**Nikolaus Castell-Castell**

**Prague Research Institute**

**Zug (CH) und Prag (CR)**

**27/02/2020**

**RSA, PGP, Bitcoin & Co.**

**25 partial considerations, using only multiplication and division to break down a composite product into its prime factors.**

**Consideration 8.**

**Lists for factoring large numbers and findings on the double rows used here and their sequences using the "Castell’s slide rule"**

For every possible total number between 0 and 9, the known double series of numbers are created. Since these only deliver the double digits 0 to 9, the result is 10 \* 10 double digits.

In the resulting table of 100 double digits, it is not asked whether there are transfers or not, and if so, which and where which constant factors are used, but all double digits are factored with all possible possibilities and then multiplied.

A “1” as the final prime digit is calculated as if it were certain that it represents 1 \* 1 or 3 \* 7 or 9 \* 9 without asking questions about transfers or factor pairs.

Assuming that it is about the double digit of the 2nd column, 5 + 9. Then these two digits 5 and 9 are not yet factors, but only small products from the factors still sought, ie products with their unit digits in the columns can be seen (while their decimal places are hidden).

After factoring these small products, for example, together with the factors “3” and “7” (and tentatively also the others mentioned), which resulted from the factorization of the 1st column, two 2-digit factors arise that already existed before their Completion can be multiplied with each other on a trial basis. If afterwards, ie after applying the corresponding factors, e.g. the factor “3” for the “5” at the top of the 2nd column and the factor “7” for the “9” at the bottom of the 2nd column, the corresponding pairs of numbers (ie Here 57 and 73) are multiplied with each other, they can already be compared to some extent with the first digits of the large number (counting from the right) and from 10 alternatives show the two-by-two-digit pair of numbers that is most similar to the first total numbers and thus represents the “correct” pair of factors out of a total of 10 pairs of factors that can be selected.

If the other possible factors are calculated in other combinations in the procedure proposed here, other factor digits will result. These can also be compared with each other and also provide information on the questions of whether there is a “transfer” and how large it is, which factors in which combination are the right ones, etc.

But these questions are not effective, because it is only a matter of finding the correct two factor numbers in their 2nd position (from the right) for 2 searched multi-digit prime factors, which in the given example result from the column numbers in the 2nd column (Summands) 5 and 7 resulted.

**Lists:**

In order to create a comprehensive concept, all 10 possible opposing series of numbers (from 0 + 10 to 0 + 19) per 10 double digits (from 0 to 9) are recorded, i.e. 100 double digits are created, which are then followed by 4 prim -End factors and their combinations (1 \* 1, 3 \* 7 (7 \* 3), 9 \* 9, 3 \* 1, 7 \* 9 (9 \* 7), 7 \* 1, 3 \* 9 (9 \* 3), 9 \* 1, 3 \* 3, 9 \* 9) can be factored.

**The 10 double rows of numbers:**

**0 1 2 3 4 5 6 7 8 9**

**+10 9 8 7 6 5 4 3 2 1**

**0 1 2 3 4 5 6 7 8 9**

**+11 10 9 8 7 6 5 4 3 2**

**0 1 2 3 4 5 6 7 8 9**

**+12 11 10 9 8 7 6 5 4 3**

**0 1 2 3 4 5 6 7 8 9**

**+13 12 11 10 9 8 7 6 5 4**

**0 1 2 3 4 5 6 7 8 9**

**+14 13 12 11 10 9 8 7 6 5**

**0 1 2 3 4 5 6 7 8 9**

**+ 15 14 13 12 11 10 9 8 7 6**

**0 1 2 3 4 5 6 7 8 9**

**+ 16 15 14 13 12 11 10 9 8 7**

**0 1 2 3 4 5 6 7 8 9**

**+ 17 16 15 14 13 12 11 10 9 8**

**0 1 2 3 4 5 6 7 8 9**

**+ 18 17 16 15 14 13 12 11 10 9**

**( 0 1 2 3 4 5 6 7 8 9**

**+19 18 17 16 15 14 13 12 11 10 )**

Logically, these series of numbers are already ordered due to their cardinal order and analogous countercurrent, i.e. they show patterns that are so clear that additions are possible without calculations and errors that would represent deviations can be recognized immediately.

If the first two factors (from the right) should be calculated from the existing pairs of numbers, the algorithm has, as always, the choice of calculating according to specifications or it asks for lists, such as the aforementioned 18 double rows or the following, 1s, Lines of 3, 7, 9, which “at a glance” show the only numbers that can occur in the factorization.

