$$\frac{3}{(p_B-p_A)^3}\,\frac{d^2p}{dx'^2}=\frac{dp}{dx'}\,\frac{2\,(2\,p-p_A-p_B)}{(p-p_A)^3\,(p_B-p)^3}\times$$

$$\times\,[(p_B+p_A-2\,p)^2+(p-p_A)\,(p_B-p)]$$

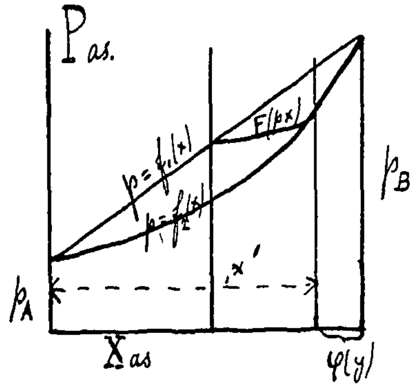


Fig. 3.

so that the locus is everywhere convex in the heterogeneous region with an inflection-point at the beginning, and we get a curve as drawn in fig. 3, which clearly indicates the different possibilities for the empiric isothermal. The point where the locus cuts the curve $p=f(x_2)$ is of course determined by the formula for ${}_1x'$.

Mathematics. — "*Factorisation of large numbers*", by Mr. F. J. Vaes, Mechanical Ingeneer at Rotterdam. (Communicated by Prof. P. H. Schoute).

Introduction.

The history of the research about the divisibility of large numbers is very simple.

Eratosthenes (275—194 b. C.) is said to have invented the method of the sieve (determination of the prime numbers under a given limit by removing from the series of odd numbers those divisible by 3, 5, 7, etc.).

In 1643 Fermat decomposed a number proposed to him by Mersenne. In a letter dated "Toulouse le 7 Avril 1643" we find: "Vous me demandez si le nombre 100895598169 est premier ou "non, et une méthode pour découvrir, dans l'espace d'un jour, s'il "est premier ou composé. A cette question, je réponds que le "nombre est composé et se fait du produit de ces deux: 898423 et "112303, qui sont premiers."

The method of Fermat has never been published [1]).

[1]) In 1640 Fermat believed $2^{2^n}+1$ gives prime numbers for all values of n. Afterwards Euler found that $2^{2^5}+1$ (a number of ten figures) is the product of 641 and 6700417. The author is inclined to ask: If in 1643 Fermat really could factorise

In the preceding century the theory of numbers was built up by Gauss, Legendre, Lejeune-Dirichlet, Riemann, Tschebicheff and others who obtained very important results. But the value of these results with reference to the factorisation of large numbers can be derived sufficiently from the following two citations: ... "dans "l'état actuel de la théorie des nombres on ne connaît aucun procédé "direct pour la recherche des diviseurs des nombres ayant plus de "dix chiffres dans le système décimal" (Edouard Lucas, *Théorie des Nombres*, Tome premier, p. 333) and "Les méthodes de Gauss "seraient impuissantes à résoudre le problème proposé par Mersenne à Fermat" (Edouard Lucas, *Récréations Mathématiques*, Tome II, p. 231).

Any number N can be factorised, if it can be thrown into the form $a^2 - b^2$, under the condition $a > b + 1$. For then we have $N = (a + b)(a - b)$, which proves that the decomposition can be performed by seeking a square b^2 that, added to N, furnishes a new square a^2. This simple property is also mentioned by Fermat, but apparently not made use of to factorise large numbers either by him or by another.

By means of a table of squares the factorisation of any number N can be performed.

However it is more convenient to determine the square root of N and to increase the last figure of this root by unity.

Example $N = 1073$.

$\sqrt{10 \mid 73} = 33$, so $1073 = 33^2 - 16 = 33^2 - 4^2 = 37 \times 29$.

$3^2 = \underline{9}$

$\overline{173}$

$63.3 = \underline{189}$

-16

As a rule the required result will not be obtained so soon; rather we shall find in general $N = a_1{}^2 - b_1$.

By adding n to a_1 we find

$$N = (a_1 + n)^2 - (b_1 + 2a_1 n + n^2);$$

so we can reach our aim by choosing n in such a manner that $b_1 + 2a_1 n + n^2$ is a square.

a number of twelve figures, wherefore did he not apply his method to this number of ten figures? May we not conclude from this that Fermat was in possession of a special method for special numbers, and that he had dictated to Mersenne a condition to which the proposed number had to satisfy? The correspondence between F. and M. may enlighten this point. In that case also could be decided if any of the methods given here be related to the method of Fermat.

