Technical Sciences, 2022, 25, 35–57

Yearbook peer-reviewed scientific journal
ISSN 1505-4675
e-ISSN 2083-4527
TECHNICAL SCIENCES
Homepage: https://czasopisma.uwm.edu.pl/index.php/ts/

DOI: https://doi.org/10.31648/ts.7278

ABOUT SPECIAL PROPERTIES OF THE HIDDEN STRUCTURE OF TRIANGULAR NUMBERS FOR IMMEDIATE FACTORIZATION

Artur Samojluk

ORCID: 0000-0001-5822-2210
Chair of Mathematics and Computer Science
University of Warmia and Mazury in Olsztyn

Received 9 December 2021, accepted 03 March 2022, available online 28 March 2022.

Keywords: factorization algorithm, RSA, cryptography, numerical experiments, triangular numbers, number theory.

Abstract

The factorization problem belongs to a group of problems important in the security of information systems and cryptography. The article describes a new number factorization algorithm designed based on numerical experiments. We present an extension of number factorization using triangular numbers features. The described algorithm can be used to increase the security of key generation for the RSA algorithm.

Introduction

Cyber security is a problem in the modern world (KALISKI 2006, COMMAND 2012, *RSA CyberCrime Intelligence Service* 2013). The increase in the number of Internet users means more opportunities for cyber criminals. Some of the most dangerous attacks are money thefts (SCHATZ et al. 2017). Cyber criminals

Correspondence: Artur Samojluk, Katedra Metod Matematycznych Informatyki, Wydział Matematyki i Informatyki, Słoneczna 54, 10-710 Olsztyn, e-mail: artur.samojluk@uwm.edu.pl.

find new vulnerabilities in security systems to gain access to areas that should be safe (STEVENS 2018, YOST 2015). Such an area is considered to be where asymmetric security is used, i.e. RSA encryption. RSA keys use pseudoprime number *N*, which consists of two prime numbers *P* and *Q*. RSA security uses a mathematical factorization problem where finding a factorization for a number large *N* is too computationally complex to break the security in a reasonable amount of time. "The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic" (GAUSS 1966).

The search for new solutions requires new tools and approaches to data analysis. Current computational capabilities of computers allow for multi-dimensional analysis of data.

Massive Data analysis open the way to new observations on data, broader calculations and drawing precise conclusions from performed numerical experiments (BREUR 1996, SEGARAN, HAMMERBACHER 2009) The use of data mining allowed for a new research perspective to be explored and conclusions to be drawn (HASTIE et al. 2009, FAYYAD et al. 1996).

Algorithms using factorization problem i.e., RSA (Rivest-Shamir-Adleman), are currently one of the most widely used tools for information encryption. The method based on public and private key is used in civil and military cryptography.

Closely related problem is the distribution of prime numbers in the set of natural numbers (ADLEMAN 2005). The sharpest estimates of the distribution are obtained using properties of the so-called by Riemann zeta function, defined by (ADLEMAN et al. 1983, NIVEN et al. 1991):

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \mathrm{Re}(s) > 1.$$

If the famous Riemann hypothesis (RIEMANN 1859, MOREE et al. 2018) is true, then many number theory problems can be solved and the theoretical complexity of the related algorithms can be improved.

The central object of the paper is the so-called triangle numbers T_n:

$$T_n = 1 + 2 + 3 + 4 + \cdots + n$$

obtained by truncating the above ζ series for $s = -1$. These numbers were studied by Diophantus of Alexandria (c. 150 AD), see also more recent book by Wacław Sierpiński (SIERPIŃSKI 1962). Remark that in certain, well-defined sense, the following limit is true:

$$\lim_{n\to\infty} T_n " = " \zeta(-1) = -\frac{1}{12} \tag{1}$$

The zero places of the function ζ in the real part less than 1, can be determined using a recursive formula:

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s) \tag{2}$$

where:

Γ – Euler's Gamma function.

Remark 1. As can be shown using eq. (2) the value of $\zeta(2) = \frac{\pi^2}{6}$ above that $\zeta(-1) = -\frac{1}{12} \approx 0.0833333$. This makes sense of the formula (1).

Note that for the values $s = -2, -4, -6...$ element $\sin\left(\frac{\pi s}{2}\right) = 0$ hence these places are called places of trivial zero.

Another interesting relation between the Riemann ζ function (SIERPINSKI 1988) and factorization problem is the formula:

$$\zeta(s) \cdot \zeta(s) = \sum \frac{d(n)}{n^s} \tag{3}$$

where:

$d(n)$ – the number of divisors of n.

The purpose of the work. Based on numerical experiments and our observations of an array of natural numbers arranged in a triangle, we propose a factorization algorithm. For this purpose, an analytical system has been designed that allows the analysis of complex number structures and the identification of new number structures with special properties (SAMOJLUK 2019). Let us move on to briefly discuss the content of the following sections.

In section *Solution approach and methodology*, the main driver of the methodology and approach to the problem is presented. Then, in section *Basic properties of triangular numbers* important mathematical elements about triangular numbers and their properties are discussed. The section *Observations of numbers* presents insights related to extended structures of triangular numbers. In section *The extended matrix* properties of extended triangular number structures are defined. Then, in section *Study of numerical structures* we deepen the analysis of extended structures and their properties. Section *Algorithm of geometric factorization* shows the practical application of the new properties in the form of a factorization algorithm, and the last substantive section 8 describes the main conclusions of the paper. Now we come to the section where we set out the basics of our system.

Solution approach and methodology

Let us move on to discuss our novel solution of using triangular numbers for factorization. This approach is new and does not appear in the already known algorithms such as those found in the works (LEHMAN 1974, COHEN 1993, BACH, SHALLIT 1996, DIXON 1981, POLLARD 1975, ADLEMAN 1991, WILLIAMS 1982).

For ease of analysis, numbers with special properties were colour-coded. Then, in a series of numerical experiments on the data, properties of objects (patterns) were identified.

Extracting strings with unique features. In the experiments conducted, matrices of size $5 \cdot 10^3$ columns by $5 \cdot 10^3$ rows were analyzed. The total number of analyzed records (information) was $2.5 \cdot 10^7$. Next, the analysis was performed on the base matrix $K = 0$, where the following lines were analyzed: diagonal (DL and DR), horizontal (H) and vertical (V). Different configurations (F) were used to generate strings and arithmetic ”jumps” on the analyzed K matrices (see Fig. 1). Over 10^6 different configurations of arithmetic strings were tested for each K.