**The 4 series of prime numbers**

0, 1, 2, 3, 4, 5, 6, 7, 8, 9 (for the factor "1"),

0, 3, 6, 9, 12, 15, 18, 21, 24, 27 (for the factor "3"),

0, 7, 14, 21, 28, 35, 42, 49, 56, 63 (for the factor "7"),

0, 9, 18, 27, 36, 45, 54, 63, 72, 81 (for the factor "9")

The above double rows show digits that are placed in different relationships to each other in order to find the two digits that have to be searched for in each column of the invoice. They have to be searched for, since only 1 factor number is known as the only number in each case, but the other must be searched for methodically and then 10 pairs of factor numbers can be found using test divisions.

The two column numbers that belong together are available 10 times, but must first be factored in order to be able to be test-multiplied.

Here, too, the algorithm has the option of converting the existing column numbers into factor numbers, using the method mentioned to divide each factorizable number by 0 to 9 and thus to find its only 2 possible factors or it asks the following list, which " at a glance ”shows which factor numbers correspond to which column numbers.

**The conversion of the two column digits into the two factor digits**

Searched factor for the upper column number (“neck”) \* constant 1st number factor and inside constant factor for the lower column number \* searched 2nd number number (in the known example it looked like this (from right to left): 5 7 \* 7 3, ie 5 \* 3 for the upper number and 7 \* 7 for the lower.

**Change of the column numbers (which represent the unit numbers of 1- and 2-digit products) in their factor numbers within the framework of their above-mentioned prime end number series**

**For the factor 3:**

**0** = 0 : 3 = **0**

**1**= 21 : 3 = **7**

**2**= 12 : 3 = **4**

**3**= 3 : 3 = **1**

**4**= 24 : 3 = **8**

**5**= 15 : 3 = **5**

**6**= 6 : 3 = **2**

**7**= 27 : 3 = **9**

**8**= 18 : 3 = **6**

**9**= 9 : 3 = **3**

**For the factor 7:**

**0** = 0 : 7 = **0**

**1**= 21 : 7 = **3**

**2**= 42 : 7 = **6**

**3**= 63 : 7 = **9**

**4**= 14 : 7 = **2**

**5**= 35 : 7 = **5**

**6**= 56 : 7 = **8**

**7**= 7 : 7 = **9**

**8**= 28 : 7 = **4**

**9**= 49 : 7 = **7**

**For the factor 9:**

**0** = 0 : 9 = **0**

**1**= 81 : 9 = **9**

**2**= 72 : 9 = **8**

**3**= 63 : 9 = **7**

**4**= 54 : 9 = **6**

**5**= 45 : 9 = **5**

**6**= 36 : 9 = **4**

**7**= 27 : 9 = **3**

**8**= 18 : 9 = **2**

**9**= 9 : 9 = **1**

**Different ways to calculate with the above 10 double rows:**

In the following, the two sought-after multi-digit prime factors, which have formed the large number (actually present as the so-called total line) by multiplication, are shown in the context of their changing two constant factors that determine them up to the 2nd digit.

This two-digit number achieved (up to now) is important because only the 2nd digit of the large number is important. The results obtained here determine the continuation of the only algorithmic (i.e. methodologically uncomplicated, because always the same) calculations.

**The "Castell’s slide rule"**

Consistent further thinking of the above considerations leads to a new approach to solve the problem with the first two (right) digits of the large number!

As has been emphasized many times, the hurdle of the first two numbers (on the right-hand side) is by far the highest (see also essay part 6), because the questions always remain open: “Is there a transfer, ie with which factors must in the 2nd and each subsequent column of the 1st line, what is the order? " etc.), and you can therefore only guess, in order to have to stop afterwards if necessary, to return to the starting point of the 1st column and start again with a new factor.

At the same time, as has often been shown in the previous essays, it is precisely this first decision that is the most decisive. Because the two factors sought, in their correctly maintained order, are decisive for the entire further calculation, since they remain constant.

The first “left digit” found is the so-called header, i.e. the 1st digit of each line that is added again and again, which as a multi-digit, sought “counted factor” always remains the same in the entire calculation. As shown in the first paragraph, this fact is just difficult to recognize, since every new line that is added slides one place to the side (in the calculation method chosen here, this is the direction to the left) and has its own new numerical number, ie it is optically “falsified ”Works. In fact, these lines are always exactly the same within the invoice. The one multi-digit factor you are looking for always consists of the same digits, which, from right to left, were called “head”, “neck”, “chest” etc. in earlier essays.