The easiest way to obtain such an n consists in increasing a_1 several times by unity and continuing this operation

$$\begin{aligned} N &= a_1^2 - b_1 \\ &= (a_1+1)^2 - (b_1 + 2a_1 + 1) \text{ or } = a_2^2 - b_2, \\ &= (a_2+1)^2 - (b_2 + 2a_2 + 1) \text{ or } = a_3^2 - b_3, \text{ etc.} \end{aligned}$$

until the number b in the last line has become a square.

Example $N = 57$.

$$\begin{aligned} \text{We write } N &= 8^2 - 7 \\ &= 9^2 - (7 + 2 \times 8 + 1) = 9^2 - 24 \\ &= 10^2 - (24 + 2 \times 9 + 1) = 10^2 - 43 \\ &= 11^2 - (43 + 2 \times 10 + 1) = 11^2 - 64 \\ &= 11^2 - 8^2 = (11 + 8)(11 - 8) = 19 \times 3. \end{aligned}$$

For shortness' sake we make use of the algorithm

$$\begin{array}{rr} 57 = 8^2 - & 7 \\ 2 \times 8 + 1 = & 17 \\ \cline{2-2} & 24 \\ & 19 \\ \cline{2-2} & 43 \\ & 21 \\ \cline{2-2} & 64 = 8^2, \end{array}$$

so $57 = (8 + \text{number of additions})^2 - 8^2$, where only the first additional number 17 has to be calculated.

An important abbreviation can be obtained by paying attention to the terminal figures, as is shown by the following example. Here the reckoning was to be:

$$\begin{array}{lr} N = 513667. & \\ N = 717^2 \quad - & 422 \\ 2 \times 717 + 1 = & 1435 \\ \cline{2-2} & 1857 \\ & 1437 \\ \cline{2-2} & 3294 \\ \quad \text{etc.} & \end{array}$$

However as a^2 can terminate in 0, 1, 4, 5, 6 or 9 only and the last figure of N is 7, a^2-N can terminate in 3, 4, 7, 8, 9 or 2 only. But a^2-N being also a square (b^2), it can only terminate in 4 of 9. So it is unnecessary to perform all the additions and the abbreviated algorithm comes to this:

$$\begin{array}{rr}
N = 717^2 & -\quad 422 \\
2 \times 717 + 1 = & 1435 \\
 & 37 \\
\hline
 & 3294 \\
 & 1439 \\
 & 41 \\
\hline
 & 6174 \\
 & 1443 \\
 & 5 \\
 & 7 \\
\hline
 & 10509 \\
 & 1449 \\
 & 51 \\
\hline
 & 13409 \\
 & 1453 \\
 & 5 \\
 & 7 \\
\hline
 & 17774 \\
 & 1459 \\
 & 61 \\
\hline
 & 20694 \\
 & 1463 \\
 & 5 \\
 & 7 \\
\hline
 & 25089 \\
 & 1469 \\
 & 71 \\
\hline
 & 28029 \\
 & 1473 \\
 & 5 \\
 & 7 \\
\hline
 & 32454 \\
 & 1479 \\
 & 81 \\
\hline
 & 35414 \\
 & 1483 \\
 & 5 \\
 & 7 \\
\hline
 & 39869 \\
 & 1489 \\
 & 91 \\
\hline
 & 42849 = 207^2 = b^2
\end{array}$$

As soon as $b^2 = 207^2$ has been found, the value of a^2 can be calculated in different manners. In the first place by adding N to the result 42849 we find

$$a^2 = 556516 = 746^2.$$

Secondly one can remark, that from 1435 unto 1491 (the first and last of the added numbers) a number of

$$\frac{1491-1435}{2} + 1, \text{ i.e. } 29$$

odd numbers have been added; this gives

$$a = 717 + 29 = 746.$$

Thirdly — and this method is the shortest — one can observe that by continuing the operation the number 1493 had to be added and that this number is equal to $2a + 1$; so

$$a = \frac{1493-1}{2} \text{ or }$$

$$\frac{1491+1}{2} = 746.$$

So we have

$$N = 746^2 - 207^2 = 953 \times 539.$$

After two additions the factor 539 appears to be equal to 30^2—19^2, i.e. equal to 49×11. On the other hand the factor 953 gives $477^2 - 476^2$, i.e. 953×1 and appears to be a prime number.