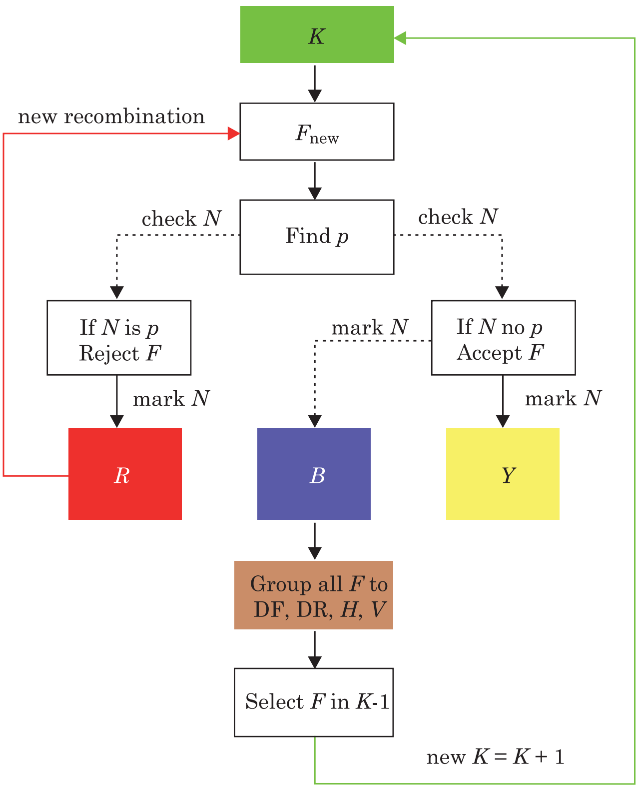


Fig. 1. Scheme of mathematical experiments searching for a new number structure

The selection parameter for arithmetic strings was considered strings in which no prime number occurs (except for the first two elements of the string). Next, calculations were performed on matrices from $K = 0$ to $K = 1{,}000$. A total of $2.5 \cdot 10^{16}$ of arithmetic operations were performed.

The feature extraction process was optimized using a genetic approach (POLI et al. 2008). The analytical assumptions are illustrated below (Fig. 1).

The colours red (R), blue (B), and yellow (Y) represent numbers with the properties given in section Observations of numbers. The sign p denotes a prime number. F is an arithmetic sequence in the study number space K.

Explanation of the colours of the numbers in the paper: red (R) denotes a prime number, blue (B) denotes a number belonging to the hidden triangular structure (numbers for immediate factorization), yellow (Y) denotes numbers lying on extensions of the hidden triangular structure.

Based on the extracted sequences, observations and mathematical analyses were conducted. In the next part of the paper there is a mathematical analysis of the obtained results. The conclusion presents the constructed and tested the factorization algorithm for *blue numbers* of arbitrary length in $O(1)$ time.

Basic properties of triangular numbers

The first observations and properties of triangular numbers were described by DIOPHANTUS (III n.e.). He presented his concept of triangular numbers as a stack of stones with one more stone in each row than in the row above it (Fig. 2).

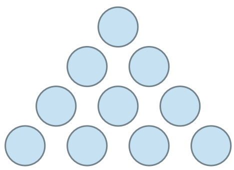


Fig. 2. A stack of stones

So we can define the triangular numbers as recursive formula:

$$T_n = n + T_{n-1} = 1 + 2 + 3 + 4 + 5 \cdots + n \tag{4}$$

where:

$T_1 = 1$,

$n > 1$ and is an integer.

The general formula for triangular numbers can be proven by mathematical induction, and is as follows:

$$T_n = \frac{n^2 + n}{2} \tag{5}$$

We can define triangular numbers for $n = 0$ by $T_0 = 0$, and for negative numbers, analogously by:

$$T_{-n} = -T_n = -1 - 2 - 3 - 4 - 5 \cdots - n \tag{6}$$

where:

$n > 0$.

Wacław Sierpiński included in his book (SIERPIŃSKI 1962) a hypothesis:

Hypothesis 1. If all subsequent natural numbers are to be written down in subsequent lines, n numbers in the *n*-th line, that is, if we create an infinite table:

1
2, 3,
4, 5, 6,
7, 8, 9, 10,
. . . .

in each successive row, starting from the second, there will be at least one prime number.

This interesting hypothesis, still unproven, raises the idea of linking triangular numbers to the distribution of prime numbers and thus to the Riemann hypothesis.

It is easy to prove that $T_n + T_{n+1} = (n + 1)^2$, where $n > 0$, and consequently an interesting equality is assumed by the Riemann function ζ for $s = 2$, then we obtain:

$$\zeta(2) = 1 + \frac{1}{T_1 + T_2} + \frac{1}{T_2 + T_3} + \frac{1}{T_3 + T_4} + \frac{1}{T_4 + T_5} \cdots = \sum_{n=1}^{\infty} \frac{1}{n^2} \tag{7}$$

Wacław Sierpiński in his book on triangular numbers (SIERPIŃSKI 1962) on page 42 and 43, presented proofs of the following theorems concerning the relationship of triangular numbers to prime numbers.

Theorem 1. Each triangular number > 3 has at least two different prime numbers divisors.

Theorem 2. There are infinitely many triangular numbers that are products of different prime numbers.

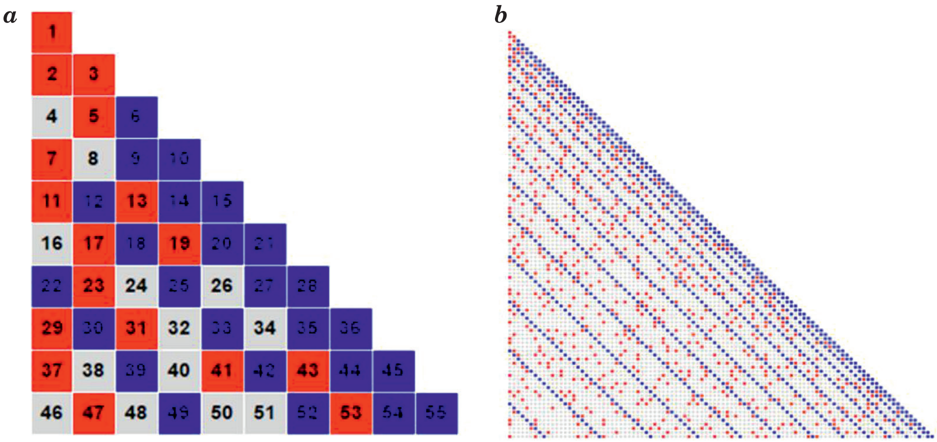
We conclude that the function T_n is an attractive object for further exploration.

Observations of numbers

We can not solve our problems
with the same level of thinking that created them
Albert Einstein

In the section *Basic properties of triangular numbers* we saw definitions of numbers arranged in the shape of a triangle. This is the basic object studied in this work. In order to visualize the prime numbers in the table, we highlight them in red (see Fig. 3*a*).

