$n\lfloor x\rfloor \le \lfloor nx\rfloor \le n(\lfloor x\rfloor +1)-1$$

3 Main Results and Proofs

Theorem 1. Let m, p and q be positive integers and $m = pq$; then

$$D_p + D_q - 1 \le D_m \le D_p + D_q \tag{2}$$

Proof. It yields by the given conditions and Lemma 2

$$m = pq \Rightarrow D_m = \lfloor \log_{10} pq\rfloor + 1 = \lfloor \log_{10} p + \log_{10} q\rfloor + 1 \le \lfloor \log_{10} p\rfloor + \lfloor \log_{10} q\rfloor + 2 = D_p + D_q$$

Meanwhile, since $\lfloor \log_{10} p\rfloor + \lfloor \log_{10} q\rfloor \le \lfloor \log_{10} p + \log_{10} q\rfloor$, it holds

$$D_m = \lfloor \log_{10} pq\rfloor + 1 = \lfloor \log_{10} p + \log_{10} q\rfloor + 1 \ge \lfloor \log_{10} p\rfloor + \lfloor \log_{10} q\rfloor + 1 = D_p + D_q - 1$$

Thereby it holds

$$D_p + D_q - 1 \le D_m \le D_p + D_q$$

which is just the (2).

□

Theorem 2. Suppose m is a positive integer and $s = \lfloor \sqrt{m}\rfloor$; then

$$2D_s - 1 \le D_m \le 2D_s$$

Proof. By the given conditions and Lemma 2 (P21) as well as Lemma 3, it leads to

$$m = \sqrt{m}\cdot\sqrt{m} \Rightarrow D_m = \lfloor \log_{10}(\sqrt{m}\cdot\sqrt{m})\rfloor + 1 = \lfloor 2\log_{10}\sqrt{m}\rfloor + 1 = \lfloor 2\log_{10}\lfloor\sqrt{m}\rfloor\rfloor + 1 = \lfloor 2\log_{10} s\rfloor + 1$$

That is

$$2\lfloor \log_{10} s\rfloor + 1 \le D_m \le 2(\lfloor \log_{10} s\rfloor + 1) - 1 + 1 = 2(\lfloor \log_{10} s\rfloor + 1)$$

which is

$$2D_s - 1 \le D_m \le 2D_s \tag{3}$$

□

Example 1. Choose 13 integers by

$$Od := Array([16637,\ 2129189,\ 4538873,\ 8772041,$$
$$1035918371,\ 2512642129,\ 5783560579,\ 9048212729,\ 80735174503,$$
$$211041144109,\ 170442776634553,\ 1808898276844231,\ 35249679931198483])$$

Program in Maple with the following codes

```
digit := proc(N)
 local m, dl, db, ds;
  dl := floor(log10(N)) + 1;
 m := floor(sqrt(N));
 db := floor(log10(m)) + 1;
 db := 2·db;
 ds := db − 1;
  printf("%d %d %d\n", ds, dl, db);
  return;
end
```

And run the program with command

for k to 13 do digit(Od(k)) end do

The output is as follows


```
5 5 6
7 7 8
7 7 8
7 7 8
9 10 10
9 10 10
9 10 10
9 10 10
11 11 12
11 12 12
15 15 16
15 16 16
17 17 18
```

The output matches to the Theorem 2.

Corollary 1. Suppose m is a positive integers and $s = \lfloor \sqrt{m} \rfloor$; then

$$D_s = \begin{cases} \dfrac{D_m}{2}, D_m \text{ is even} \\ \dfrac{D_m + 1}{2}, D_m \text{ is odd} \end{cases} \tag{4}$$

Proof. Since D_m is an integer, the inequality (3) shows that, when D_m is even it is equal to $2D_s$ while it is equal to $2D_s - 1$ when it is odd.

□

Theorem 2. Suppose m, p and q are positive integers with $1 < p \le q$; let $m = pq$ and $k = \dfrac{q}{p}$; then

$$D_q = \begin{cases} \dfrac{D_m}{2} \oplus (\dfrac{D_m}{2} + 1), \ D_m \text{ is even} \\ \dfrac{D_m + 1}{2}, \ D_m \text{ is odd} \end{cases}$$

Proof. By the given conditions it yields

$$m = pq \Rightarrow D_m = D_{pq} = \lfloor \log_{10}(pq) \rfloor + 1 = \left\lfloor \log_{10}(\frac{q^2}{k}) \right\rfloor + 1 = \lfloor 2\log_{10} q - \log_{10} k \rfloor + 1$$

By Lemma 1 (P2), it yields

$$\lfloor 2\log_{10} q \rfloor - \lfloor \log_{10} k \rfloor \le D_m \le \lfloor 2\log_{10} q \rfloor - \lfloor \log_{10} k \rfloor + 1$$

