



ON A REGULARITY THAT DETERMINES PRIME NUMBERS

RUSTEM CHINGIZOVICH VALEYEV

NPO CKTI, Joint-Stock Company I.I.Polzunov Scientific & Development Association on Research and Design of Power Equipment
Atamanskaya str., 3/6, St-Petersburg, 191167, Russian Federation

ABSTRACT

Nowdays the order, existing in set of primes, and laws of their arrangement among other numbers remains unknown. Found dependences and algorithms are applicable only for some subsets of primes or primes of a special kind. The possible point of view is presented in article to a question of reality of detection and use of regularities (including Riemann hypothesis) to which all set members of a set of prime numbers are submitted. Any regularity which determines the size of each prime number, can't be (allegedly can't be) adequately and completely defined. And also it can't be (can't be for sure) reliably proved and successfully used in actions which belong to any prime numbers.

Keywords: *Primes, Riemann Hypothesis, Algorithm AKS, Complexity, NP-Complete Problem, P Vs NP, Discrete Structures, The Uncertainty Principle*

1. INTRODUCTION

Many theoretical and practical problems and the ambiguities concerning prime numbers, eventually demand the clear answer to the one and the same question: what is regularity which all prime numbers submit to? [7], [4], [12], [13], [23]. How is it possible to express ones prime numbers through other prime numbers? How can set members of this capricious and uncontrollable (now) infinite set be received by means of set members of any more convenient set?

Determination of primality, cryptographic data security, Riemann hypothesis – it is possible to continue this list of most often mentioned questions within the subject of “prime numbers” (“primes”).

In article of 1859 B. Riemann offered a new method of an asymptotic assessment of distribution of prime numbers. At the heart of a method there was function later called “Riemann zeta function”. Riemann showed that distribution of primes depends on where zeta function became a zero. The problem consists of describing all the non-trivial zeros of the Riemann zeta function. There were no counterexamples of the hypothesis. Arguments in favor of the validity of the Riemann hypothesis are strong, but there are also doubts about it [19]. Numerical experiments with zero of zeta function impress: calculation methods to the one million billion billion first zero (are checked 10^{13}) have already offered.

For a long time it has been noticed, that the primes are very similar to the physical bodies or elementary particles that are in a position of minimal potential energy. Probably the analog of energy for primes is the number of parameters that determine it (only one parameter “the value of this number”).

The natural frugality of the nature is also evident in the internal structure of composite numbers: here the role of factors plays a minimal quantity of the minimal primes.

Numerous researches study carefully those or other sequences and subsets of primes [3], [6], [8], [11], Riemann zeta function from various points of view [2], [14], [17], less obvious questions [9], [15], [18], [20], [22] etc. This article is always only about a certain dependence “Fpr”, which all without exception set members of the set “primes” submit to.

2. ABOUT PRIMES LESS FORMALLY

It is known that primes are those natural numbers which are divisible by [without the excess] 1 and by itself. The same can be expressed less formally: primes are not divisible at all.

Hereinafter in square brackets there are words which are clear from a context and can be missed.



If the natural number n is composite, the set N of natural numbers can be divided at least into two subsets of identical power. If the composite number has k factors, the set N can be presented visually as a certain discrete k -dimensional space of S_k . Each of axes of this space corresponds to one of k of primes, and all cells are filled with set members of a set N (see Figures 1 ... 4). If $k > 1$ and to “a k -dimensional parallelepiped”, which is S_k space (i.e. to a natural number n) add unit, two variants are possible:

1) S_k space with “an excess ledge” can be “deformed” (it is possible to change by means of use of other primes as axes and/or change of quantity of axes) so that “the excess ledge” disappeared and became one of cells in S_k space. It means that the natural number $(n+1)$ is a composite number too.

See figure 1 in the appendix

2) No manipulations with space of S_k to which “the excess ledge” was added, will lead to that “the excess ledge” will disappear and become one of cells in k -dimensional S_k space. It means that the natural number $(n+1)$ is already prime number and S_k space expressing it can be only one-dimensional.

See figure 2,3,4 in the appendix

Natural numbers are very similar to drops of physical viscous liquid or abstract connected topological structure, aspiring to reduce its outer surface to a minimum (or until a certain equilibrium state). Composite numbers do it in every possible virtual spaces with dimensions $k > 1$.

For primes this state is also possible – but only in one-dimensional virtual space S_1 (the most primitive indivisible form of the quantity – and the most primitive indivisible form of the space). That is quite logical: the nature does not tolerate emptiness, redundancy and absence of contraries.

3. ORACLE AND DETACHED ONLOOKER

There is a constructive well-known concept “oracle”. Therefore, the natural and symmetric concept has the right for existence – it can be identified, for example, as “detached onlooker”.

Definition: oracle is something that has all without exception opportunities and data on all

values parameters of all essences, dependencies and the phenomena existing in the real world.

Definition: detached onlooker is something extremely omnipotent (after the oracle) that has not all opportunities and all information existing in the nature; the detached onlooker can be not only the person (“the one who studies the phenomenon, solves a problem, investigates system, creates algorithm, looks for the task answer” etc), but also the relevant technical or any other system operating independently or together with the person.

The detached onlooker is always out of what he studies, solves, investigates, creates, looks for, etc.

Definition: algorithm – a set of parameters and actions that allow to achieve the intended goal for all valid values of these parameters.

Among other mathematical tools there is a universal and almighty method from a theoretical (only from a theoretical) point of view:

Definition: exhaustive method – a detection of all without exception set members and determination of value (values) of the parameter (parameters) of each separate member of the set; synonym: brute force.

Definition: algorithm “exhaustive search” – an algorithm using the exhaustive method.

4. INACCESSIBILITY

In case of identity absence of the detached onlooker and the oracle the emergence of the concepts of “accessibility” and “unavailability” (i.e. surmountable and insurmountable for the detached onlooker complexity) is inevitably.

Definition: accessibility of a parameter A – an opportunity for the detached onlooker to use all values of the parameter A in his own purposes and desires; antonym: inaccessibility.

Definition: accessibility of a set B on parameter A – an accessibility of parameter A of all set members of the set B .

Definition: threshold of predictability of a set B on parameter A – a border between the accessible (on parameter A) and inaccessible (on parameter A) subsets of the set B .

Definition: “hypothesis about the threshold of predictability” – an assumption about the existence of the sets that have at least one inaccessible subset.



The concept “threshold of predictability” can be applied in a more comprehensive sense: it is a maximum of these or other opportunities (resources) which the detached onlooker has in the system. All system’s elements which are behind this floating or fuzzy virtual border, at least in one item are not supervised (are not controlled) by the detached onlooker and therefore can not be used in any utilitarian purposes.

Example: the threshold of predictability for system “Traveling Salesman Problem” (TSP) on parameter “the exact answer” at present is: for a personal computer – graph with 15...16 nodes, for all existing and simultaneous acting supercomputers – probably, graph with several hundreds (but not with thousands) nodes.

For the oracle by definition there is nothing inaccessible. But for the detached onlooker of the concepts “inaccessible regularity” and “regularity which doesn't exist” are identical.

5. ABOUT A DEPENDENCE BETWEEN SET MEMBERS OF TWO SETS

Such based on a phenomenon “quantity” dependence between the independent and dependent sets (Figures 12, 13) is the majority of enough laconic (from the point of view of length of record which completely determines this dependence) analytic (“calculated on the tip of the pen”) functions and regularities:

Definition: “compact analytic” regularity – a general conventional name used further for accessible to use by the detached onlooker analytical (calculated), logical and topological regularities, etc; antonym: “compact nonanalytic” regularity.

Examples of the “compact analytic” regularities: any quantitative and functional dependences, which are controlled by totality of calculations, functions, algebraic formulas, systems of the equations, algorithms, mathematical models, geometrical constructions, etc.

Definition: non-quantitative parameter – a parameter which values are not expressed by numbers or can not be expressed by numbers.

Examples of the “compact nonanalytic” regularities: dependencies between non-quantitative parameters; boolean functions; tabulated functions; logical and verbal conditions etc.

Among mathematical tasks and problems (i.e. among systems “sets of the data and dependences between these sets”) it is also possible to allocate two remarkable spacious groups:

Definition: “task of a geodesist” – a task or a problem, in which detection (or creation) of a required set member of considered set is possible by means of an accessible set of “compact analytic” regularities; here enough one action (one finite set of manipulation by numbers, functions etc), the result of this action predicts such regularities.

Examples: the purposes which successful decision professional actions direct to of land surveyors, navigators, experts in technical calculations, detectives etc; definition of a site of a source of a radio signal by means of two and more passive radars; sorting of a mix of spheres of different diameter by means of a sieve.

Definition: “task of the Cinderella” – a task or a problem, in which detection (or creation) a required set member of considered set is possible only with the help of exhaustive method; here the result cannot be predicted by any accessible analytic regularity, so we need to commit large quantity of same-type actions.

Examples: the purposes to which successful decision efforts of a bee are directed by search of nectar; actions of a Pointillism artist or a scanner; sorting of a mix of grains of different plants which have the identical form, the size and weight.

6. IRREGULARITY

Any regularity (dependency) f can be viewed as a kind of a set of information that fully describes this regularity. In general case the regularity F can be a set, which consists of many regularities f_i , which are independent from each other (Figures 5, 6). Unless otherwise stated, here and everywhere below we speak only about the phenomenon of “quantitative regularity”: it is only determined by quantitative regularities.

Definition: regular regularity F – regularity, satisfying the condition $|F|=1$

Example: the trajectory of a thrown stone.

Definition: irregular regularity F – regularity, satisfying the condition $|F|>1$

Example: the trajectory of the Space Shuttle (consists of regularities “ascent”, “orbital flight”, “braking”, “gliding”).

It is logical to assume that increasing of $|F|$ regularity F can fail to be compact. It is difficult to give a clear universal definition – for assessing the complexity of the regularities (and the complexity of the data sets) the concept “threshold of predictability” is more convenient.

