Citation:

Vaes, F.J., Factorisation of large numbers. (3rd part), in:
KNAW, Proceedings, 4, 1901-1902, Amsterdam, 1902, pp. 501-508

Mathematics. — *"Factorisation of large numbers."* (3rd part). By F. J. VAES. (Communicated by Prof. P. H. SCHOUTE).

XIII. *Abbreviated method of* § I.

The determination of the differences of squares allows of a very considerable abbreviation.

According to that method we write $G = a_1^2 - b_1$, and to b_1 we add $2a_1 + 1$, $2a_1 + 3$ etc. until a square b^2 is arrived at.

If to reach this p additions are necessary, then

$$b^2 = b_1 + p \times 2a_1 + \underbrace{(1 + 3 + 5 + \ldots\ldots)}_{p \text{ terms}}$$

$$= b_1 + p \times 2a_1 + p^2,$$

$$\text{so } b^2 = p\,(2a_1 + p) + b_1.$$

Example: $G = 513667 = 717^2 - 422$. (See pag. 328).

We test for p successively the values 1, 2, 3, etc. as follows

$$1 \times (1434 + 1) + 422 = 1435 + 422 = 1857$$
$$2 \times (1434 + 2) + 422 \qquad = 3294$$
$$3 \times (1434 + 3) + 422 \qquad = 4733$$
$$4 \times (1434 + 4) + 422 \qquad = 6174$$

etc.,

and we see whether the result is a square. It is immediately evident, that in this way the same numbers are obtained as for the additions on pages 328 and 329, but at the same time that it is not necessary to take all values 1, 2, 3, etc. for p.

For b^2 must terminate in 4 or 9 (pag. 328), so that the product (before 422 is added) can have only 2 or 7 as final figure. So we have but to calculate:

$2 \times (1434 + 2) + 422 =$	$2872 + 422 =$	3294
4×1438	5752	6174
7×1441	10087	10509
9×1443	12987	13409

etc.,

33

where we obtain exactly the sums, found on page 329 by adding 2 or 3 numbers at the same time.

So the operation gives a good insight into the reason of the addition of the numbers in groups of 2 or 3; it admits however still of a simplification if we pay attention to the last *two* figures of the sums.

The terminal figure 4 or 9 of b^2 must be preceded by an *even* figure, so the terminal figure 2 or 7 of the product must likewise be preceded by an *even* figure. If on the place of the tens an *odd* figure appears, we need not continue.

We directly see that this is the case for 2×1436, and 4×1438, but then also for 12×1446, 14×1448, 22×1456, 24×1458, in general for $(2 + 10\,n)\,(1436 + 10\,n)$ and $(4 + 10\,n)\,(1438 + 10\,n)$.

So there remains:

$7 \times 1441 + 422 =$	$10087 + 422 =$	10509
9×1443	12987	13409
17×1451	24667	25089
19×1453	27607	28029
	etc.	

Only the first two multiplications need be executed; after that additions suffice.

For $(7 + 10\,n) \times (1441 + 10\,n) = 7 \times 1441 + 14480\,n + 100\,n^2$, so that we can arrive at 17×1451 by adding $14480 + 100$ or 14580 to 10087; in the same way we find 27×1452 by adding to the obtained result

$$14480 + 300 \text{ or } 14780,$$

etc.; each following number to be added is 200 more than the preceding.

This holds good for the products with factors 9, 19, 29 etc. and the operation becomes

$$\begin{array}{rr|rr} 7 \times 1441 + 422 = & 10509 & 9 \times 1443 + 422 = & 13409 \\ (7 + 1441) \times 10 + 100 = & \underline{14580} & (9 + 1443) \times 10 + 100 = & \underline{14620} \\ & 25089 & & 28029 \\ & \underline{14780} & & \underline{14820} \\ & 39869 & & 42849 = 207^2. \end{array}$$

In both columns the addition must be performed at the same time; the entire number of additions is only 4.