The second “right digit” found is a sequence of individual numerical digits (listed here from right to left) that have nothing to do with each other, only show the “incorrect” numerical digits for the various lines from right to left. Since only one of these numerals is responsible for a certain line, one can imagine this multi-digit “counting factor” as moving, while the multi-digit “counted factor” (here on the left) remains immobile, static, or as above was called, always the same.

That this picture in the previous paragraph is not arbitrary, but arises arithmetically, can be seen from the following “Castell’s slide rule”. This designation is arbitrary and not meant to be dogmatic, but is intended to illustrate the aforementioned principle:

The upper part, in which the 1st line with the 1st digit (in the example mostly used here was the units digit “1” of “21” and to the left of it the “5” of “15” in the 2nd column ) remains, regardless of which total number is under the 1st and additionally 2nd column, the order of the numerical values ​​always remains the same.

The entire, multi-line, lower part under this 1st line is always in lateral movement within the scope of its decimal possibilities. Specifically, it moves with every change in the total number, e.g. in cardinal order, in small steps of one and in one direction (here to the left), permanently!

Because one part (here the part above) remains constant, while the lower part changes and results in different values ​​in the total line in relation to the above part or, conversely, reacts to other values ​​in the total line, the picture of a simple slide rule is presented at.

The digits occurring here are the digits that are shown in pairs at the top and bottom when using the so-called double row method. Specifically, these upper digits always remain the same in the upper digit sequence, regardless of the numerical value of the corresponding total digit, while the lower digit is adapted to the common total digit.

The total digits that occur are 0 to 9 or 10 to 19. (Both are identical, depending on whether the respective units digit is on the numerically higher left side of the lower line or on its right side (because the lower line begins with its theoretically possible highest value (e.g. 19, 18, 17 etc.) and counts down to the right.) The movement of the bottom row takes place as follows: With every further step up in the total number of the 2nd column, the one on the far right moves outer digit of the lower line to the left to the beginning (this time calculated from left to right).

In the following, the only possible 10 cases of the relation between the constant upper part and the changing lower part are shown: The sum figure and the left-hand initial figure of its lower summand is 10, or 11 or 12, etc. to 19).

The number after the equal sign on the right is the factor that resulted from the factorization. It is calculated by adding the column number created using the double row method with its decimal number, if available, and dividing it with the correctly selected PrimEnd factor (1, 3, 7, 9).

The units digit cannot be seen without adding its decimal place, which prime final number it represents and which factorization digit it will produce. Depending on the added decimal digit (or the information that it does not have a decimal place in this case), other factorization factors result.

So the ones digit “4” with the prime end factor “1” together is a “4” and also results in a “4” when factoring. But even with the prime ending digit “3”, this “4” becomes a “24” and results in (24: 3 =) a factorization digit equal to “8”. With the prime end digit 7 (14: 7 =) results in a factorization digit of “2” and with the prime end digit “9” this “4” becomes “54” and results in (54: 9 =) a factorization Digit from 6.

The above takes place in the same way with all 10 digits (the only exception is the “5”, where the factorization digits always give “5”. However, the difference remains that the total number, “5”, “15”, “35” and “45” cause different transfers (namely 0, 1, 3 or 4) in the calculation