Definition: ordered regularity – a regular (or irregular) accessible regularity.

Definition: disordered regularity – a regular (or irregular) inaccessible regularity.

Definition: regular on a parameter A data set is a set in which the values of the parameter A for all set members of this set are the values of the regular regularity.

Definition: irregular on a parameter A data set is a set in which the values of the parameter A for all set members of this set are the values of the irregular regularity.

Definition: ordered on a parameter A data set is a set in which the values of the parameter A for all set members of this set are the values of the ordered regularity; antonym: “disordered on a parameter A data set”.

The concepts “irregularity” and “disorder” are often practically synonymous.

See figure 5-10 in the appendix

7. ABOUT DEPENDENCE BETWEEN THE SET MEMBERS OF THE INITIAL SET T AND THE SET Q OF ITS COMBINATIONS

Here we are talking only about the Cartesian product, but much is fair for other combinations (Figure 11):

$Q = X*Y$, $T = \{X, Y\}$ – an example of a “combinatorial” dependence for the sets T and Q

Definition: structural set member is a set member, which is treated as the fact of existence of the considered set member in this set, without taking into account all other parameters of this set member.

Comment: The term considers set members as certain absolutely abstract featureless identical “carriers of parameters”. Inexact analogy from linguistics: structural set members and their parameters are similar nouns and adjectives accordingly.

Combinations, i.e. set members of a Q set, are only possible to be created from set members of an initial set T , but they can't be found by means of algebraic manipulations with set members of T set. It is impossible for a combination directly to be used in formulas as it is can be done with analytical dependences. Combinations are defined only by the existence fact (or non existence) of t_i set member in a combination q_j and by the rule according to which the combination under consideration is created. Only “not analytical” algorithms (instructions for a person or a computer) are possible which according to compact verbal and logical rules make numerous primitive clonings of the mentioned set members, their placements in these or those subsets and the subsequent quantitative operations with their parameters.

7.1. Combinations and function compositions

Structural elements of a T set by definition have no quantitative parameters. They can't be operated by means of regular or irregular quantitative dependences. Therefore they can't form any regular composition of quantitative dependences to irregular composition. Structural elements both T and Q sets always play only a role of a certain neutral environment in which they are realized and interact and can form to irregular these or those quantitative parameters and communications between them.

Nevertheless structural elements of a Q set always comprise a certain order (Q is always possible to present in the form of matrixes with natural frequency of cells and with natural numbering of set members of T on matrix axes). This harmony in T operated by natural numbers can be:

a) kept in Q – if combinations of regular quantitative parameters of set members of T are considered (for example, the Cartesian product of regular sets is a regular set: Figure 7);

b) destroyed in Q – if combinations irregular quantitative or combinations with participation of any not quantitative parameters of set members of T (Figure 8 and 9) are considered;

Note: “regular regularity” follows from definition that not quantitative parameters of set members of a set can submit to certain regularities as well. Example (Figure 11): the structural elements marked with symbols “rhombus”, “triangle”, “ellipse” submit to “not quantitative” regularity

“geometrical figures”, “snowflake” and “lightning” – “the weather phenomena”, “shuriken”, “lash” and “the ankh sign” – “antiquarian subjects”.

But in general case not quantitative parameters can't essentially be used directly in analytical formulas (even if certain conditional quantities are delivered to them in compliance), or they form irregular or even the disordered set.

7.2. Complexity of a dependence

Complexity of any dependence is always directly proportional to quantity of its domains and complexity of the dependence in each such domain.

If in a certain dependence of kind $Y=f(X)$ each value of argument X is put in conformity E values of Y , where $E \geq 1$, the main distinction between “analytic” and “combinatory” dependences looks so (Figure 11):

a) At “analytic” dependence (function) $Y=f(X)$ quantity of values of the dependent variable is equal $1 \leq E \ll |Y|$, and the graph of dependence allows to receive nontrivial values of the dependent variable; X it is determined on a unique range, complexity of dependence is equal to complexity of f ;

b) At “combinatory” dependence $Y=f(X)$ concept “function” loses sense, here always $E=|Y|$, and from graph of Y here (i.e. from a matrix of structural set members of Q) there is no more benefit, than from a sheet of the lighted photographic paper or from “The Black square” of K.Malevich; complexity of such dependence for structural set members is equal $|X|*|Y|$, for parameter (for example, quantitative) of these set members is directly proportional to $|R_x|*|R_y|$ (R_x and R_y are dependences which determine values of this parameter for all set members of X and Y accordingly).

If in Q there is a minimal on complexity regularity R for values of quantitative parameter P_q of all set members of Q , the minimal complexity of definition P_q at all set members of Q is equal to complexity of regularity R .

See figure 11-14 in the appendix

8. ACCESSIBILITY OF THE SET OF ALL PRIMES

“God made the integers, all else is the work of man.”

Leopold Kronecker

Most successful of created for many centuries modeling analytical laws give quite inadmissible deviations (absolute and relative errors – see Figures 15, 16), while the neighbor primes in size of billions of billions can differ from each other on 2, some primes and their subsets, probably, remain invisible even to such regularities, etc.

See figure 15-16 in the appendix

Hypothesis which has the right to existence is the following: most likely, for primes such “formula” which all primes are distributed on the set of natural (or any other) numbers (such more-less compact law, suitable for practical application) does not exist.

8.1. The best algorithm of the identification of primes which exists on today

The first unconditionally universal polynomial determined primality test of M.Agrawal – N.Kajal – N.Saksena known as test AKS (algorithm AKS), has complexity which is estimated by size only $O(\log^6 n) \dots O(\log^3 n)$, where n is considered natural number (Agrawal et al., 2008).

Complexity (labour-input, resource capacity) of revealing of primes by means of the polynomial test AKS incommensurably is more effective than usual exponential factorization. Set of primes, as well as the set of natural numbers, is infinite set. Consequently, complexity of revealing of all members of set of primes by means of AKS-algorithm is limited to nothing from above too.

“Point” polynomial test AKS is intended for revealing only the fact of primality of presented natural number, without the information on the nearest primes. From here there is the second, much more important question: how does this algorithm transform to the unconditional universal polynomial determined tool (to the formula, algorithm etc.) which would allow analytically, “on a pen tip”, to own all set of primes? Which would allow to apply this set and functional dependences working in it in any mathematical constructions and calculations?

This can be told also about any future similar “point” primality algorithms: its essentially can not make accessible the set of all primes even if its are polynomial.

On January 2013 mankind has known tens of millions of first primes, the biggest of them, the 48th Mersenne prime, consists of 17 425 170



decimal figures. If all previous primes are known, than this prime defines the threshold of predictability for the set of all primes at January, 25, 2013. Let's notice also, that for this prime the operating time of the polynomial algorithm AKS evidently show absence of identity between concepts "polynomial" and "effective".

The name of article [1] has some linguistic ambiguity: "Primes is in P". More exact would be "Any separately taken prime is in P". Because [at present time] all set of primes in whole is inaccessible to the detached onlooker – i.e., in terms of the authors, "The set of all primes is in NP".

8.2. A regularity that determines primes: from point of view of prime's external image

From the external unbiased point of view a randomness of primes is more than obvious: the graph of their arrangement externally looks as typical "casual histogram" (as a set of sizes which does not dependent on neighbours, Figures 15, 16).

There is a great resemblance of this histogram with graphs that illustrate the independent variables or the appearance of the goal function in NP-complete task TSP (Figures 17, 18).

Each value of the independent variable "not forbidden tree edge" in TSP (i.e. coordinates and length of separately taken edge) represent one independent variable. Not one separately considered value of any independent variable, namely a separate independent variable which has the unique value.

Here the similarity, most likely, comes to an end:

In each individual case of the general problem TSP independent variables are dictated at the desire by the user of algorithm of its decision. Therefore these variables are absolutely arbitrary and in general case do not depend from each other.

Figuratively speaking independent variables in Fpr dependence are "dictated" by the oracle whom by definition everything is available that exists. Therefore it is impossible to exclude that the oracle (i.e. the nature) for creation of any prime number by means of, for example, set N of natural numbers uses certain composition of "compact analytical" dependences:

$$Fpr(N) = fpr_2(fpr_1(U))$$

Perhaps, fpr_1 , fpr_2 and U argument are available. But now the detached onlooker doesn't know

anything about them: until the proof, for example, of Riemann hypothesis.

8.3. Trifling point of view

These or those kinds of a "quantity" phenomenon eventually are formed by natural numbers. The rational decimal number can be presented in the form natural if to move a decimal point as much as possible to the right, irrational – as natural with an infinite number of figures, complex – as two-dimensional rational, whole negative – by means of a natural and conventional sign "always to subtract this number from other numbers", etc.

Therefore, any forms of quantity can be also considered as value of certain as much as bulky composition of dependences where the role of "initial" arguments is played by prime numbers.

We will assume that a certain regularity of Fpr which form certain quantities to all without exception primes (i.e. expresses primes through other primes). Let's say that marsh feats of Myunkhgauzen are impossible only within physics. But it only aggravates a problem: where should we look for such "prime numbers arguments" and what to do if they are set members of an uncontrollable infinite set?

Note: Very strong argument of that Fpr will be included in a mathematics arsenal sooner or later: just as a huge number of physical dependences are successfully modelled by means of virtual mathematical models, Fpr dependence, perhaps, sooner or later will be successfully simulated by means of any other mathematical model without direct participation of primes.

Counterarguments apropos of "other" model are very weak, but are rather obvious. From "where a guarantee that such virtual analytical and quantitative constructions are completely adequate to the deep nature hopelessly initial and the slippery modelled phenomenon "prime numbers" if they don't lean on this phenomenon" – to "the best mathematicians are engaged in it at least 2300 years, they could find this "a black cat in the dark room" a long time ago.