Example $G = 1677803 = 1296^2 - 1813$.

Here b^2 can end only in 1, so $b^2 - 1813$ or $p(2a_1 + p)$ only in 8.

Of 1×2593, 2×2594, etc. we need but take those, whose first factor ends in 2 or 6.

This gives the operation (at the same time in two columns):

$2 \times 2594 + 1813 = 6901$	$6 \times 2598 + 1813 = 17401$
$(2 + 2594) \times 10 + 100 = 26060$	$(6+2598) \times 10 + 100 = 26140$
32961	43541
2626	2634
5922	6988
2646	2654
8568	9642
2666	2674
11234	12316
2686	2694
13920	15010
2706	2714
166261	$177241 = 421^2$

from which ensues $G = 1362^2 - 421^2$

$$= 1783 \times 941.$$

According to the common method of § I

$$1362 - 1296 = 66$$

numbers ought to have been added; now their number is only 12.

The additions of the first column are useless and the question might be put whether this was not discernible beforehand.

This is really the case, if we make use of the table of the 4 last figures of a square (page 332).

For b^2 can terminate only in 1, so a^2 in 04, 24, 44, 64, 84.

According to the table a number terminating in 04 can be square only when the number formed by thousands und hundreds is a 4-fold or a 4-fold — 1. For shortness' sake we shall indicate this by: $\binom{4v}{4v-1}04$. If we subtract this number 7803 formed by the

33*

4 last figures of G, there remains $\binom{4v+2}{4v+1}01$, for the 4 last figures of b^2, because 78 is a 4-fold + 2.

According to the table the terminal figures 01 in a square can be preceded only by a 4-fold, or a 4-fold + 2, so that for b^2 we can only have: $(4v+1)01$ and for a^2: $(4v-1)04$.

If we apply the same to the terminal figures 24, 44, 64, 84 of a^2, we arrive at:

$$\binom{4v}{4v-1}04, \binom{4v+2}{4v-1}24, \binom{4v+1}{4v+2}44, \binom{4v}{4v+1}64, \binom{4v}{4v-1}84$$

to be subtracted 7803

$$\text{remainder } \binom{4v+2}{4v+1}01, \binom{4v}{4v+1}21, \binom{4v-1}{4v}41, \binom{4v+2}{4v-1}61, \binom{4v+2}{4v+1}81,$$

of which are only possible the cases:

$$(4v+2)01,\ (4v+1)21,\ (4v)41,\ (4v-1)61,\ (4v+2)81.$$

Now the first column of the additions begins with 6901, and therefore with a $(4v+1)01$, to which is added 26060, that is $(4v\quad)60$

which gives $(4v+1)61$ and therefore never a square.

To this is added 26260, a $(4v+2)60$, together $(4v)21$, which can neither be a square.

And in succession we shall have:

$$\begin{array}{r} (4v\quad)21 \\ (4v\quad)60 \\ \hline (4v\quad)81 \\ (4v+2)60 \\ \hline (4v-1)41 \\ (4v\quad)60 \\ \hline (4v\quad)01 \\ (4v+2)60 \\ \hline (4v+2)61 \\ (4v\quad)60 \\ \hline (4v-1)21 \\ (4v+2)60 \\ \hline (4v+1)81 \\ (4v\quad)60 \\ \hline (4v+2)41 \\ (4v+2)60 \\ \hline (4v+1)01 \end{array}$$

etc.,

from which is evident, that a square can never be obtained.

So it is only necessary to calculate the second column, which however still admits of a simplification.