**Upper part:**

**Always the same row above, in four versions (i.e. divided into rows of 1, 3, 7 and 9):**

**0 1 2 3 4 5 6 7 8 9**

**0 : 1 =0 1:1=1 2:1=2 3:1=3 4:1=4 5:1=5 6:1=6 7:1=7 8:1=8 9:1=9**

**0:3=0 21:3=7 12:3=4 3:3=1 24:3=8 15:3=5 6:3=2 27:3=9 18:3=6 9:3=3**

**0:7=0 21:7=3 42:7=6 63:7=9 14:7=2 35:7=5 56:7=8 7:7=1 28:7=4 49:7=7**

**0:9=0 81:9=9 72:9=8 63:9=7 54:9=6 45:9=5 36:9=4 27:9=3 18:9=2 9:9=1**

**Lower part:**

**Rows of 1, 3, 7, 9 at the bottom (in ten versions, i.e. for the total numbers 10 to 19).**

**Here for total number 10 below:**

**+10 9 8 7 6 5 4 3 2 1**

**0 :1 =0 9:1=9 8:1=8 7:1=7 6:1=6 5:1=5 4:1=4 3:1=3 2:1=2 1:1=1**

**0:3=0 9:3=3 18:3=6 27:3=9 6:3=2 15:3=5 24:3=8 3:3=1 12:3=4 21:3=7**

**0:7=0 49:7=7 28:7=4 7:7=1 56:7=8 35:7=5 14:7=2 63:7=9 42:7=6 21:7=3**

**0:9=0 9:9=1 18:9=2 27:9=3 36:9=4 45:9=5 54:9=6 63:9=7 72:9=8 81:9=9**

**Here for total number 11 below:**

**+11 10 9 8 7 6 5 4 3 2**

**1:1=1 0 : 1 =0 9:1=9 8:1=8 7:1=7 6:1=6 5:1=5 4:1=4 3:1=3 2:1=2**

**21:3=7 0:3=3 9:3=3 18:3=6 27:3=9 6:3=2 15:3=5 24:3=8 3:3=1 12:3=4**

**21:7=3 0:7=0 49:7=7 28:7=4 7:7=1 56:7=8 35:7=5 14:7=2 63:7=9 42:7=6**

**81:9=9 0:9=0 9:9=1 18:9=2 27:9=3 36:9=4 45:9=5 54:9=6 63:9=7 72:9=8**

**Here for total number 12 below:**

**+12 11 10 9 8 7 6 5 4 3**

**2:1=2 1:1=1 0 : 1 =0 9:1=9 8:1=8 7:1=7 6:1=6 5:1=5 4:1=4 3:1=3**

**12:3=4 21:3=7 0:3=3 9:3=3 18:3=6 27:3=9 6:3=2 15:3=5 24:3=8 3:3=1**

**42:7=6 21:7=3 0:7=0 49:7=7 28:7=4 7:7=1 56:7=8 35:7=5 14:7=2 63:7=9**

**72:9=8 81:9=9 0:9=0 9:9=1 18:9=2 27:9=3 36:9=4 45:9=5 54:9=6 63:9=7**

**Here for total number 13 below:**

**+13 12 11 10 9 8 7 6 5 4**

**3:1=3 2:1=2 1:1=1 0:1=0 9:1=9 8:1=8 7:1=7 6:1=6 5:1=5 4:1=4**

**3:3=1 12:3=4 21:3=7 0:3=3 9:3=3 18:3=6 27:3=9 6:3=2 15:3=5 24:3=8**

**63:7=9 42:7=6 21:7=3 0:7=0 49:7=7 28:7=4 7:7=1 56:7=8 35:7=5 14:7=2**

**63:9=7 72:9=8 81:9=9 0:9=0 9:9=1 18:9=2 27:9=3 36:9=4 45:9=5 54:9=6**

**Here for total number 14 below:**

**+14 13 12 11 10 9 8 7 6 5**

**4:1=4 3:1=3 2:1=2 1:1=1 0:1 =0 9:1=9 8:1=8 7:1=7 6:1=6 5:1=5**

**24:3=8 3:3=1 12:3=4 21:3=7 0:3=3 9:3=3 18:3=6 27:3=9 6:3=2 15:3=5**

**14:7=2 63:7=9 42:7=6 21:7=3 0:7=0 49:7=7 28:7=4 7:7=1 56:7=8 35:7=5**

**0:9=0 81:9=9 72:9=8 63:9=7 54:9=6 45:9=5 36:9=4 27:9=3 18:9=2 9:9=1**

**Here for total number 15 below:**

**+ 15 14 13 12 11 10 9 8 7 6**

**5:1=5 4:1=4 3:1=3 2:1=2 1:1=1 0:1 =0 9:1=9 8:1=8 7:1=7 6:1=6**

**15:3=5 24:3=8 3:3=1 12:3=4 21:3=7 0:3=3 9:3=3 18:3=6 27:3=9 6:3=2**

**35:7=5 14:7=2 63:7=9 42:7=6 21:7=3 0:7=0 49:7=7 28:7=4 7:7=1 56:7=8**

**45:9=5 54:9=6 63:9=7 72:9=8 81:9=9 0:9=0 9:9=1 18:9=2 27:9=3 36:9=4**

**Here for total number 16 below:**

**+ 16 15 14 13 12 11 10 9 8 7**

**6:1=6 5:1=5 4:1=4 3:1=3 2:1=2 1:1=1 0:1=0 9:1=9 8:1=8 7:1=7**

**6:3=2 15:3=5 24:3=8 3:3=1 12:3=4 21:3=7 0:3=3 9:3=3 18:3=6 27:3=9**

**56:7=8 35:7=5 14:7=2 63:7=9 42:7=6 21:7=3 0:7=0 49:7=7 28:7=4 7:7=1**

**36:9=4 45:9=5 54:9=6 63:9=7 72:9=8 81:9=9 0:9=0 9:9=1 18:9=2 27:9=3**

**Here for total number 17 below:**

**+ 17 16 15 14 13 12 11 10 9 8**

**7:1=7 6:1=6 5:1=5 4:1=4 3:1=3 2:1=2 1:1=1 0:1 =0 9:1=9 8:1=8**

**27:3=9 6:3=2 15:3=5 24:3=8 3:3=1 12:3=4 21:3=7 0:3=3 9:3=3 18:3=6**

**7:7=1 56:7=8 35:7=5 14:7=2 63:7=9 42:7=6 21:7=3 0:7=0 49:7=7 