See figure 17-18 in the appendix



8.4. Regularity that defines composite numbers: from the point of view of an internal structure of composite numbers

The size of composite numbers is dictated by quantity and size of these or those prime numbers. Prime numbers correspond to ruptures of Fcs regularity which defines all composite numbers (i.e. to the facts of Fcs values absence on an axis of natural numbers).

It is logical to assume that the absence fact (the fact of a limit minimality) of positive number corresponds to the fact of existence of zero. The last makes to remember not trivial zero of Riemann zeta function.

Theorem 1: Regularity Fcs that determines all composite numbers, represents infinite set of different and in general case not depended from each other functions.

Proof: a) Any composite number cs_i is product of k primes. This product can be considered as unique set acs_i , consisting of k factors.

b) Change of power of acs_i or/and of size of even one its set member necessarily changes size of cs_i : of i -th value of regularity $Fcs(Pr)$. It means, that each set member of the set acs_i is an independent variable of some dependence $fcs_i()$:

$$cs_i = fcs_i(acs_i)$$

$$Cs = \{cs_1, cs_2, \dots, cs_i, \dots\}$$

$$Cs = \{fcs_1(acs_1), fcs_2(acs_2), \dots, fcs_i(acs_i), \dots\} = \{Fcs_1(Pr), Fcs_2(Pr), \dots, Fcs_k(Pr), \dots\} = Fcs(Pr)$$

here: $i=1, 2, 3, \dots$ – serial number in the set Cs of composite numbers

Pr – the set of primes

c) All sets acs_{kt} , consisting from k factors are possible to unit in infinite set Acs_k :

$$Acs_k = \{acs_{k1}, acs_{k2}, \dots, acs_{kt}, \dots\}$$

here: $t=1, 2, \dots$ – serial number in the set Acs_k

$$k = |acs_{k1}| = |acs_{k2}| = \dots = |acs_{kt}| = \dots$$

d) It doesn't demand the proof that only obviously different functions can have different amount of arguments. In other words, each of the Fcs_k functions differs from any other such function:

$$Fcs_1(Pr) \neq Fcs_2(Pr) \neq \dots \neq Fcs_k(Pr) \neq \dots$$

Each of the Fcs_k functions doesn't depend on none of such function: otherwise they could be expressed one through another and to be the one Fcs function. Therefore, Fcs regularity which defines all composite numbers, represents a set of the different and not depending from each other Fcs_k functions:

$$Fcs = \{Fcs_1, Fcs_2, \dots, Fcs_k, \dots\}$$

e) Each Fcs_k defines k infinite subset of unknown distributed composite numbers. All these numbers are unique product of k of prime numbers.

f) The set “regularity Fcs” is infinite set:

$$|\{2 + 3 + \dots + k + \dots\}| = \infty$$

and so

$$|Fcs| = |\{Fcs_1, Fcs_2, \dots, Fcs_k, \dots\}| = \infty$$

Consequence 1: The set Cs of all composite numbers is the disordered set.

Consequence 2: Any composite number is an unique set member of disordered set Cs even if it is a set member of any ordered subsets of the set Cs simultaneously.



Comment: There is, for example, the infinite quantity of the ordered subsets which submit to dependences of a kind “this composite numbers share on pr”, where $pr > 1$ is any prime.

8.5. A regularity that determines composite numbers: from the point of view of reality, which combinatorics studies

Validity of the statement considered above is possible to show in another way (designations – see the theorem 1):

Theorem 2: Regularity Fcs that determines all composite numbers is the disordered regularity

Proof: a) Any composite number cs_i can be considered as an unique combination with repeating elements of k primes.

b) Each set member of a set Acs_k is formed by the same rule of combinatorics – with the help of “combinatorial” dependence $f_k(Pr)$:

$$Acs_k = \{acs_{k1}, acs_{k2}, \dots, acs_{kt}, \dots\} = \{f_k(Pr_{k1}), f_k(Pr_{k2}), \dots, f_k(Pr_{kt}), \dots\}$$

$$Pr = \{Pr_1, Pr_2, \dots, Pr_u, \dots\}$$

here: Pr_u – finite subsets of primes (the fact of their necessity puts accessibility of Fcs under doubt)

c) Different sets Acs_k form different rules of combinatorics:

$$Acs_k = \{acs_{k1}, acs_{k2}, \dots, acs_{kt}, \dots\} = \{f_k(Pr_{k1}), f_k(Pr_{k2}), \dots, f_k(Pr_{kt}), \dots\}$$

$$Acs_r = \{acs_{r1}, acs_{r2}, \dots, acs_{rs}, \dots\} = \{f_r(Pr_{r1}), f_r(Pr_{r2}), \dots, f_r(Pr_{rs}), \dots\}$$

$$k \neq r, Acs_k \neq Acs_r, acs_{kt} \neq acs_{rs}, f_k(Pr) \neq f_r(Pr)$$

d) Different functions $Fcs_k(Acs_k)$ can be considered as function compositions which contain different “combinatorial” dependences:

$$Fcs_k(Acs_k) = Fcs_k(f_k(Pr))$$

$$Fcs_r(Acs_r) = Fcs_r(f_r(Pr))$$

$$f_k(Pr) \neq f_r(Pr)$$

e) Hence, each function $Fcs_k(Acs_k)$ differs from any other such function:

$$Fcs_1(Acs_1) \neq Fcs_2(Acs_2) \neq \dots \neq Fcs_k(Acs_k) \neq \dots$$

f) Each Fcs_k does not depend on one other such function: otherwise it would be one function Fcs. Therefore, regularity Fcs is irregular:

$$Fcs = \{Fcs_1(Acs_1), Fcs_2(Acs_2), \dots, Fcs_k(Acs_k), \dots\}$$

g) Fcs is infinite and therefore inaccessible set:

$$|\{2 + 3 + \dots + k + \dots\}| = \infty$$

$$|Fcs| = |\{Fcs_1, Fcs_2, \dots, Fcs_k, \dots\}| = \infty$$

h) Any irregular and simultaneously inaccessible regularity by definition is the disordered regularity.

Character of function graph of Fcs (for $|Acs| = 2$) illustrates figure 14.

8.6. Internal structure of the regularity that determines primes

Theorem 3: The regularity Fpr that determines all primes is the disordered regularity.



Proof: a) Sizes of composite numbers (all of them are determined by regularity Fcs) are a certain function f_{cs} from sizes of primes (all primes are determined by regularity Fpr):

$$Fcs = f_{cs}(Fpr)$$

b) Hence, there is an inverse function:

$$Fpr = f_{cs}^{inv}(Fcs) = f_{pr}(Fcs)$$

c) A structure, properties and behaviour of function (dependence) f_{pr} now have no basic value. Only the fact that f_{pr} somehow unequivocally displays set members of the Fcs in set members of the Fpr is important, i.e. regularity Fcs is the only independent variable of the regularity Fpr.

d) The regularity Fpr is fair to consider as composition of function f_{pr} and function Fcs.

e) According to theorems 1 and 2 regularity Fcs is irregular set. Domain of Fcs has not one, but $|Fcs|$ of the ranges (Figure 6).

f) The amount of independent regularities in composition of dependences can't decrease just because they are independent. Therefore if in any composition at least at one irregular dependence F range of definition consists of the M ranges, composition is an irregular set whose power at least is equal to $|F| = M$ (Figure 10).

g) Therefore, Fpr regularity represents a set of certain different and in general case independent from each other functions $Fpr_j, j=1, 2, 3, \dots$, i.e. is irregular regularity.

h) Fpr is infinite set:

$$|Fpr| \geq |Fcs| = \infty$$

i) Irregular infinite regularity is always inaccessible to the detached onlooker.

j) Any irregular inaccessible regularity by definition is the disordered regularity.

Consequence 3: The set Pr of all primes is the disordered set.

Consequence 4: Any prime is a unique set member of disordered set Pr even if it is a set member of any ordered subsets of set Pr simultaneously.

Comment: The oracle (i.e. the nature) for creation of any primes uses ultimately composition of two dependences which are not neither compact, nor analytical:

$$Fpr(N) = f_{pr2}(f_{pr1}(U)) = f_{pr}(Fcs(U))$$

Dependence $f_{pr2} = f_{pr}$ is disordered: its argument is the disordered dependence $f_{pr1} = Fcs$.

Note: The same regularity by definition can not be simultaneously ordered and disordered. In the case with composite numbers traditional representations about absolute omnipotence of convenient (i.e. ordered) functions isn't confirmed: existence of a certain compact analytical dependence which traces all values of [disordered] Fcs regularity, would mean at least, that all composite numbers are values of an accessible set of the functions having identical quantity of independent variables. But it not so.

As one would expect from the definition of concept "composite number", argument U of dependence Fcs is disordered set Acs of unique subsets Acs_j of primes:

$$U = Acs$$

8.7. Complexity of the regularity that determines primes

Theorem 4: Any algorithm using regularity Fpr which determines primes, has infinite complexity.