The last operation is rather long, a number of 446 numbers having to be added; as for larger numbers the number of additions nearly increases proportionally it is peremptorily necessary to seek for a shorter method.

Such an abbreviation can be derived from the consideration of last *two* figures of the number to be factorised.

For a square must terminate in one of the following pairs of figures: 00; 01, 21, 41, 61, 81; 04, 24, 44, 64, 84; 25; 16, 36, 56, 76, 96; 09, 29, 49, 69, 89.

The last pair of figures of the number N being 53 we have to determine out of the given pairs those pairs which, by addition of 53, furnish another pair.

So one sees immediately that b^2 only can terminate in one of the pairs 16, 36, 56, 76, 96, in which cases a^2 terminates in 69, 89, 09, 29, 49 respectively.

So we can shorten our algorithm to:

$$\begin{array}{rr}
953 = 31^2 & -\;\;8 \\
2 \times 31 + 1 = & 63 \\
 & 65 \\
\hline
 & 136 \\
 & 67 \\
 & 69 \\
 & 71 \\
 & 73 \\
\hline
 & 416 \\
 & 75 \\
 & 77 \\
 & 79 \\
 & 81 \\
 & 83 \\
 & 85 \\
\hline
 & 896 \\
\text{etc.} &
\end{array}$$

Now, as is immediately evident $67 + 69 + 71 + 73 = 4 \times 70$, and $75 + 77 + 79 + 81 + 83 + 85 = 6 \times 80$; as similar groups present themselves over and over, we can shorten still more as follows:

$$
\begin{array}{lrr}
 & 953 = 31^2 \quad - & 8 \\
 & 2 \times 31 + 1 = & 63 \\
 & & \underline{65} \\
a^2 = 33^2 & & 136 \\
 & 4 \times 70 \quad = & \underline{280} \\
37^2 & & 416 \\
 & 6 \times 80 \quad = & \underline{480} \\
43^2 & & 896 \\
 & 4 \times 90 \quad = & \underline{360} \\
47^2 & & 1256 \\
 & 6 \times 100 \quad = & \underline{600} \\
53^2 & & 1856 \\
 & \text{etc.} &
\end{array}
$$

The importance of this last abbreviation is self-evident.

The numbers obtained by addition must be looked for in a table of squares. For shortness' sake one can make use of the following table (see next page) representing all the possible groups of four figures, in which a square can end[1]).

For if this table shows that the four terminal figures of a number cannot occur in a square, it is unnecessary to use the table of squares.

II. *Classification of the row of natural numbers according to their divisibility.*

By diminishing any square, e.g. 13^2 by the squares 1^2, 2^2, 3^2, etc. we obtain the composed numbers 168, 165, 160, 153, etc. or if we pay attention to the odd numbers only: 165, 153, 133, 105, 69, 25.

It is immediately evident that in the factorisation of any of these numbers 13^2 *may*, but not that 13^2 necessarily *must* present itself as a^2.

For shortness' sake we will say that 13^2 *dominates* these numbers. So a number admitting of more than two factors is dominated by more than one square, e.g. 273 by 137^2, 47^2, 23^2, 17^2.

In following the method developed in § I one always finds the *least* dominating square.

[1]) In his "Théorie des Nombres" LUCAS states that PRESTET has published a table for the same purpose in his "Nouveaux Eléments de Mathématiques, 1689. It has been impossible for us to make out if this table was constructed in an analogous manner.

TABLE

CONTAINING ALL THE GROUPS OF FOUR FIGURES IN WHICH A SQUARE CAN END.