Note that, $k < 10$ yields $\lfloor \log_{10} k \rfloor = 0$; hence it holds

$$\lfloor 2\log_{10} q \rfloor \le D_m \le \lfloor 2\log_{10} q \rfloor + 1$$

By Lemma 3, it holds

$$2\lfloor \log_{10} q \rfloor \le D_m \le 2(\lfloor \log_{10} q \rfloor + 1)$$

That is

$$2(D_q - 1) \le D_m \le 2D_q$$

Since D_m is an integer, it takes $2D_q - 1$ when it is odd. Thereby, when D_m is odd, $D_q = \dfrac{D_m + 1}{2}$, whereas, when it is even $D_q = \dfrac{D_m}{2} \oplus (\dfrac{D_m}{2} + 1)$

□

Theorem 3. Suppose m, p and q are positive integers with $1 < p \le q$; let $m = pq$ and $k = \dfrac{q}{p}$; then $1 \le k < 10$ yields $D_p = D_q$.

Proof. From the given conditions, it can see

$$m = pq \Rightarrow m = kp^2 \Rightarrow \begin{cases} p^2 = \dfrac{m}{k} \Rightarrow 2\log_{10} p = \log_{10} m - \log_{10} k \\ q^2 = km \Rightarrow 2\log_{10} q = \log_{10} m + \log_{10} k \end{cases}$$

Since $k < 10$ yields $\lfloor \log_{10} k \rfloor = 0$; hence when $k < 10$ it holds

$$\log_{10} p = \log_{10} q$$

which naturally results in

$$D_p = D_q$$

□

Corollary 2. Suppose m, p and q are positive integers with $1 < p \le q$; let $m = pq$ and $k = \dfrac{q}{p}$; then $1 \le k < 10$ yields

$$D_p = D_q = \begin{cases} \dfrac{D_m}{2} \oplus (\dfrac{D_m}{2} + 1), \ D_m \text{ is even} \\ \dfrac{D_m + 1}{2}, \ D_m \text{ is odd} \end{cases}$$

Proof. (Omitted).

Example 2. Look at Table 1 and analyze the data in the table, it can see that, all the data fit Corollary 2. In addition, take the RSA numbers as examples, analyze their divisor-ratios and number of digits in the RSA numbers and their divisors; the results are list in Table 3. It can see these data completely fit Corollary 2.

Table 3. RSA numbers, their divisor-ratios plus related number of digits

No.	RSA numbers	k=q/p	D_{RSA}	D_p	D_q
1	RSA100	1.056	100(even)	50	50
2	RSA110	1.047	110(even)	55	55
3	RSA120	2.118	120(even)	60	60
4	RSA129	93.880>10	129(odd)	64	66
5	RSA130	1.147	130(even)	65	65
6	RSA140	1.843	140(even)	70	70
7	RSA150	1.281	150(even)	75	75
8	RSA155	1.039	155(even)	78	78
9	RSA160	1.043	160(even)	80	80
10	RSA170	1.188	170(even)	85	85
11	RSA180	1.190	180(even)	90	90
12	RSA190	1.897	190(even)	95	95
13	RSA200	2.244	200(even)	100	100
14	RSA210	1.290	210(even)	105	105
15	RSA220	2.084	220(even)	110	110
16	RSA576	1.188	174(even)	87	87
17	RSA640	1.163	193(odd)	97	97
18	RSA704	1.116	212(even)	106	106
19	RSA768	1.098	232(even)	116	116
20	RSA230	1.141	230(even)	115	115

Corollary 3. All the RSA numbers must have two divisors of the equal length.

Proof. By the American Digital Signature Standard (DSS)[5], an RSA number, is a big semiprime composed of two distinct prime divisors, say p and q with $3 \le p < q$ such that $1 < q / p < \sqrt{2}$. By Corollary 2, it is sure that all the RSA numbers must have two divisors of the equal length.

□

4 Conclusion

Knowing the relationship between multiplication and its factors helps know the range of the factors in practice of integer factorization. By the conclusions drawn in this paper, it is known that the two divisors of an RSA number are of the equal length. This provides a mathematical foundation in knowing of the RSA numbers. Hope to be a benefit to the researchers.

Acknowledgments. The research work is supported by the State Key Laboratory of Mathematical Engineering and Advanced Computing under Open Project Program No.2017A01, Department of Guangdong Science and Technology under project 2015A010104011, Foshan Bureau of Science and Technology under projects 2016AG100311, Project gg040981 from Foshan University. The authors sincerely present thanks to them all.

References

1. wikipedia. RSA number, https://en.wikipedia.org/wiki/RSA_numbers
2. K H Rosen. *Elementary Number Theory & Its Application* (6th eds), Addison-Wesley ,2010, pp.66
3. X WANG. "Brief Summary of Frequently-Used Properties of the Floor Function," *IOSR Journal of Mathematics*, vol. 13, no. 5, pp. 46 – 48, 2017.
4. X WANG, "Some New Inequalities With Proofs and Comments on Applications," *Journal of Mathematics Research*, vol. 11, no. 3, pp. 15-19, 2018
5. National Institute of Standards and Technology (NIST). Digital signature standard (DSS), FIPS publication 186-3, June 2009.