Proof: a) According to the theorem 3 regularity Fpr is infinite set of different and not depended from each other functions:

$$Fpr = \{Fpr_1, Fpr_2, Fpr_3, \dots\}$$

$$|Fpr| = |\{Fpr_1, Fpr_2, Fpr_3, \dots\}| \sim |Pr| = \infty$$

b) Complexity of any ALG algorithm is always directly proportional to the sum of complexities of all those ALG_j algorithms

which aren't depending from each other and which allow to achieve all those objectives for which ALG is intended:

$$ALG = \{ALG_1, ALG_2, ALG_3, \dots\}$$

$$O(ALG) = O(\{ALG_1, ALG_2, ALG_3, \dots\}) \sim O(ALG_1) + O(ALG_2) + O(ALG_3) + \dots$$

here: O(ALG_j) – complexity of algorithm ALG_j

O({ALG}) – complexity of set of algorithms

c) Complexity of any ALG algorithm using F regularity is always directly proportional to quantity of all those undepended from each other F_j dependences, which form F regularity.

$$O(ALG(F)) = O(\{ALG_1(F_1), ALG_2(F_2), ALG_3(F_3), \dots\})$$

$$O(ALG_j(F_j)) \sim |F_j|$$

$$O(ALG(F)) \sim (|F_1| + |F_2| + |F_3| + \dots) \sim |\{F_1, F_2, F_3, \dots\}|$$

here: ALG_j(F_j) – algorithm which uses dependence F_j

d) Therefore, complexity of any ALG(Fpr) algorithm which will use Fpr regularity, can have only infinite complexity:

$$|Fpr| = |\{Fpr_1, Fpr_2, Fpr_3, \dots\}| \sim |Pr| = \infty$$

$$O(ALG(Fpr)) = O(\{ALG_1(Fpr_1), ALG_2(Fpr_2), ALG_3(Fpr_3), \dots\}) \sim (|Fpr_1| + |Fpr_2| + |Fpr_3| + \dots) \sim |\{Fpr_1, Fpr_2, Fpr_3, \dots\}| = \infty$$

Comment: Regardless of the fact that Fpr represents also algorithms which successfully use Fpr, in a set of all prime numbers there will be a predictability threshold. This circumstance influences on the minimum complexity of such algorithms.

Research or use of an irregular set represents at best some few “geodesist’s tasks”. In the worst (including for the disordered set of all prime numbers) – “the Cinderella’s task” whose successful decision in general case is possible only by means of exponential exhaustive method.

8.8. An irremovable property of the set of all primes

Obvious proposition: The set of all primes is fundamentally impossible to separate from the set of all composite numbers.

It is impossible to speed up process of separation of sets Pr and Cs: each of infinite quantity of odd numbers which will not be eliminated at once on the basis of divisibility, separately is necessary to analyse by some algorithm of primality.

It is obvious and quite explained full (except for quantity of chemical elements) analogy between set of natural numbers and variety of all chemical substances in the nature: primes correspond to chemical elements, powers of primes – to elementary substance, products of different primes – to chemical compounds.

8.9. Optimistic point of view

Conclusion from all the above:

The set of primes is inaccessible to the detached onlooker.



In other words, the regularity Fpr exists in the nature (exists for the oracle by definition): but does not exist for the detached onlooker (because Fpr has infinite complexity).

But let's assume the opposite. Supposing (although it raises some doubts) that we know all, without exception, primes from number 2 to the 48th Mersenne prime. We admit, that the "casual histogram" is only external erroneous impression. Already found rules between set members of some subsets of primes can serve as indirect confirmation of it. Let's assume, that in one fine day the problem "primes" at last has solved: certain absolutely ingenious regularity Fpr (law, dependence, formula, algorithm etc) is found to which all primes submit now.

The first question which will arise right after it: how does to prove that this regularity (for example, best in all senses Riemann hypothesis) is fair also for all other primes? Including for what are behind a threshold of predictability for set of primes? Is this statement true, that this law supervises those primes which size we haven't known yet? Including those which sizes we will never learn?

9. IN CLOSING

The initial cause of all difficulties connected to primes is the nature of set of primes:

1) Regularity Fcs which determines all composite numbers, is set which consists of the infinite quantity different and not depended from each other elementary arithmetic functions.

The reason of such structure of Fcs: set members of the set "regularity Fcs" have different quantity of independent variables (see sections 8.4, 8.5.).

2) Fpr regularity which defines all prime numbers, is a set which consists of an infinite number of the different and not depending from each other functions. It isn't excluded that some (or even all) such functions have a unique value: size of a prime number.

Reason of such structure of Fpr: the disordered Fcs regularity can be considered as argument of Fpr regularity. Initial absence of a controlled order in argument inevitably makes disordered values of the function (section 8.6.).

3) Complexity of Fpr regularity is equal to infinity. It makes a set of all prime numbers inaccessible to the detached onlooker both from the point of view of utilitarian use of this set, and from

the point of view of check of adequacy of any mathematical models for Fpr. Such situation is characteristic for many other infinite and materially-infinite sets (sections 8.7, 8.9.).

4) The set of all primes cannot be separated from the set of all composite numbers (section 8.8.).

Comment: Possibly, the reason of some theoretical difficulties with primes in the following: primes eventually form not only any other quantities, but also any quantitative dependences – the last always arise naturally where there is a fact of existence of at least two quantities. And than this or that theoretical difficulty is farther from the above-mentioned initial cause, more respectable and problematic a formal description and overcoming of this difficulty becomes.

The classical technique of detection of the mathematical regularity existing in the nature applied almost since the time of Pythagoras ("a black cat in the dark room") consists of two main parts:

a) The reliable not determined proof of the fact of existence of unknown regularity – regularity Fpr is "black cat" in our case.

b) Definition of required properties of this regularity.

In the case with primes the situation is not classical:

a) The statement "everything exists in the nature, including certain for all prime numbers regularity of Fpr", is so indisputable and trivial as it is useless.

b) Accessibility of regularity Fpr: that is the question. Fpr is sprayed to fragments, each of which defines the subset of prime numbers or, perhaps, the prime number. A problem is that "the black cat" is not in one, and at the same time in an infinite set unpredictably located independent "dark rooms". The most distant, but not the last from them (according to information for 2013) was with very big expenses of time and energy found on January 25, 2013.

10. ADDITIONAL NONSTRICT OBSERVATION: ABOUT THE PHENOMENA "QUANTITY", "THE MOST GENERAL CASE OF A MATHEMATICAL TASK (MATHEMATICAL PROBLEM)" AND "PARTICLE, WHICH IS A WAVE"



Any as much as complex virtual model of a reality by definition simulates no more than a side of this reality seen from some point of view. Sometimes even the elementary sketches of such models make appreciable curious (though also disputable enough) analogies between observably properties of completely different entities: for example, between some properties of primes, tasks of class NP and ultimate particles.

10.1. Primes

The paradox in the fact that discovery of regularity Fpr will be able to change nothing neither in the field of the theory, nor in the field of practice:

It is very difficult to find this regularity. But justice of this regularity (even if known primes submit to it all without exception) can't be checked (it is impossible to prove) for as much as large primes.

Frivolous hypothesis: possession of Fpr regularity would be equivalent to opportunity to operate not only all simple (and others) numbers, but also all without exception dependences which are a natural consequence of existence fact of these or those numbers. But the second (and, therefore, the first) is impossible.

10.2. Primes and “P versus NP” problem

If the hypothesis of discrepancy of classes of complexity of P and NP is fair (i.e. if the problem of “P vs NP” is solved as “ $P \neq NP$ ”) then is found a certain relationship of problems “primes” and “P vs NP” [5], [10], [16], [21]. And the second of these problems looks more harmless, especially – against well known informal definition of tasks of the class NP:

The [exact] answers of tasks of class NP are very difficult to find. Soundness of a received [by some way] allowable answer of a task of class NP is easy to check.

Classical hypothesis: possession of effective algorithm of the exact solution at least of one NP-complete task would be equivalent to possibility of the exact solution of all tasks (problems) of the NP class. But it is impossible.

The reason of such state of affairs for primes and for answers of tasks of class NP is the same – the fundamental uncontrollability (disorder) of these sets in general case easily wins inevitable finiteness

(limitation) of physical possibilities (“resources”: space, time, energy etc.) of the detached onlooker.

Disorder of prime numbers can be considered as a result of demonstrable disorder of composite numbers (the case of “infection with irregularity” of analytical dependence between composite and prime numbers which has infinite complexity). And disorder of a set of possible answers of any NP-complete task – as a result of obvious irregularity of a set of arguments in such tasks (there is “an infection with irregularity” of “combinatory” dependence which turns a polynomial set of parameters of arguments into an exponential set of parameters of possible answers).

For obvious reasons of irregular sets should be much larger than regular sets. The regularity is no more than a convenient special case of irregularity. We can also assume the same thing about mathematical and other problems that are the consequences of the existence of unmanaged irregular (i.e. disordered) sets.

10.3. Primes, NP-complete tasks and the strangeness of the quantum world

Impressions of the ingenuous layman: the picture becomes even more full and logical if you recall the phenomenon of uncertainty in quantum mechanics (about the Heisenberg's uncertainty principle).

The first line of curious analogies:

- a) an unknown prime;
- b) the unknown exact answer of a task of class NP;
- c) an ultimate particle.

The second line:

- a) discrete set of primes;
- b) discrete set of possible combinations of values of variable of a task of class NP;
- c) discrete structure of energies and spaces (quants of energy, electron's orbits, natural harmony of crystal lattices etc).

The third line:

- a) “the uncertainty principle for primes”: it is impossible to determine value of unique coordinate of required prime in that virtual one-dimensional space (it is an axis of natural numbers) where there is this prime number.



b) “the uncertainty principle for tasks of class NP”: it is impossible to determine simultaneously all r values of r coordinates of the required exact answer of this task in that virtual r -dimensional space (it is the Cartesian product of all discrete sets “the independent variables”) where there is this exact answer.

c) Principle of uncertainty of Heisenberg: it is impossible to define at the same time values of all spatial coordinates and an impulse of the considered elementary particle in that virtual space (it is created, in particular, by spatial coordinates and coordinate particle “impulse”) where this particle is.

10.4. Environment?

Possibly, “inconvenient” properties of elementary particles to some extent can be explained first of all with discretization of the environment of their existence and those “inconvenient” features of laws of combination theory to which such environments have to submit.

As is known, in the quantum world the particles have simultaneously properties of a particle and of a wave. Any wave phenomena by definition are possible only in some environment. Against associations with transverse or longitudinal waves such institutional objects are defined much better with the name “point wave”.

The primitive two-dimensional mechanical analogy – the infinite plane matrix in which cells domino stones stand vertically. Each stone on this field at external influence bends, surely hits top of the next neighbor and reverts to the initial state of rest.