Definition 1. By $K = 0$ table we mean the left-justified infinite triangular array of consecutive natural numbers written down in subsequent lines, n numbers in the n-th line, that is, if we create an infinite table.



$T = 55$ $T = 5{,}050$

Fig. 3. Triangular matrix: *a* – $T = 55$, *b* – $T = 5{,}050$

Observation 1. (First key observation) On a triangular stack (Fig. 3) formed of consecutive numbers, there are diagonal lines (blue) on which the prime numbers do not lie.

By $T_{(n,m)}$ the note the natural number in n-th row and m-th column at the table.

Fact 1. For $n \geq 1$, $n \geq m \geq 1$

$$T_{(n,m)} = T_{n-1} + m = T_n - (n - m) \tag{8}$$

Especially $T_{(n,1)} = T_{n-1} + 1$.

Definition 2. Elements $T_{(m+k-1,\,m)}$, $k \geq 1$ form the k-th diagonal. The diagonal corresponding to the number $k = T_{r-1} + 1$ is called the r-th main diagonal.

Remark 2. These main diagonals are those colored in blue in observation 1.

Fact 2. The r-th main diagonal starts with the number $T_{T_{r-1}} + 1$.

Proof. Put $m = 1$ and $k = T_{r-1} + 1$ into the definition (2) and the formula (8).

Fact 3. The consecutive numbers lying on the r-th main diagonal are of the form:

$$A_{r,c} = c\left(r + \frac{c-1}{2}\right), \qquad c \geq T_{r-2} + 1 \tag{9}$$

Remark 3. Parameter c with numerates elements of the diagonal, start from $c = T_{r-2} + 1$. We discuss the meaning of elements with $c < T_{r-2} + 1$ in the next section.

Proof. These numbers are elements of the table $T_{(m+T_{r-1},m)}$, $m \geq 1$; so we should have $c = m + T_{r-2}$ (A. Doliwa).

Fact 4. If $c \to$ even, then the divisor $P = \frac{c}{2}$ and $Q = 2r + c - 1$. If $c \to$ odd, the divisior is $P = c$ and $Q = \frac{r + c - 1}{2}$.

Fact 5. For natural c and r, $A_{(r,c)}$ is a natural number.

Fact 6. $A_{(r,c)}$ can be prime number, only if $c = 1$ or $c = 2$.

Fact 7. For every odd c and r there is a factorization of $N = A_{(r,c)} = P \cdot Q$.

Proof. If N is $N = P \cdot Q$ where $1 < P \leq Q$ for odd P and Q is $N = A_{(r,c)}$ where $c = P$ and $r + \frac{P-1}{2} = Q$, so $r = Q - \frac{P-1}{2} > 0$.

Next we move on to the part of the paper where we discuss the new extended properties of triangular numbers.

The extended matrix

Definition 3. The extended matrix $K = 0$ is the matrix enlarged by successive numbers. We extend $K = 0$ to the left, each row is completed in sequence with smaller integers. The points of the major diagonals correspond to the formula $T_{(m+T_{r-1},m)}$.

To expand the space of numbers, we expand the lines of the figure to the right by incrementing (hyperspace) and to the left by decrementing (subspace). We will get an image $K = 0$ for transformation (4).

Observation 2. (Second key observation) The extended blue lines from the observation (1) marked in yellow in figure (4) also do not contain prime numbers, excluding the first two elements of the line.

Fact 8. Elements of the extended array $K = 0$ are given by the formula (8).

Definition 4. ($K = r$ table) The left-justified an infinite trapezoidal array of consecutive natural numbers written $m + r$ in row m (see Fig. 4).

Create transformation $K > 0$. For this purpose, we expand the main space $K = 0$ by subsequent columns. For a $K = k$ transformation, we expand each row $K = 0$ by k columns. This means that in each subsequent row of the transformation, the number of elements in the row is equal to $T_a + k$.

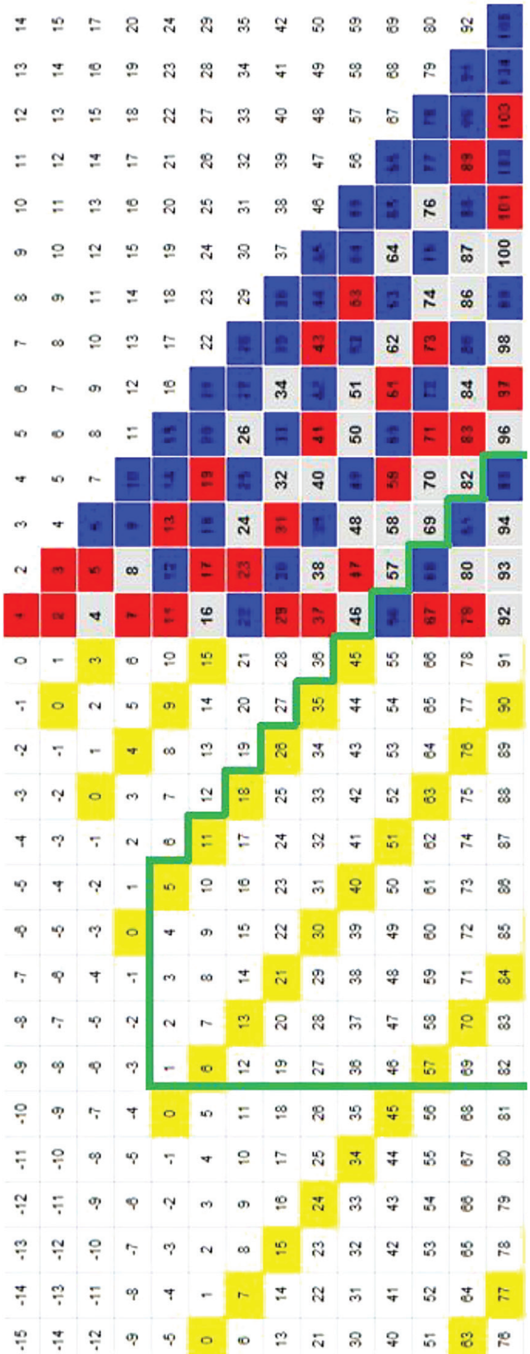


Fig. 4. Extended triangular space in the $K = 0$ transformation with an array $K = 4$