NUMBER FORMED BY THE HUNDREDS AND THOUSANDS.																									NUMBER FORMED BY THE UNITIES AND TENS																			
																									01	21	41	61	81	04	24	44	64	84	16	36	56	76	96	09	29	49	69	89
00	04	08	**12**	**16**	**20**	24	28	**32**	**36**	**40**	44	48	**52**	**56**	**60**	64	68	**72**	**76**	**80**	84	88	**92**	**96**	×		×		×	×			×	×	×	×			×	×		×		×
01	05	09	13	17	21	25	29	33	37	41	45	49	53	57	61	65	69	73	77	81	85	89	93	97		×		×				×	×		×			×	×		×		×	
02	**06**	**10**	14	18	**22**	**26**	**30**	34	38	**42**	**46**	**50**	54	58	**62**	**66**	**70**	74	78	**82**	**86**	**90**	94	98	×		×		×		×	×					×	×		×		×		×
03	07	11	15	19	23	27	31	35	39	43	47	51	55	59	63	67	71	75	79	83	87	91	95	99		×		×		×	×			×		×	×				×		×	

The numbers printed in fat type can terminate in 25.

Example: A square may terminate in 4164; for the intersection of the row of 41 with the column of 64 is marked by a cross (×). A square cannot terminate in 4156; for the intersection of the row of 41 with the column of 56 has not been marked.

In the following table are indicated under each square the numbers dominated by it:

TABLE I.

1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2	9^2	10^2	11^2	12^2 etc.
1	4	9	16	25	36	49	64	81	100	121	144
	3	8	15	24	35	48	63	80	99	120	143
		5	12	21	32	45	60	77	96	117	140
			7	16	27	40	55	72	91	112	135
				9	20	33	48	65	84	105	128
					11	24	39	56	75	96	119
						13	28	45	64	85	108
							15	32	51	72	95
								17	36	57	78
									19	40	63
										21	44
											23

The classification of the numbers in this table is very remarkable:

1°. In the columns as well as in the rows the successive differences are 1, 3, 5, 7, etc.

2°. Parallel to the odd numbers in the hypothenusa of the triangle we find the fourfolds 4, 8 12, 16 etc.

3°. Ascending from one of the odd numbers of the hypothenusa in a direction perpendicular to it one finds 3, 5, 7, etc. times this number, e. g. starting from 9 one finds 27, 45, 63, 81.

Now descending from 81 in the direction of the hypothenusa we find the continuation 11, 13, 15 etc. times 9 or 99, 117, 135, etc.

So all the odd multiples of 9 are to be found in two lines passing through 81 and inclined under 45°.

4°. Ascending from one of the fourfolds, e. g. 16, in a direction perpendicular to the hypothenusa we find 2×16, 3×16, $4 \times 16 = 8^2$ and from this point parallel to the hypothenusa 5×16, 6×16, etc. The proof of all these properties is easily given.

From the remark sub 3^0 ensues that the number 7×11 will be found in the line passing through 7^2 parallel to the hypothenusa and also in the line passing through 11^2 perpendicular to it.

So the factors of a number prove to be the roots of the squares that can be reached by proceeding from this number in the two directions inclined under 45°.

The prime numbers present themselves only once (in the hypothenusa), the composed odd numbers present themselves still one time or several times more.

As it is not very convenient to make out if a given number is contained in the table, if this table is continued much farther than here, the classification of Table II recommends itself more. Here equal numbers are placed in the same row, the head of each column bearing the dominating square. The prime numbers appear only in the inclined line at the right side; their rows are denoted by horizontal lines.

Beneath any square a^2 are arranged the numbers a^2-1, a^2-4, a^2-9, etc. with the differences 1, 3, 5, 7, etc. The last number of each column is always *zero*, the last but one $a^2-(a-1)^2=2a-1$, and this number appears always in the inclined line at the right side.

If we assume any number of this line, e.g. 19, then we find above it: $19+17=36$, $19+17+15=51$, $19+17+15+13=64$, $64+11=75$, $75+9=84$, $84+7=91$, $91+5=96$, $96+3=99$, $99+1=100$.

Now 19 can be called the *base* of the numbers 36, 51, 64 etc. Above the base $2a-1$ we then find:

$$(2a-1)+(2a-3)=4(a-1),\ (2a-1)+(2a-3)+(2a-5)=3(2a-3),$$

$$3(2a-3)+(2a-7)=8(a-2),\ 8(a-2)+(2a-9)=5(2a-5),$$

$$5(2a-5)+(2a-11)=12(a-3),\ 12(a-3)+(2a-13)=7(2a-7),\ \text{etc.}$$

Therefore the 3-folds, 5-folds, etc. of the odd numbers are situated on oblique lines passing through the numbers 3, 5, 7, etc., whilst the 4-folds, 8-folds, etc. are situated on intermediate oblique lines commencing at 4, 8, 12, etc.