For 17401 is a $(4v+2)01$, and 26140 a $(4v+1)40$, so that we obtain in succession:

$$\begin{array}{l}
(4v+2)\,01 \\
(4v+1)\,40 \\ \hline
(4v-1)\,41 \\
(4v-1)\,40 \\ \hline
(4v+2)\,81\ * \\
(4v+1)\,40 \\ \hline
(4v\quad\ \ )\,21 \\
(4v-1)\,40 \\ \hline
(4v-1)\,61\ * \\
(4v+1)\,40 \\ \hline
(4v+1)\,01 \\
(4v-1)\,40 \\ \hline
(4v\quad\ \ )\,41\ * \\
(4v+1)\,40 \\ \hline
(4v+1)\,81 \\
(4v-1)\,40 \\ \hline
(4v+1)\,21\ * \\
(4v+1)\,41 \\ \hline
(4v+2)\,61 \\
(4v-1)\,40 \\ \hline
(4v+2)\,01.\ *
\end{array}$$

Only the numbers marked with an asterisk can be squares and the operation can become:

$$\begin{array}{r}
6 \times 2598 + 1813 = 17401 \\
26140 + 26340 = 52480 \\ \hline
69881 \\
53280 \\ \hline
123161 \\
54080 \\ \hline
177241 = 421^2
\end{array}$$

with only *three* additions.

Example: $G = 33379631 = 5778^2 - 5653$.

Now a^2 can terminate only in 00 or 56, b^2 in 69 or 25, and $p(2a_1 + p)$ in 56 or 92.

The terminal figure of p can be only 2, 6 or 8 and we have

$$\begin{array}{r|r}
2 \times 11558 + 5653 = 28769 & 6 \times 11562 + 5653 = 75025 \\
(2 + 11558) \times 10 + 100 = 115700 & (6 + 12562) \times 10 + 100 = 115780 \\
\overline{144469} &
\end{array}$$

$$\begin{array}{r}
8 \times 11564 + 5653 = 98165 \\
(8 + 11564) \times 10 + 100 = 115820 \\
116020 \\
116220 \\ \hline
446225
\end{array}$$

The sums of the second and third columns must always have 25 as terminal figures, so that we shall be able to add 5 numbers at a time.

So we must add to the second column:

5×116180, 5×117180, 5×118180, etc.,

or 580900, 585900, 590900, that is a $\binom{4v+1}{4v-1}$ 00, and as 75025 is a $(4v+2)\,25$, we shall have:

$$\begin{array}{l} (4v+2)\,25 \\ \underline{(4v+1)\,00} \\ (4v-1)\,25 \\ \underline{(4v-1)\,00} \\ (4v+2)\,25. \end{array}$$

According to the table 25 can be preceded only by a 4-fold or a 4-fold + 2; consequently the second column can produce a square only after addition of successively 10 numbers.

To the third column we shall have to add successively:

5×116820, 5×117820, 5×118820, etc.,

or 584100, 589100, 594100, that is a $\binom{4v+1}{4v-1}\,00$,

and as 446225 is a $(4v+2)\,25$, also this column can produce a square only after addition of every time 10 numbers.

As 28769 of the first column is a $(4v-1)\,69$ and 115700 a $(4v+1)\,00$, we shall have successively

$$\begin{array}{l} (4v-1)\,69 \\ \underline{(4v+1)\,00} \\ (4v\quad)\,69 \\ \underline{(4v-1)\,00} \\ (4v-1)\,69, \end{array}$$

from which in connection with the table is evident, that only the 2nd, 4th, 6th etc. additions can produce squares, so that the operation becomes:

$$2 \times 11558 + 5653 = 28769$$

$$(2 + 11558) \times 10 + 100 = \left.\begin{array}{r}115700 \\ 115900\end{array}\right\} 231600$$

$$\begin{array}{r} \hline 260369 \\ 2324 \\ \hline 4927 \\ 2332 \\ \hline 7259 \\ 2340 \\ \hline 9599 \\ 2348 \\ \hline 11947 \\ 2356 \\ \hline 14303 \\ 2364 \\ \hline 16667 \\ \text{etc.} \end{array}$$

The numbers 2316, 2324, etc. ascend with 4. Another small abbreviation can be brought about by remarking that b^2 must be a $(4v-1)\,69$, so $a^2\,(=b^2+G)$ a $(4v)\,00$, so that a^2 can terminate only in .400 or .600, and by this b^2 only in .769 or .969. So we could have added the numbers 2316 and 2324 at once, the numbers 2356 and 2364 likewise, etc. Of every 4 additions one is dropped.