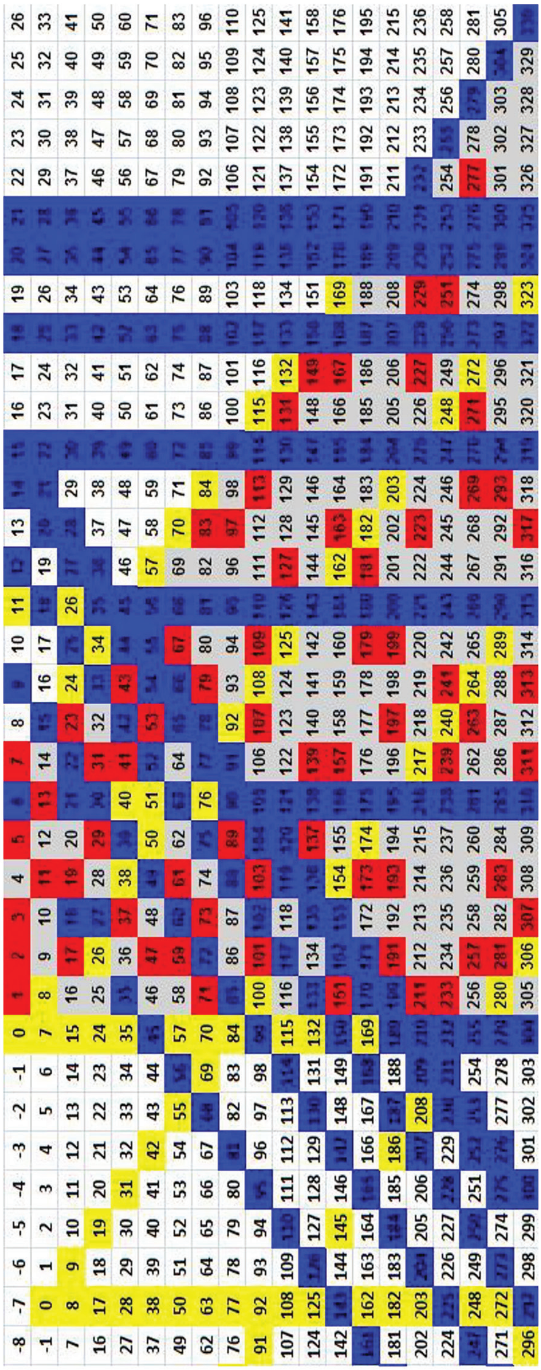


Fig. 5. Matrix transformation $K = 6$

Transformations $K = 6$ are now filled with blue lines that appear on it (Fig. 5), and the expanded structure of the yellow lines. We then get:

$$T_{(n,m)} = T_{n-1} + m \text{ where } n \geq 1, m \geq -T_{n-1}.$$

Definition 5. Transformation K is the part of the extended array having the shape of a trapezoid with the upper left corner $T_{(k+1,-T_k+1)}$, the upper right corner $T_{(k+1,-T_k+K+1)}$, vertical left wall and diagonal right wall.

Observation 3. In the K transformations of the basis matrix, there are new diagonal lines and vertical lines free of prime numbers that extend beyond the unique space of the matrix.

In the next section we will put the blue lines in order and point out their main property related to factorisation.

Study of numerical structures

Let's start with a statement. The elements in the array $T_{(n,m)}$ do not repeat and there are all natural numbers.

Proof. The first row consists of the following numbers $1 = T_{(K+1,-T_K+1)}$, 2, …, $K + 1 = T_{(K+1,-T_K+K+1)}$. The first element in the l line $T_{(K+1,-T_K+1)}$ is greater by one than the last element $T_{(K+l-1,-T_K+K+l-1)}$ in the previous line.

$$\begin{aligned} T_{(K+l,-T_K+1)} - T_{(K+l-1,-T_K+l+K-1)} &= T_{K+l-1} - T_K + 1 - T_{K+l-2} + T_K - l - K + 1 \\ &= K + l - 1 + 1 - l - K + 1 = 1 \end{aligned} \tag{10}$$

From the observation (1) (2) we obtain a drawing of the numerical structure (see Fig. 6) which has several important properties.

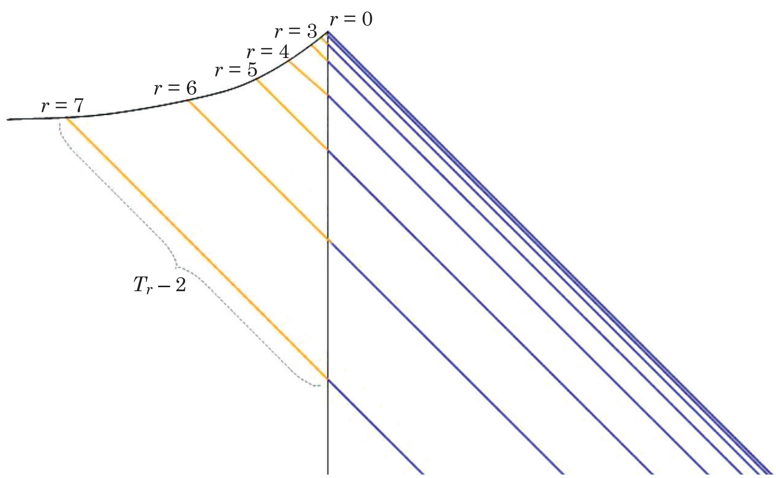


Fig. 6. Transformation $K = 0$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	3	6	10	15	21	28	36	45	55	66	78	91	105	120	136	153	171	190	210	231
2	5	9	14	20	27	35	44	54	65	77	90	104	119	135	152	170	189	209	230	252
3	7	12	18	25	33	42	52	63	75	88	102	117	133	150	168	187	207	228	250	273
4	9	15	22	30	39	49	60	72	85	99	114	130	147	165	184	204	225	247	270	294
5	11	18	26	35	45	56	68	81	95	110	126	143	161	180	200	221	243	266	290	315
6	13	21	30	40	51	63	76	90	105	121	138	156	175	195	216	238	261	285	310	336
7	15	24	34	45	57	70	84	99	115	132	150	169	189	210	232	255	279	304	330	357
8	17	27	38	50	63	77	92	108	125	143	162	182	203	225	248	272	297	323	350	378
9	19	30	42	55	69	84	100	117	135	154	174	195	217	240	264	289	315	342	370	399
10	21	33	46	60	75	91	108	126	145	165	186	208	231	255	280	306	333	361	390	420
11	23	36	50	65	81	98	116	135	155	176	198	221	245	270	296	323	351	380	410	441
12	25	39	54	70	87	105	124	144	165	187	210	234	259	285	312	340	369	399	430	462

Fig. 7. Filled matrix θ for $c = 21$ and $r = 12$

From the drawings (4), (5), (6) we obtain formulas describing the structures of sequences in $K = k$ transformation matrices. Where r is a number of *blue line* in analyzed structure.