Easy click on top of any stone gives unexpectedly familiar picture: across the field flies, like a photon in interstellar emptiness, local indignation (“point wave”). This gradually dying away in material (and therefore viscous) circumference indignation (“relay- race of transfer of change”) moves as a particle: strictly in a straight line in the direction of initial click where stones stand on the horizontal plane, and on a curvilinear orbit where the plane is bent like gravitational distortions of physical space.

At a meeting with a place where there are no stones (if they are model of estimated property of “vacuum”, their absence corresponds to model of “vacuum” of an obstacle, impenetrable for this version), indignation particle moves where it is possible (i.e. on the existing stones) and therefore

bends around an obstacle in full accordance with the wave phenomenon “diffraction”.

If the group of stones to deprive of opportunity to bend, there is a model of absolutely black body. If these stones react to influence from the outside an inclination towards this influence, they will turn into exact similarity of a mirror or other reflecting surface.

If for any reason indignation was transferred at the same time, for example, to two stones, there can be a bifurcation of a indignation orbit. If to forget that the particle not tiny “bullet” from substance, and only a relay-race spike, capable to replication and disappearing, the detached onlooker will find paradox: the particle at the same time is in two different points of physical space.

The extremity greatest speed possible in the world (to velocity of light) specifies also that even vacuum isn't the primitive fact of absence of everything. Especially as involuntary working assumption: perhaps, the vacuum is a circumference which because of the viscosity can't move any changes quicker, than with a speed of 299 792 458 m/s.

If we assume that the external source of indignation of balance (in the considered model it is the moment of click on stones) is able to move with greater speed, consequences of its influence on surrounding all the same won't be able to extend in the environment quicker, than it is offered by A. Einstein's theory. In other words, for the world known to us there are no objects with heretical speeds: here they can't be registered.

Irregularity is the lack of a uniform regularity. Accident is a regularity that inaccessible for detached onlooker. Chaos is the irregular accident.

The most important feature of environments in which there are phenomena “prime”, “exact answer of a task of class NP” and, probably, “ultimate particle” is essentially ineradicable chaos in discrete sets with arbitrarily large quantity of set members.

11. CONCLUSIONS

1. Many statements about a regularities in the set of primes (and the Riemann hypothesis) are fair for properties of these or those subsets and groups of subsets of primes. Some statements – even for the entire infinite set of primes.

2. But any statements about regularity that determines the sizes of all primes, including the



Riemann hypothesis, in principle cannot be proven strictly and absolutely trustworthy.

3. Taking last circumstance into consideration it can appear not less fruitful, than a support on the assumption of accessibility for the detached onlooker even one of those laws whom all without exception “atoms of quantity” submit to.

REFERENCES:

- [1] Agrawal, M., Kayal, N. & Saxena, N. (2008). *Primes is in P*. Retrieved from www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf
- [2] Albeverio, S. & Cacciapuoti, C. (2011). *The Riemann zeta in terms of the dilogarithm*. Retrieved from <http://arxiv.org/pdf/1101.4786v2.pdf>
- [3] Ares, S. & Castro, M. (2003). *Hidden structure in the randomness of the prime number sequence?* Retrieved from www.arxiv.org/abs/cond-mat/0310148v2
- [4] Avigad, J., Donnelly, K., Gray, D. & Raff, P. (2005). *A formally verified proof of the prime number theorem*. Retrieved from www.arxiv.org/abs/cs/0509025v3
- [5] Barrón-Romero, C. (2010). *The Complexity Of The NP-Class*. Retrieved from www.arXiv.org/abs/cs.LG/0610221
- [6] Buhler, J. P. & Harvey, D. (2009). *Irregular primes to 163 million*. Retrieved from <http://arxiv.org/pdf/0912.2121v2.pdf>
- [7] Conway, J. H. & Guy, R. K. (1996). *The Book of Numbers*. Copernicus.
- [8] Crandall, R. & Pomerance, C. (2005). *Prime Numbers: A Computational Perspective*. Springer-Verlag.
- [9] Farkas, G., Kallós, G. & Kiss, G. (2011). *Large primes in generalized Pascal triangles*. Retrieved from <http://arxiv.org/pdf/1111.3670v1.pdf>
- [10] Fukuyama, J. (2012). *Computing Cliques is Intractable*. Retrieved from <http://arxiv.org/abs/1305.3218>
- [11] Goldston, D. A. & Ledoan, A. H. (2011). *On the differences between consecutive prime numbers, I*. Retrieved from <http://arxiv.org/pdf/1111.3380v2.pdf>
- [12] Green, B. & Tao, T. (2008). *The primes contain arbitrarily long arithmetic progressions*. *Annals of Mathematics*, 167 (2): 481–547. <http://annals.math.princeton.edu/wp-content/uploads/annals-v167-n2-p03.pdf>
- [13] Halupczok, K. (2012). *Goldbach's problem with primes in arithmetic progressions and in short intervals*. Retrieved from www.arxiv.org/math/1212.4406v1
- [14] King, C. (2011). *Fractal Geography of the Riemann Zeta Function*. Retrieved from <http://arxiv.org/ftp/arxiv/papers/1103/1103.5274.pdf>
- [15] Latorre, J. I. & Sierra, G. (2013). *Quantum Computation of Prime Number Functions*. Retrieved from <http://arxiv.org/pdf/1302.6245v3.pdf>
- [16] Malinina, N. L. (2012). *On the principal impossibility to prove P=NP*. Retrieved from www.arxiv.org/abs/1211.3492
- [17] Nuttall, J. (2011). *Determinantal approach to a proof of the Riemann hypothesis*. Retrieved from <http://arxiv.org/pdf/1111.1128v1.pdf>
- [18] Pozdnyakov, D. (2012). *Physical interpretation of the Riemann hypothesis*. Retrieved from <http://arxiv.org/ftp/arxiv/papers/1202/1202.2115.pdf>
- [19] Sabbagh, K. (2003). *The Riemann hypothesis: The Greatest Unsolved Problem in Mathematics*. Farrar, Straus and Giroux.
- [20] Schumayer, D. & Hutchinson, D. A. W. (2011). *Physics of the Riemann Hypothesis*. Retrieved from <http://arxiv.org/pdf/1101.3116v1.pdf>
- [21] Valeev, R. Ch. (2014). *“P=NP” versus “P ≠ NP”*. *Life Science Journal* 2014; 11(12s): 506-512. http://www.lifesciencesite.com/ljsj/life1112s/109_26544life1112s14_506_512.pdf
- [22] Vepstas, L. (2011). *Yet Another Riemann Hypothesis*. Retrieved from <http://arxiv.org/pdf/1101.0311v1.pdf>
- [23] Weber, H. J. (2012). *Remarkable and Reversible Prime Number Patterns*. Retrieved from www.arxiv.org/math/arXiv:1203.5227v1

APPENDIX

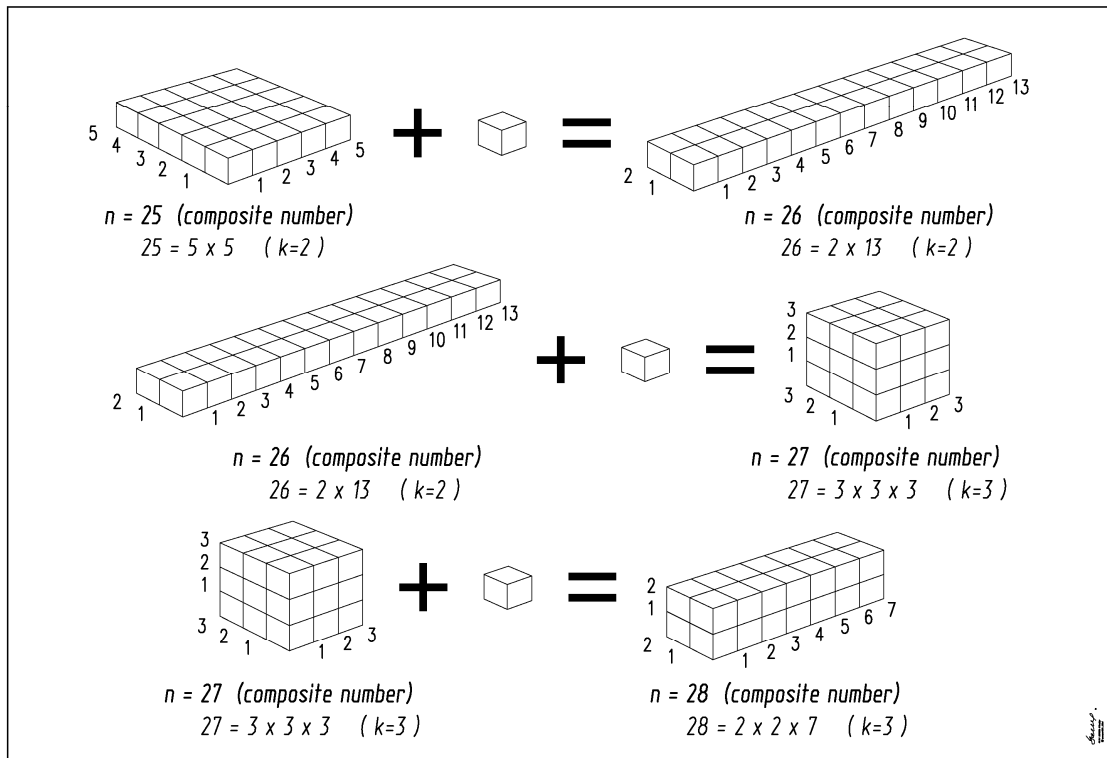


Figure 1. Representation Of Natural Numbers As Completely Filled K-Dimensional Discrete Cartesian Spaces: $N=25, 26, 27, 28$