After adding 44 numbers, so after about 36 additions, we find

$$b^2 = 10975969 = 3313^2,$$

so that

$$G = 6660^2 - 3313^2 = 9973 \times 3347.$$

The second and third columns were not continued for a reason to be mentioned in the following §.

According to the common method of § I 6669 — 5778 or 882 numbers would have to be added, which can be taken in groups, but which would require a considerably larger number than 36 additions.

Also the method of § VII would require a greater number of operations.

A table showing the 6 or 8 last figures which may appear in a square, would undoubtedly lead to further abbreviations.

§ XIV. *Property of a^2 and b^2.*

If for shortness' sake we call $\left(\frac{G+1}{2}\right)^2$ and $\left(\frac{G-1}{2}\right)^2$ c^2 and d^2, then $G=c^2-d^2$. If moreover $G=a^2-b^2$, we have $a^2-b^2=c^2-d^2$.

Now b^2 and d^2 can never have the two terminal figures alike; neither can a^2 and c^2.

To show this we consider the table, giving the four last figures, which can appear in a square; immediately the following theorem strikes us: *in a column under an even number and in a column under an odd number, there is always one of the two* ××, *but never more than one at the same height.*

Or: *In the columns under an even number the two* ×× *are placed immediately under each other, in the other columns there is every time a space of a line.* We must moreover fancy that under the fourth line of the table the two first lines have been repeated.

The consequence is evident from an example:

On pag. 504 a number a^2 of the form $\binom{4v}{4v-1}\,04$ is given, from which 7803, a $(4v+2)\,03$ is subtracted.

The remainder was $\binom{4v+2}{4v+1}$ 01; by the subtraction we arrive from the lines of the 4-folds and the 4-folds — 1 on two lower lines, namely those on which for instance the $\times\times$ of column 44 are to be found.

As b^2 is odd, only one of those two $\times\times$ can be used, namely on the line of the 4-folds+2. Consequently b^2 can be but a $(4v+2)\,01$, and therefore a^2 only a $(4v)\,04$.

The same consideration holds good for c^2 and d^2.

If now b^2 and d^2 were to have the same two terminal figures, then also d^2 must be a $(4v+2)\,01$, and c^2 $(4v)\,04$.

Now $c^2-a^2=d^2-b^2$; and the second member will be a $(4v+2)\,00$, the first a $(4v)\,00$.

So d^2 and b^2 can never have the terminal figures alike.

In the last example in § XIII d must end in 5, so d^2 in 25; so the second and third columns will lead to $\left(\frac{G-1}{2}\right)^2$.

Apparently there is an exception to the property mentioned here, namely in the case, that the number formed by thousands and hundreds of G are just a $\begin{matrix}\text{4-fold}\\ \text{4-fold}-1\end{matrix}$ and the two terminal figures form a number $\begin{matrix}\text{smaller}\\ \text{greater}\end{matrix}$ than the number formed by the two terminal figures of a^2.

For if in the example under consideration (page 505).

$$G = \ldots . 76\,03$$

we should have:

	a^2 $\binom{4v}{4v+3}04$	of which is possible only:
		for b^2 (and so also for d^2) $(4v)\,01$
to be subtracted	76 03	„ a^2 („ „ „ „ c^2) $(4v)\,04$.
remainder	$\binom{4v}{4v+3}01,$	Then $d^2-b^2=(4v)\,00$
		and $c^2-a^2=(4v)\,00$

Evidently the 4-folds preceding the terminal noughts must however be the same for both remainders, so that G would have to be 0003. But then we shall make use of the same consideration as above for the number formed by the 5th and 6th figure of G (reckoned from the right side).

(March 20, 1902).