Ordering of the line r to the set θ. The set θ we can draw a one-consistent matrix, where any row is the yellow line and extension is a blue line. For triangular numbers in the columns, we add the ordinal value of the column multiplied by the row number minus 1 (see formula 12). We get a matrix containing the grid of all the complex numbers.

$$\theta = \begin{bmatrix} T_1 & T_2 & T_3 & T_4 & T_5 & \cdots & T_c \\ T_1 + 1 & T_2 + 2 & T_3 + 3 & T_4 + 4 & T_5 + 5 & \cdots & T_c + U_{c1} \\ T_1 + 2 & T_2 + 4 & T_3 + 6 & T_4 + 8 & T_5 + 10 & \cdots & T_c + U_{c2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ T_1 + U_{1r} & T_2 + U_{2r} & T_3 + U_{3r} & T_4 + U_{4r} & T_5 + U_{5r} & \cdots & T_c + U_{cr} \end{bmatrix} \quad (11)$$

Where T_c is formula (5), c is θ column, and r is θ row and value U_{cr} – factor for matrix cell. Next we get:

$$U_{cr} = c(r - 1) \quad (12)$$

The main property of this matrix is that the column number c is its divisor. If the result of division is with the remainder, the divisor of the numbers in the columns will be $2c$. In the columns where the ordinal number is divisible by the ordinal number of the other columns, some numbers will be repeated. This arrangement of the grid causes it to contain all the complex numbers.

Figure 7 is an example set θ for max $c = 21$ generated using matrix (11). Figure 7 can be represented in binary form (see Fig. 8), where we mark numbers that are *blue numbers* in blue and numbers that are not – in white. Prime numbers are marked in red. We get then:

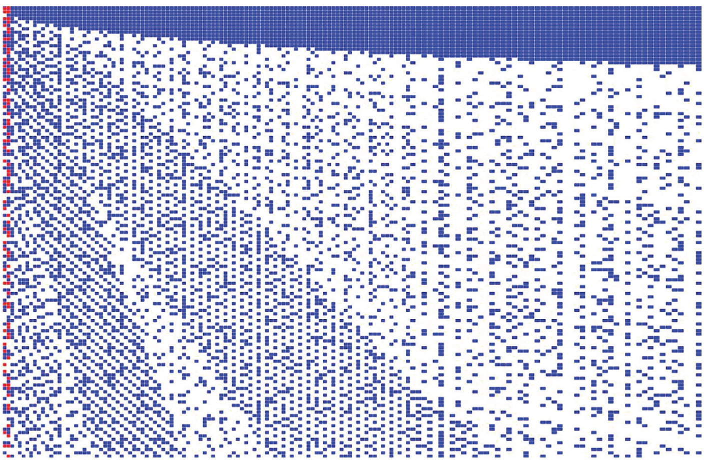


Fig. 8. θ matrix – binary representation (blue and non-blue numbers)

Observation 4. In the θ matrix there are structures of increased density duplicating the blue numbers. These appear as diagonal lines that originate near the upper left corner of the matrix and lay diagonally down the matrix.

The *blue numbers* (which factorise immediately) are distributed in the matrix θ in such a way that their distribution patterns can be determined. The repetition of a *blue number N* in different columns *c* of the matrix indicates that the number has more than one distribution factor. In the next last section, we present the factorization algorithm.

Algorithm of geometric factorization

The algorithm presented in the following part of the chapter invoices every *blue number*. The operation of the algorithm boils down to determining the position of the number *N* in the space U. Then it checks if the tested number N lies on the line *r*. If the number lies on the line *r* it means that it belongs to the matrix θ. Knowing the position of the number in the θ matrix we determine the column *c*. Determining the column *c* for a number lying, is equivalent to finding the divisor of the number $N = P \cdot Q$ under study. Let's start with the theorem.

Theorem 3. For each $N \in \mathbb{Z}$ in the unique space U, in the transformation K and lying on a diagonal or vertical line and belonging to line *r* in the matrix θ, a divisor can be determined.

Execution of the algorithm. In the numerical structure of the space U defined as the transformation $K = 0$ there are diagonal lines *r* belonging to the matrix θ. In the Figure 9 they are marked as yellow-blue lines. In the following steps of the algorithm we will focus on the blue line part.

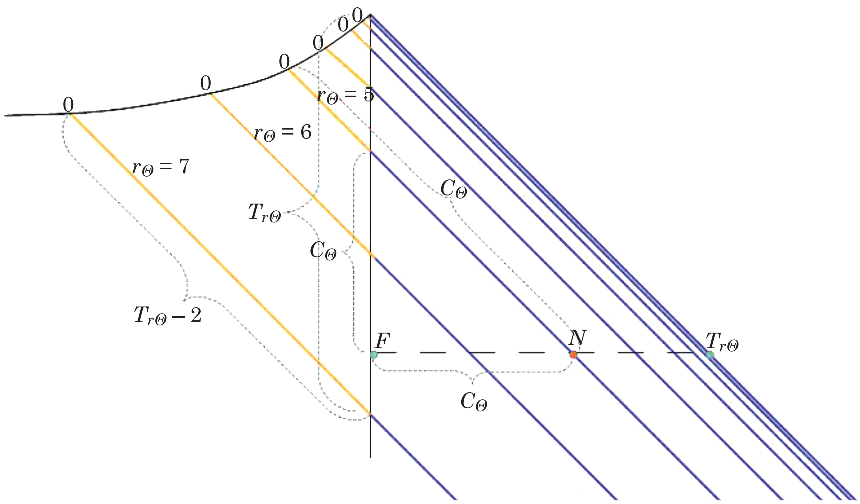


Fig. 9. Transformation $K = 0$ with unique space U

We begin the algorithm by checking the row number in the space U on which the number N we are looking for lies. For this purpose, we will start with a fact:

Fact 10. N is a triangular number if and only if $8N + 1$ is a square number.

Let us define the parameters r_U as the line number in the space U, and r_θ as the line number in the matrix θ. If r_U belongs to a part of any of the blue lines, then $r_U = r_\theta$. Next we will use one of the most important operations on triangular numbers, which is the ability to instantaneously determine the position of a number in the sequence T_r. The property is described in W. Sierpiński book *Triangular numbers*, discussed earlier (SIERPIŃSKI 1962). Using it we determine the value of r_U:

$$r_U = \frac{\sqrt{(8N+1)} - 1}{2} \tag{13}$$

Remark 4. The parameter r_U takes an integer value only if N lies on an edge of the space U. This means that N is then a triangular number.

Knowing the number of the row r_U in which the number N lies, we can determine the first number from this row, this number we denote as F. The number F is necessary to determine the number of the column c_U of the number N in the space U. To determine the number F, we use the basic formula for triangular numbers (5), which after substitutions has the form:

$$F = \frac{\lfloor r_U \rfloor (\lfloor r_U \rfloor + 1)}{2} + 1 \tag{14}$$

Remark 5. The parameter r_U is rounded down to get the correct result F.

Fact 11. $N \geq F$.