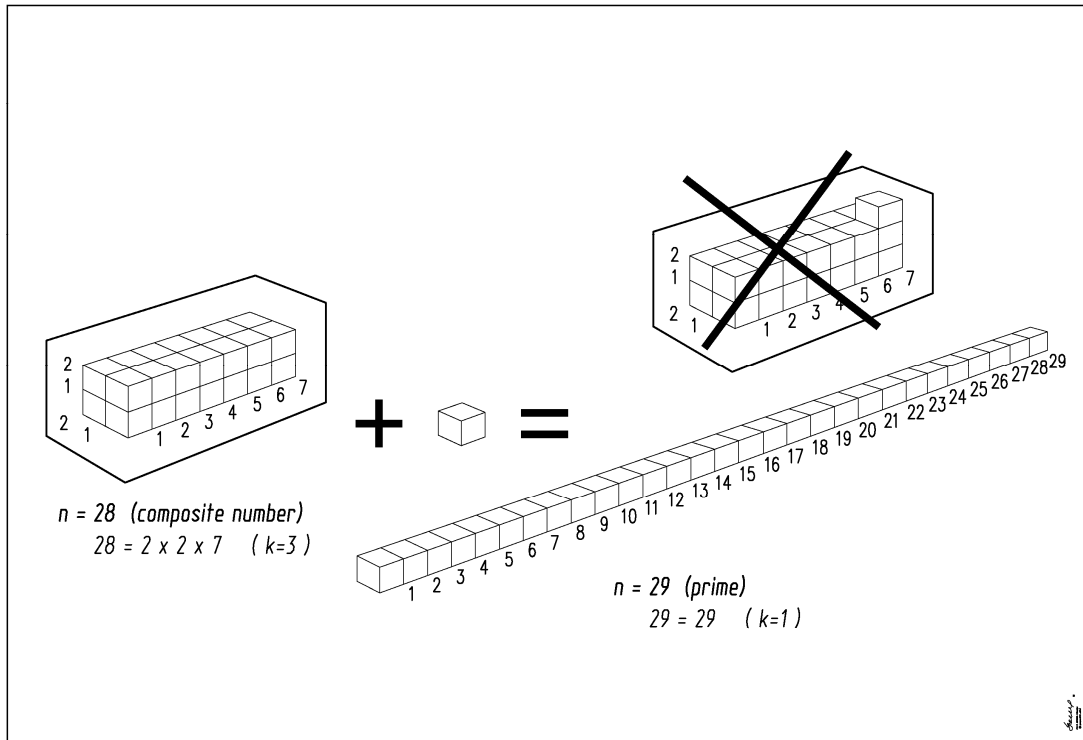


Figure 2. Representation Of Natural Numbers: $N=28, 29$

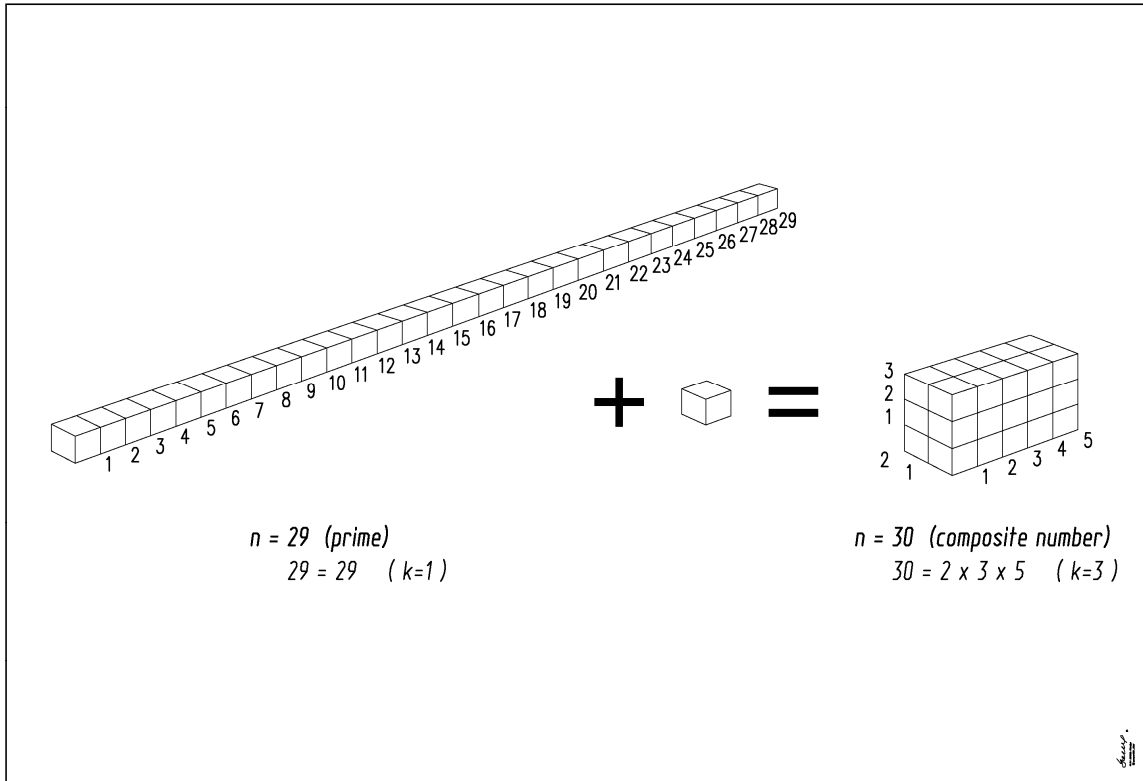


Figure 3. Representation Of Natural Numbers: $N=29, 30$

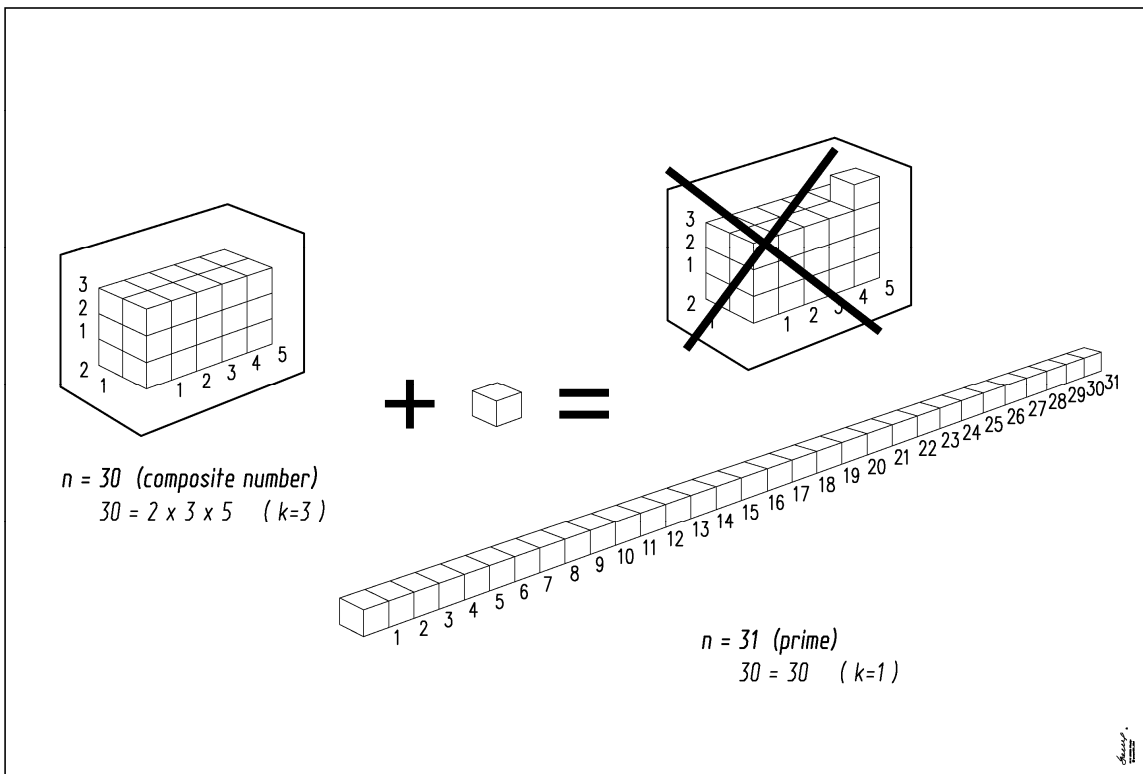


Figure 4. Representation Of Natural Numbers: $N=30, 31$

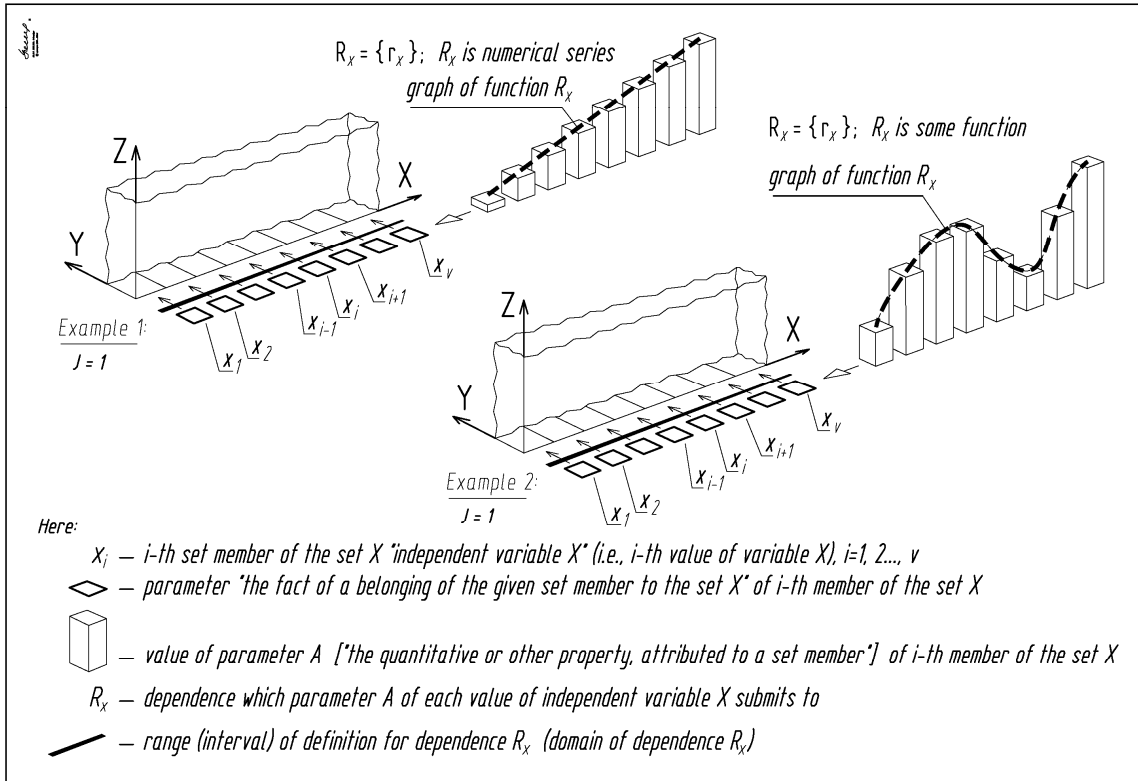