28:7=4**

**27:9=3 36:9=4 45:9=5 54:9=6 63:9=7 72:9=8 81:9=9 0:9=0 9:9=1 18:9=2**

**Here for total number 18 below:**

**+ 18 17 16 15 14 13 12 11 10 9**

**8:1=8 7:1=7 6:1=6 5:1=5 4:1=4 3:1=3 2:1=2 1:1=1 0 :1 =0 9:1=9**

**18:3=6 27:3=9 6:3=2 15:3=5 24:3=8 3:3=1 12:3=4 21:3=7 0:3=3 9:3=3**

**28:7=4 7:7=1 56:7=8 35:7=5 14:7=2 63:7=9 42:7=6 21:7=3 0:7=0 49:7=7**

**18:9=2 27:9=3 36:9=4 45:9=5 54:9=6 63:9=7 72:9=8 81:9=9 0:9=0 9:9=1**

**Here for total number 19 below:**

**+19 18 17 16 15 14 13 12 11 10**

**9:1=9 8:1=8 7:1=7 6:1=6 5:1=5 4:1=4 3:1=3 2:1=2 1:1=1 0:1 =0**

**9:3=3 18:3=6 27:3=9 6:3=2 15:3=5 24:3=8 3:3=1 12:3=4 21:3=7 0:3=3**

**49:7=7 28:7=4 7:7=1 56:7=8 35:7=5 14:7=2 63:7=9 42:7=6 21:7=3 0:7=0**

**9:9=1 18:9=2 27:9=3 36:9=4 45:9=5 54:9=6 63:9=7 72:9=8 81:9=9 0:9=0**

**Observing this previously shown order of digits finally enables the final solution to the problem:**

As indicated at the beginning of the previous slide rule description, for seven essays it was not possible to solve the initial problem, i.e. the question of which constant prime-end factors can be used to solve the task quickly and clearly (because for this solution it is sufficient to produce only one of the two multi-digit factors; in the case of a “1” as the counting factor, the first line is even “unadulterated”, ie its recognizable numerical values ​​are identical to the multi-digit “counted factor” sought. Specifically, no calculation could be made in the 2nd column, not even by means of the successful double number series used here, because precisely for this, as described above, the knowledge of the responsible factors is required.

Observing the above-mentioned slide rule in its perfect order and predictability now makes it clear that only relatively few digits and numbers can be considered as the first two digits (seen from the right)! Two 2-digit factors multiplied together result in a 3 to 4-digit product. It couldn't get any bigger. However, only the first two digits are “to be used” (counting from the right). The 3rd and 4th digits mainly consist of transfers and are only of interest to "connect" to the other digits of the invoice if the large number has more than 3 or 4 digits.

The solution to the aforementioned problem consists in producing the theoretically possible products of the initially 2-digit factors, keeping them in the database and calling them up if necessary. Your first two factor digits are always suitable for “automatically” solving the previously unanswered questions about the factors, their sequence and their transfer, and delivering them in such a way that they can be used for further calculations.

Logically there can only be a maximum of 1,000 results that deliver the first two (2) factors you are looking for:

Because there are exactly 10 possibilities, in which the searched digits x (for the upper number) and y (for the lower number) also each deliver 10 possible possibilities (0 to 9):

**x 1 \* y 1 x 1 \* y 3 x 1 \* y 7 x 1 \* y 9**

**x 3 \* y 3 x 3 \* y 7 x 3 \* y 9**

**x 7 \* y 7 x 7 \* y 9 x 9 \* y 9**

**Nikolaus Graf zu Castell-Castell**

**Dipl. Vw.**

**Prague Research Institute**

**Zug (CH) und Prague (CR)**

**Nikolaus.Castell@mail.com**

**mob. 00420 778 037 633**