Using this fact we calculate a column c_U for number N. Hence, subtract the first number of row F from the factorized number N and add 1:

$$c_U = (N - F) + 1 \tag{15}$$

When $c_U = 0$, the value of c_U takes the value r_U, so then $c_U = r_U$. We then compute the diagonal number D for the matrix space U. This is needed to check that this diagonal line is the blue recursive line later in the proof. We round the value of r_U up to an integer.

$$D = \lceil r_U \rceil - (c_U - 1) \tag{16}$$

Next we need to check that the given diagonal line D is a blue line. To do so, we will again use the fact (10), the action will be denoted as L. For the result to be correct, assume that the blue line count starts from 0, so subtract 1 from the value of D. Write the new line number as $D_{\text{new}} = D - 1$:

$$L = \sqrt{8D_{\text{new}} + 1} \tag{17}$$

If the resulting number L is an integer, this means that the number N lies on the blue line θ. It also means that we can immediately decompose this number into factors P and Q.

If the resulting L is a fraction, then the number is not in space. The execution of the algorithm can then be terminated. If $L \in \mathbb{Z}$ then $D_{\text{new}} \in \theta$, then determining the parameter c_θ is equivalent to finding a divisor P of the number N. To determine c_θ, add the length of the yellow line to the part of the blue line (see Fig. 6 and 9). The part of the yellow line has length $T_{r_\theta - 2}$. To determine the parameter r_θ we will again use the property of triangular numbers to determine the position in a series.

$$r_\theta = \frac{\sqrt{(8D_{\text{new}} + 1)} - 1}{2} + 1 \tag{18}$$

and

$$c_\theta = c_U + T_{r_\theta - 2} \tag{19}$$

Next we determining a divisor of a number N. The final step of the algorithm is to determine the P and Q factors.

$$Q = \frac{N}{c_\theta} \tag{20}$$

If new result $Q \in \mathbb{Z}$ we calculate $P = \frac{N}{Q}$ and finish the algorithm, if the result Q ended with a remainder value of 0.5 then new value of Q_{new} is:

$$Q_{\text{new}} = 2Q \tag{21}$$

and we calculate P using the obvious formula:

$$P = \frac{N}{Q_{\text{new}}} \tag{22}$$

Factorisation results for numbers $N > 10^{800}$. The numbers shown below are examples of pseudoprime numbers N lying on the blue lines of the matrix θ (see Eq. 11 and Fig. 7). The N numbers have been factorised into products of P and Q at time $O(1)$. The products P and Q, after examination by the Rabin-Miller algorithm, were marked as prime numbers.

Example 1: length of number N is 856 digits.

$N = P \cdot Q$:

24500003634679768990720359931122629789054129036731950939180706695724290608989365391399846392305826771143790151554444187435543395928542593168836512046447689574942858308098075864418887107862817126976471341465593389737655820902769991449125762133266315621946560829012

217486569575750843346328428345270623619604114530311515074001607690
780345002322220472477428702565481557366584957925117989480227077016
093079583758358683039141105250214625262527284733608088542303121151
659434905303009532066332713776738626913406917420721941467029751074
391519374463464365512479708850631016401140509507315469879247073243
379461678874143379726483085496001765044695643443036444505065149804
977483481024078970106904806482353923899808649942104364541825491 80
523149303880531964472069480198375530986095092335490853941008205767
880963923845053673137476975088070960479813291521409701014060792537

Result of factorisation:

P :

700000051923994774080838499891589877111945018747175506716205263 13
414826220965603687043609953189668799224104320713602293290204041 5
626970447860736819513957721087759786715778064520875070721701899318
256382294775878171081892119857992553178225175050874529733723414728
508559885785282035325112403959661997089601741167425925080900568 27
649970731371358881005234137921691898133232973749586341208901772 22
830049340071185449889263859605 2012223

Q :

350000025961997387040419249945794938555972509373587753358102631 56
707413110482801843521804976594834399612052160356801146645102020 78
134852239303684097569788605438798933578890322604375353608509496 5
912819114738793908554094605992899627658911258752543726486686170 73
642542799428926410176625562019798309985448008705837129625404502 8
413824985365685679440502617068960845949066616486874793170604450 8
8611415024670035592724944631929802600 6119

Example 2: length of number N is 1012 digits.

$N = P \cdot Q$:

100133722014599215537243501526216728648503377861520810263350851 9
343521288747235351069013274638720343999003505026358143079265908 4
653151541295373940070991025354797867569383104178667999999142610 0
480123907551850978610608003711964034995972765928502605266730029
507990937377185169090452075124573336035320565619881760470760662 8
713764604674515110693283114138620200222466679813646008058666238 7
801036876171318740920570319151082714190937626531723808736403994 63
651793548838508467630927465339837186732838031859165950506008983
535371810476625374513180169556642065162396000895900157651085041 2
324342221481395094085059848149576852251063645327844931465657835 6
293684287719025705149138205367065346189347403912072622268997409 1
881101770598693022663705350552687233352351353436330156760332650 8

7012478367007908569354828566524587320274399954346933021064165610
7426431996430739860190339109962839012965785473397079077794432205
2177450653693681661476537064503373687218999339537804548952140286
47712633369315659118839807500888531286932571511291341

Result of factorisation:

P :

44751250712041382126107540800165752835106714952155965882614702998
40891416031963816510601574217756824945010749902958954445493896269
53800722678524868367899342385284024493174024894015283513140613578
06480558146884060316949780669261045052471536861677050061257769804
27745316527397093499622166683582438857010195513204376396468272470
38980607000735306053655489546551975668685923732378955161461738654
7153652782063253366449120994005508361345593615043042899524751709
6310440903891739976771831357806364319274476592705969

Q :

22375625356020691063053770400082876417553357476077982941307351499
20445708015981908255300787108878412472505374951479477222746948134
76900361339262434183949671192642012246587012447007641756570306789
0324027907344203015847489033463052252623576843083852503062888490
21387265826369854674981108334179121942850509775660218819823413623
51949030350036765302682774477327598783434296186618947758073086932
73576826391031626683224560497002754180672796807521521449762375854
8155220451945869988385915678903182159637238296352989

Example 3: length of number N is 1970 digits.