Figure 5. Regular Dependence

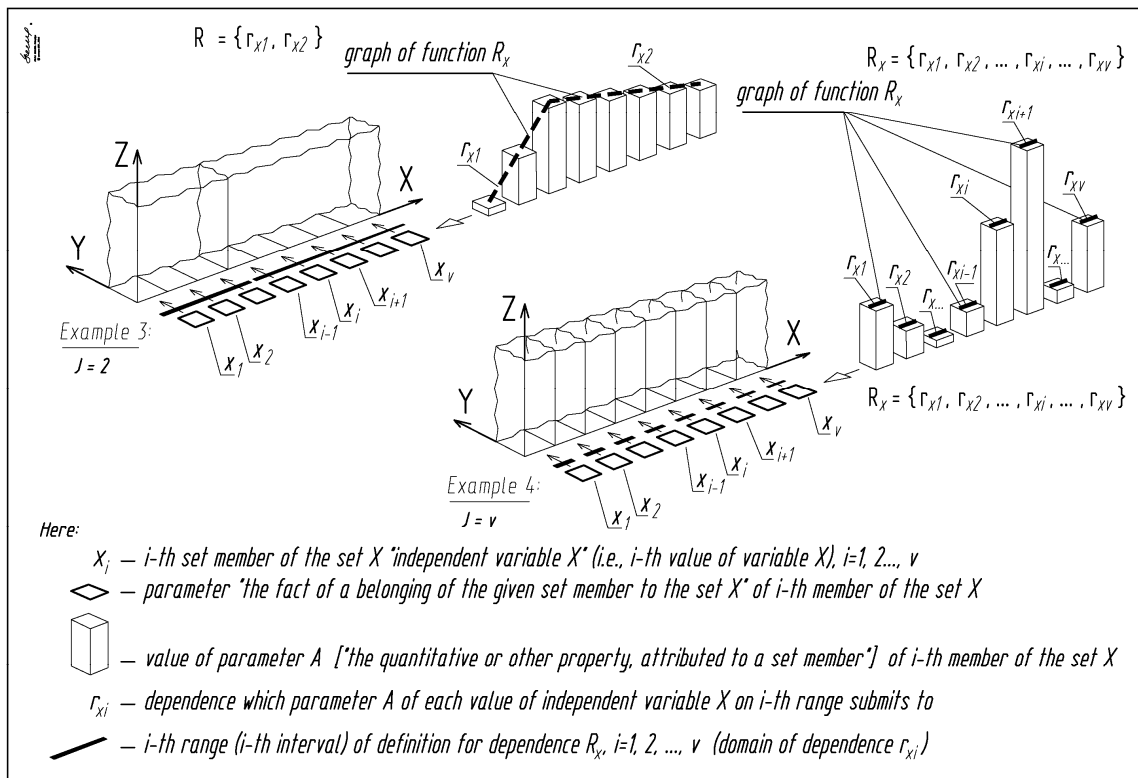


Figure 6. Irregular Dependence

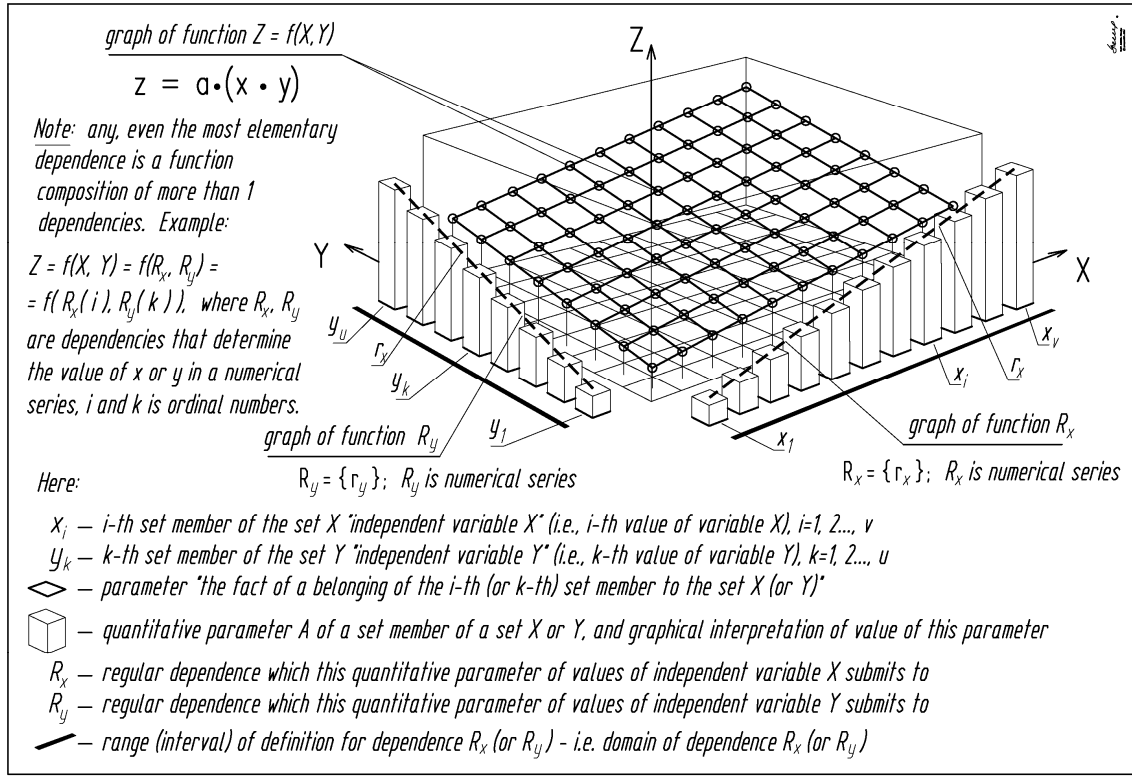


Figure 7. Composition Of Two Regular Dependencies

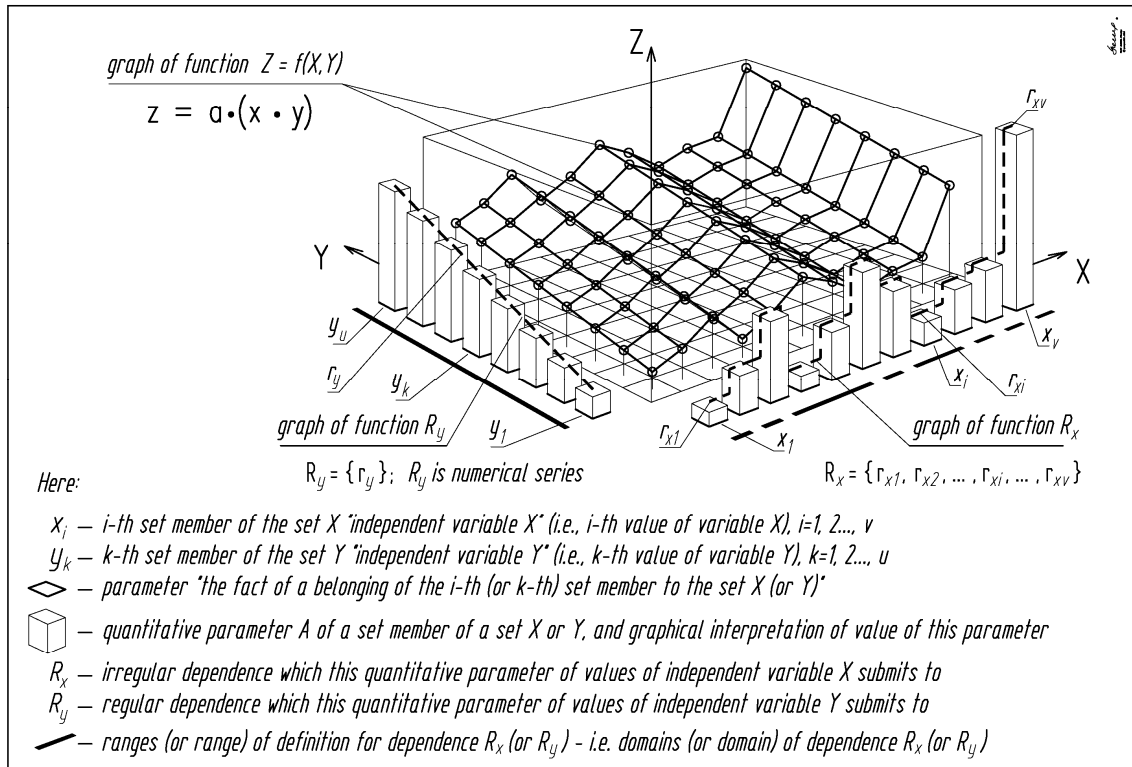


Figure 8. Composition Of Irregular And Regular Dependencies