Twofolds of prime numbers do not present themselves.

For immediate application this table has the inconvenience, that it cannot be continued far enough without becoming unmanageable.

However it leads to an important abbreviation of the method given in § I by means of the simple remark that between the oblique lines no numbers can present themselves. For illustration a small number is chosen; the application to a large number will be evident.

Example $N=83=10^2-17$.

To 17 we must successively add $2\times 10+1=21, 23, 25$, etc.

until a square is obtained. As 83 is a primenumber, one will be forced to continue until 83 has been added; so the number of additions amounts to $\frac{83-21}{2}+1=32$. Now if in Table II we proceed horizontally from the base 83, this number is not found in the oblique line $4(a-1)$; so we can pass to the line $3(2a-3)$. This means however that it is not necessary to continue the additional operations until $\left(\frac{83+1}{2}\right)^2=42^2$, but only until $\left(\frac{31+1}{2}\right)^2=16^2$, the base of which is 31, as this number is the base of the larger one of the two numbers 81 and 87 between which 83 is situated.

If it is found that 83 is not a threefold, we can pass from the line $3(2a-3)$ over the lines $8(a-2)$, $5(2a-5)$ and $12(a-3)$, to the line $7(2a-7)$. So the operation can be stopped at $\left(\frac{19+1}{2}\right)^2=10^2$.

In the case of the number $N=112303$ (see the introduction) one would have to perform nearly 398 additions, (if the numbers to be added were combined in groups of 4 and 6). If however division proves that none of the numbers 3, 7, 11, 13, 17, 19, 23 is a factor, only 211 additions are necessary.

III. *Determination of non-divisors.*

If we put $N=ab+c$, any codivisor of a and c or of b and c will be divisor of N, whilst a divisor of c relative prime to a and b cannot be a divisor of N.

Example $N=73489207$[1].

We put $N=8573^2-7122$

$$\text{or} = 8573^2-1^2-7121 = 8574\times8572-7121$$
$$=2\times3\times1429\times4\times2143-7121;$$

this proves that 3, 1429, 2143 and 7121 are non-divisors of N.

[1] This number was not obtained by multiplication of smaller numbeıs but chosen arbitrarily. Likewise all the other numbers of five and more figures decomposed in this study were chosen at random, the number mentioned in the introduction excepted.

If on the other hand we put

$$N = 8573^2 - 2^2 - 7118 \quad = 8575 \times 8573 - 7118$$

$$= 5^2 \times 7^3 \times 8573 - 2 \times 3559,$$

$$N = 8573^2 - 3^2 - 7113 \quad = 8576 \times 8570 - 7113$$

$$= 2^7 \times 67 \times 10 \times 857 - 3 \times 2371,$$

$$N = 8577 \times 8569 - 7106 \quad = 9 \times 953 \times 11 \times 19 \times 41 - 2 \times 11 \times 17 \times 19,$$

then N appears to be divisible by 11 and 19, but not by 8573, 3559, 67, 857, 2371, 953, 41, 17.

The series 7121, 7118, 7113, 7106, etc. of the numbers c shows the differences 3, 5, 7, etc. if a is increased and b diminished by unity.

The division having been achieved, we find as quotient $N_1 = 351623 = 593^2 - 26$, with 13 (factor of 26) as non-divisor.

By means of 14 operations already 23 of the 106 prime numbers minor to $\sqrt{N}$ can be declared to be non-divisors; by testing 47 and 61 by direct division all divisors minor to 71 are shut out.

If we put $N = \left(\frac{N+1}{2}\right)^2 - \left(\frac{N-1}{2}\right)^2$, at least one of the two successive numbers $\frac{N+1}{2}$ and $\frac{N-1}{2}$ is divisible by 2 or 3 or 2 × 3. The divisors of the quotient so obtained are non-divisors of N.