$N = P \cdot Q$:

50000049557813450819513337974258437022991928946794095932766147601
45562630179200122684506019831273556068070910116753384878391776037
86409938854477134439597474552836086751413956486939739001499669352
86517177412124326727262822217834286164941337284056452699744272125
36234615671068526402414253933790475700909659727345715409614285995
28745614647973247526656690232060752070600645746675725476636694805
16356682221678471500866015676971663478326891732756290765839913898
03512476186782219451848814338833467571794799158640519022386561952
712161799585147209044898518445263326419761635581380341649717501498
12026291630181307631561707666382704237365317269883216261722255270
42464828354057788763683771083574098553171756204100390344515187324
8293951433653523323822589448187772619950374621366242716066057939
2458761787823265863338256110598542138551323454113009215099426773
327567328447905074684303236308928623648036294444206603167995352
8889421201809624600725296213447393036978509896748705637157010617

7504640253515082951872543868931792719807094769467287787979306135
336879303652424374842603934624730300924410618535455092476246156
3840618191290025995330795912224661225051356972429846381802859173
6502697104578705192322135886609149324126489598222855614969725854
99780465012943257477425679919107004833310770557528317424170216763
17041242879311910181174293198029101075499956163648472508464148139
531297440995899435286370966348946973789030068934712552624457795
7991313089633754401713523118947034181948118119064900759980364924
7276410569885796731774694453060660996185131050179692342369221088
1268863269389818188092477367528834313987674346529383742755684071
0467092889368512053482031213679080177519200913925037039882415159
1694622282270382697961431400924413389643413069539858482182133038
495662089269083346631252773031371871235073034465051636383554603
8005821576011421328875307733875048118164305930992838130243709905
5017634700506564320339842044054884234434275152891479512809977834
1798475362524496179005328042131927398081

Result of factorisation:

P :

10000004955780117094122884525509424638684731274190306155862905990
08433091152686604823911410388180930868952853537625062875445324440
103299295131085962536013229157996539862028181215563582285792741583
586009357780631775151113020349944403871864918054112216636134793251
018869892406101081170790477102899246842958417169007068315048105326
838150559154505637357138041478871263113392819130469967066085685282
348580366162937147976674540772517303505888764527502358716868938388
703374089498898607319095171302453316248934353405875337910342492914
666356766481697969824522782164192929291023564352461243947850484949
277402032283541102225582418003689905068096780776043515436811762791
566980191614162567785768855219787638513345953664396655115933897294
85355321625931228930104451604220413302991988954914420823989919445
505939023653253023490866137985237589574492645157654896322459173518
32069545639255156949336029858510643530736391020375960837904294553
2117472892781807581251781267445388857907501411848395657697076529563

Q :

5000002477890058547061442262754712319342365637095153077931452995
0421654557634330241195570519409046543447642676881253143772266222
0051649647565542981268006614578998269931014090607781791142896370
7917930467889031588757555651017497220193593245902705610831806739
662550943494620305054058539523855144962342147920858450353415752
405266341907527957725281867856902073943563155669640956523498353
3042842641174290183081468573988337270386258651752944382263751179

3584344691943516870447494493036595475856512266581244671767029376
6895517124645733317838324084898491226139108209646464551178217623
0621973925242474638701016141770551112791209001844952534048390388
0217577184058813957834900958070812838928844276098938192566729768
3219832755796694864742677660812965614465052225802110206651495994
47745721041199495972275296951182662651174543306899261879478724632
25788274481612295867591603477281962757847466801492925532176536819
5510187980418952147276605873644639090379062589063372269442895375
0705924197828848538264787

Example 4: length of number N is 2201 digits.

$N = P \cdot Q$:
83241347552730596369787208161338048046042350250242419173402492179
78150948900581696789123636806342654464819748539901787257705501877
113857191579115537794412361439492758746699091210317277318836066190
32098368651676523711729108608617262621563386808582010995423063216
35191821802734402313937053654573529253900548079893006400036741783
33635211317077161893100560165444342040740334840537786375631731103
05620898904041937386400872573261660679161386725791414225807422648
33049890936698228659006358893651450195523192875292973402216765799
18215807316159283686934937783389113673984578099271694839301996626
05996683034481578738600220695978417135744181061796141837358712559
61707924082248675282663744792997454208958712637271721061764506362
20228305084713125208239627852814143676558688761117754479429603097
3902383283898425804602427027663181236283523246036956593230226365
52161510446462640889061359392374302627439432474186876812847122237
44199181267459119135251227704744412985045111859670900629769068978
07455857013445925664956792913338816782439353269307312036137643511
6049752259054336289291913907654421384760814333856238696957090849
64170004790397135322186827889260934121460193509287345872324176117
175291133927909561469620987424240159591881512155752614938010935328
6379956280208674548034967632604657396185428114634305773263962034
0678469277799809007078050919061536577079657628997095909004403928
33838160606812479382596049870296134316813699245839053517539185157
08690716579996409880931625716414962212728457438671491240323493462
99717509401845826446177687639291841946868122577638695077480074344
40916879913186118756155316132312866820152733835899496558767683418
92875653911360933531177331631623192870723257403628255091215573548
4279577895932543449616577455008793838594015965048254868057767900
06484942740568095613042050938057916154406699232363061195821348161
3993195920543132064665966045827150178771346058686949671835253968
9770629607778350499087029759532310998596577475956013209868476075

6290430956426821130337900175371767593630211835467269222851781143
3115063544456735213371128139448282655839975799520562755085798708
8126180845747906270584946985353436955300968423878227237171533100
9772285073027678432560594575532118858558882459807626899796326 47

Result of factorisation:

P :

4080229100252352162516286158826346725011214528985201002201487942 9
2362400454501820056271645000272626359900235562037362212324955780
1170941228845255094246386847312741903061558629059900843309115268 6
6048239114103881809308689528535376250628754453244401032992951310 8
5962536013229157996539862028181215563582285792741583586093577806 3
1775151113020349944403871864918054112216636134793251018869892406 10
1081170790477102899246842958417169007068315048105326838150559154 5
0563735713804147887126311339281913046996706608568528234858036616 2
9371479766745407725173035058887645275023587168689383887033740894 9
8898607319095171302453316248934353405875337910342492914666356766 4
8169796982452278216419292929102356435246124394785048494927740203 2
2835411022255824180036899050680967807760435154368117627915669801 9
1614162567785768855219787638513345953664396655115933897294853553 2
1625931228930104451604220413302991988954914420823989919445505939
0236532530234908661379852375895744926451576548963224591735183206
9545639255156949336029858510643530736391020375960837904294553 21
1747289278180758125178126744538885790750141184839565769707662097 9

Q :

2040114550126176081258143079413173362505607264492600501100743971 4
6181200227250910028135822500136313179950117781018681106162477890 05
8547061442262754712319342365637095153077931452995042165455763433 0
2411955705194090465434476426768812531437722662220051649647565542 9
8126800661457899826993101409060778179114289637079179304678890315 8
8757555651017497220193593245902705610831806739662550943494620305 0
5405853952385514496234214792085845035341575240526634190752795772 5
2818678569020739435631556696409565234983533042842641174290183081 4
6857398833727038625865175294438226375117935843446919435168704474 9
4493036595475856512266581244671767029376689551712464573331783832 4
0848984912261391082096464645511782176230621973925242474638701016 1
4177055111279120900184495253404839038802175771840588139578349009
5807081283892884427609893819256672976832198327557966948647426776
6081296561446505222580211020665149599447745721041199495972275296
9511826626511745433068992618794787246322578827448161229586759160
3477281962757847466801492925532176536819551018798041895214727660 5
8736446390903790625890633722694428953750705924197828848538310493

Conclusion

The algorithm presented in this paper extends the factorization possibilities previously offered by the properties of triangular numbers. The algorithm is easy to implement and its complexity for factorization in the group of *blue numbers* is $O(1)$. Using the algorithm in generating new RSA keys increases their security. The presented algorithm is also a new look at experimental approach to the analysis of number spaces generated by triangular numbers and derived patterns.