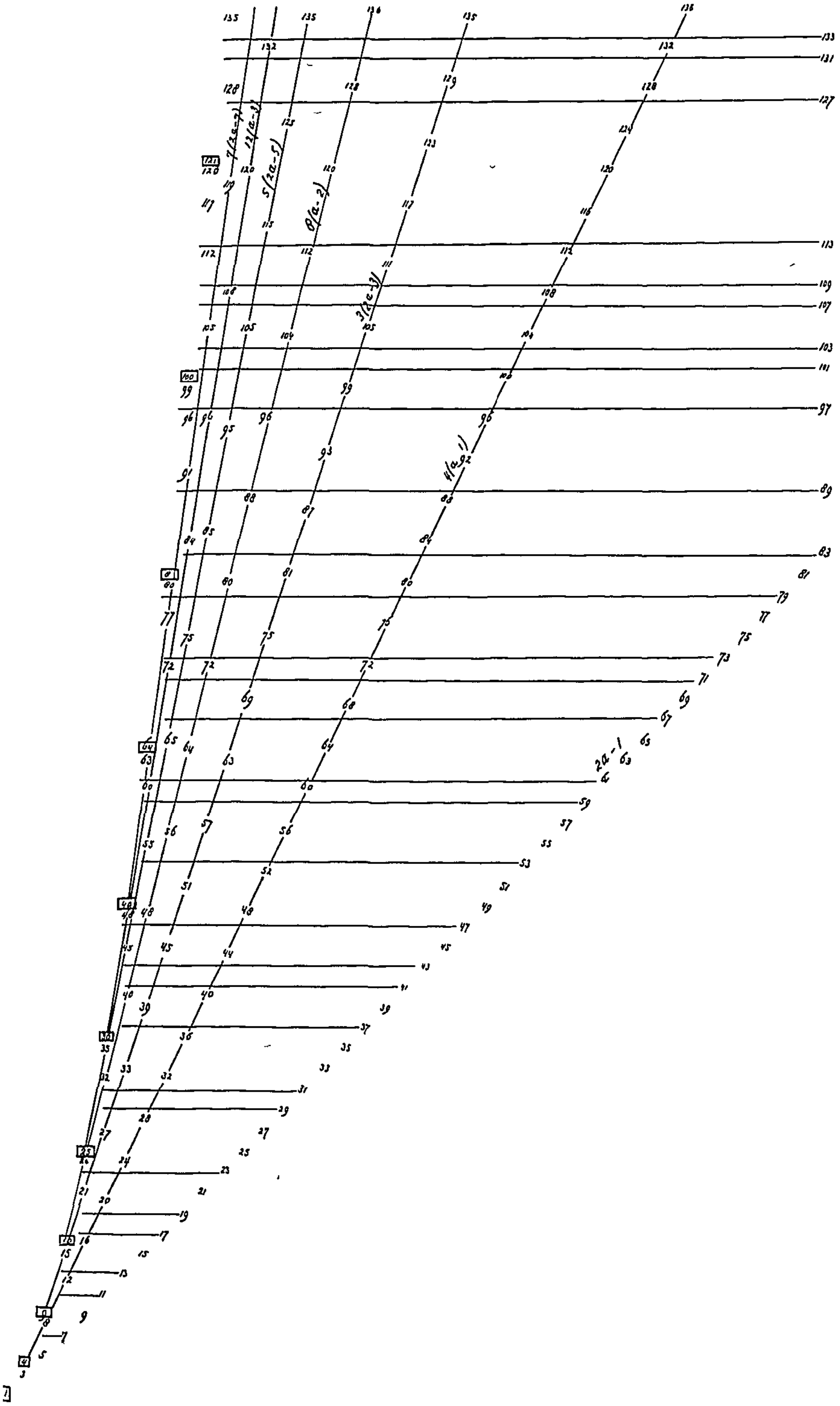
IV. *Determination of the difference of the factors.*

We put $a = b + m$ and therefore $N = (b + m)^2 - b^2 = m(m + 2b)$. Now we try to determine b and m by assuming for m a value near to $\sqrt{N}$, calculating $N^2 - m^2$ and then $2b = \frac{N^2 - m^2}{m}$. If this quotient be not an entire number we repeat this calculation with an m smaller by two (m being odd with N).

(To be continued.)

F. J. VAES. „Factorisation of large numbers."

Table II.


7(2a-7)
12(a-9)
5(2a-5)
8(a-2)
3(2a-3)
4(a-1)
2a-1
121
100
81
64
49
36
25
16
9
4
133
131
127
113
109
107
103
101
97
89
83
81
79
77
75
73
71
69
67
65
63
61
59
57
55
53
51
49
47
45
43
41
39
37
35
33
31
29
27
25
23
21
19
17
15
13
11
9
7
5
3