It should be noted that the disclosure of new hidden triangular number structures may result in the need to check the currently used RSA keys to exclude pseudoprime numbers that are blue numbers. The realization that there may be pseudoprime numbers that lie on the hidden triangular number structure is a new weakness in the cryptographic security of RSA keys. It is recommended to arm the algorithms that generate RSA keys with a verifier that checks if a given pseudoprime number is not a *blue number*.

Acknowledges

We would like to thank Professor Adam Doliwa for valuable math tips.

References

ADLEMAN L.M. 1991. *Factoring numbers using singular integers*. Proc. 23rd Annual ACM Symp. on Theory of Computing (STOC), New Orleans, p. 64-71.

ADLEMAN L.M. 2005. *Algorithmic number theory and its relationship to computational complexity*. Proceedings 35th Annual Symposium on Foundations of Computer Science, p. 88-113. https://doi.org/10.1109/SFCS.1994.365702.

ADLEMAN L.M., POMERANCE C., RUMELY R.S. 1983. *On distinguishing prime numbers from composite numbers*. Annals of Mathematic, 117: 173-206.

BACH E., SHALLIT J. 1996. *Algorithmic number theory. Efficient algorithms*. MIT Press, Cambrigde.

BONEH D. 1999. *Twenty Years of attacks on the RSA Cryptosystem*. Notices of the American Mathematical Society, 46(2): 203-213.

BREUR T. 1996. *Statistical Power Analysis and the contemporary "crisis" in social sciences*. Journal of Marketing Analytics, 4(2–3): 61–65. https://doi.org 10.1057/s41270-016-0001-3.

COHEN H. 1993. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, Berlin, Heidelberg.

Command and Control in the Fifth Domain. 2012. Command Five Pty Ltd.

DIOPHANTUS. III n.e. *Arithmetica*.

DIXON J.D. 1981. *Asymptotically Fast Factorization of Integer*. Mathematics of Computation, 36(153): 255-260.

FAYYAD U., PIATETSKY-SHAPIRO G., SMYTH P. 1996. *From Data Mining to Knowledge Dis-covery in Databases*. AI Magazine, Norwich.

GAUSS C.F. 1966. *Disquisitiones Arithmeticae By Arthur A. Clarke*. Yale University Press, New Haven.

HASTIE T., TIBSHIRANI R., FRIEDMAN J. 2009. *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. Springer, New York.

KALISKI B. 2006. *Growing Up with Alice and Bob: Three Decades with the RSA Cryptosystem*. RSA Security.

LEHMAN R.S. 1974. *Factoring Large Integers*. Mathematics of Computation, 28(126): 637-646.

MARTÍN-LÓPEZ E., LAING A., LAWSON T. 2012. *Experimental realisation of Shor's quantum factoring algorithm using qubit recycling*. Nature Photonics, 6: 773–776. arxiv.org. https://doi.org/10.1038/nphoton.2012.259. arXiv:1111.4147.

MOREE P., PETRYKIEWICZ I., SEDUNOVA A. 2018. *A Computational History of Prime Numbers and Riemann Zeros*. arXiv:1810.05244. https://doi.org/10.48550/arXiv.1810.05244.

NIVEN I., ZUCKERMAN H., MONTGOMERY H. 1991. *An Introduction to The Theory of Numbers*. John Wiley and Sons, Hoboken.

POLI R., LANGDON W.B., MCPHEE N.F. 2008. *A Field Guide to Genetic Programming*. Lulu Enterprises, Morrisville.

POLLARD J.M. 1975. *A Monte Carlo method for factorization*. Nordisk Tidskrift for Informationsbehandlung (BIT), 15: 331-334.

RIEMANN'S B. 1859. *Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse*. On the Number of Primes Less Than a Given Magnitude. Monatsberichte der Berliner Akademie, Berlin.

RIVEST R.L., SHAMIR A., ADLEMAN L. 1978. *A Method for Obtaining Digital Signatures and Public-key Cryptosystems*. Communications of the ACM, 21(2): 120–126. https://doi.org/10.1145/359340.359342. MIT Laboratory for Computer Science, Cambridge, Massachusetts.

RSA CyberCrime Intelligence Service. 2013. RSA Security, Rsa.com.

SAMOJLUK A. 2019. *Algorithm of Geometric Factorization*. Master thesis. Chair of Mathematics and Computer Science, Uniwersytet Warmińsko-Mazurski, Olsztyn.

SANJEEV A., BOAZ B. 2009. *Computational Complexity: A Modern Approach*. Cambridge University Press, Cambridge.

SCHATZ D., BASHROUSH R., WALL J. 2017. *Towards a More Representative Definition of Cyber Security*. Journal of Digital Forensics, Security and Law, 12(2).

SEGARAN T., HAMMERBACHER J. 2009. *Beautiful Data: The Stories Behind Elegant Data Solutions*. O'Reilly Media, Sebastopol.

SIERPIŃSKI W. 1962. *Liczby trójkątne* (*Triangle numbers*). Biblioteczka Matematyczna, t. 12, Państwowe Zakłady Wydawnictw Szkolnych, Warszawa.

SIERPIŃSKI W. 1987. *Wstęp do teorii liczb*. Third Edition. Biblioteczka Matematyczna, t. 12, Państwowe Zakłady Wydawnictw Szkolnych, Warszawa.

SIERPINSKI W. 1988. *Elementary Theory of Numbers*. Państwowe Wydawnictwo Naukowe, Warszawa.

STEVENS T. 2018. *Global Cybersecurity: New Directions in Theory and Methods*. Politics and Governance, 6(2): 1–4. https://doi.org/10.17645/pag.v6i2.1569.

WILLIAMS H.C. 1982. *A p+1 Method of Factoring*. Mathematics of Computation, 39(159): 225-234.

YOST J. R. 2015. *The Origin and Early History of the Computer Security Software Products Industry*. IEEE Annals of the History of Computing, 37(2): 46–58. https://doi.org/10.1109/MAHC.2015.21.