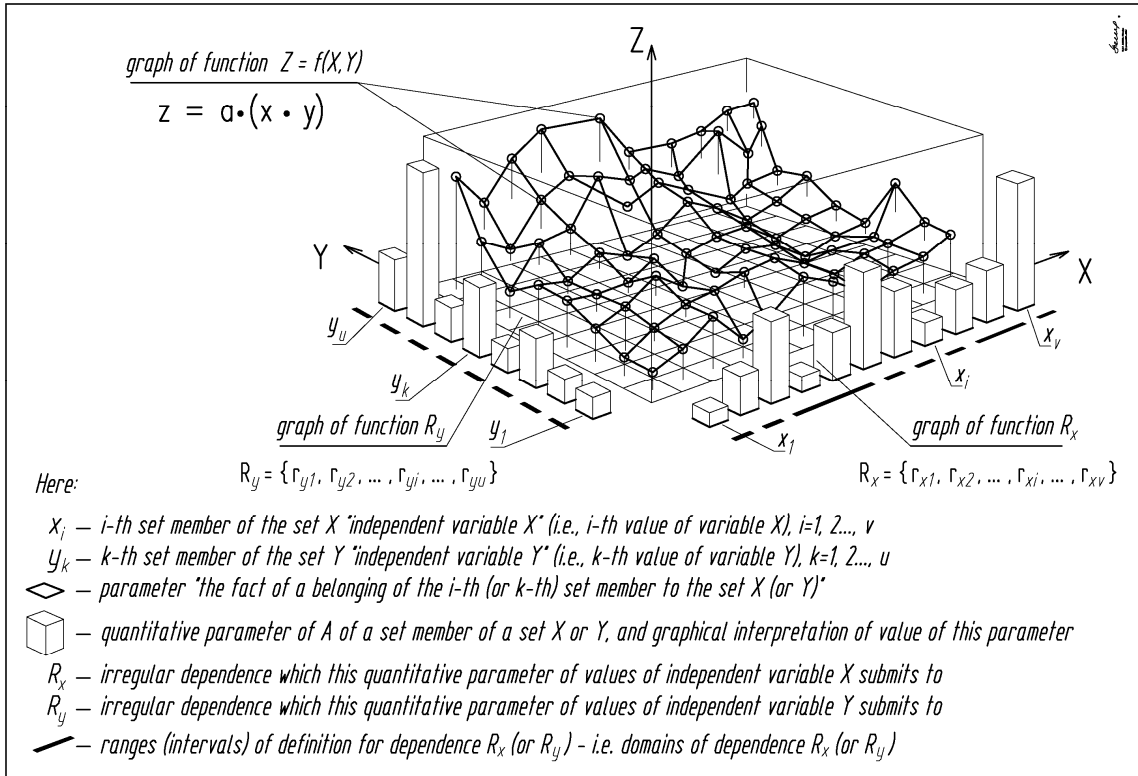


Figure 9. Composition Of Two Irregular Dependencies

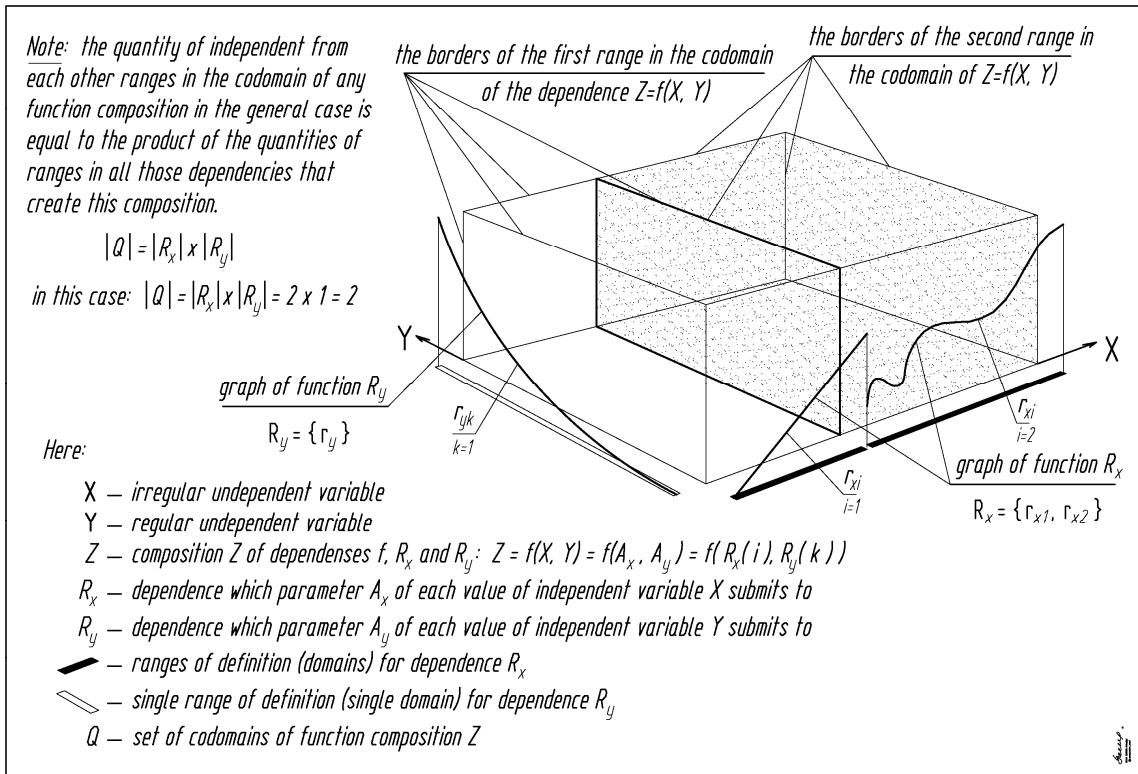


Figure 10. Codomain Of Composition Of Irregular And Regular Dependencies

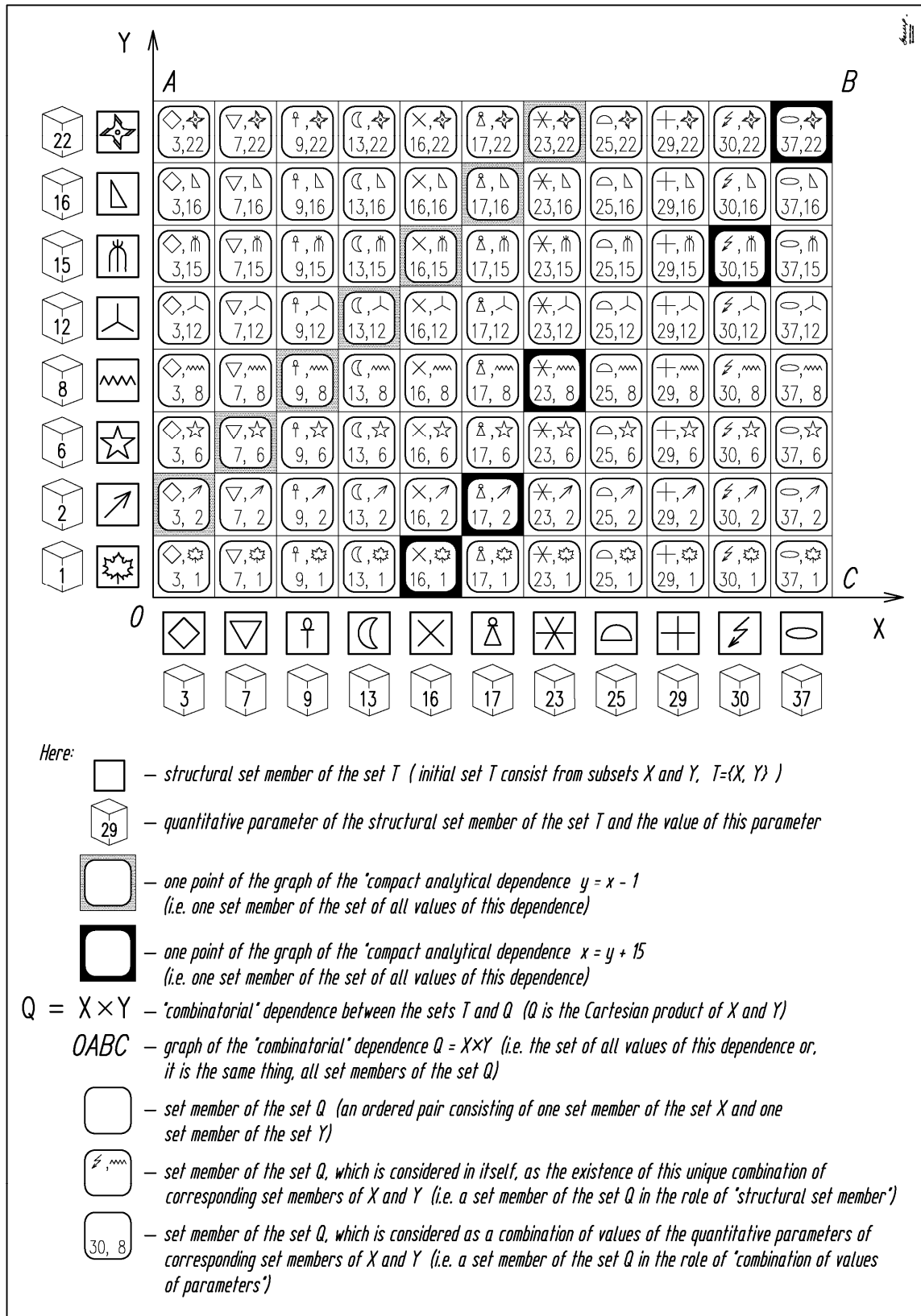


Figure 11. Distinctions Between "Compact Analytical" And "Combinatory" Dependencies

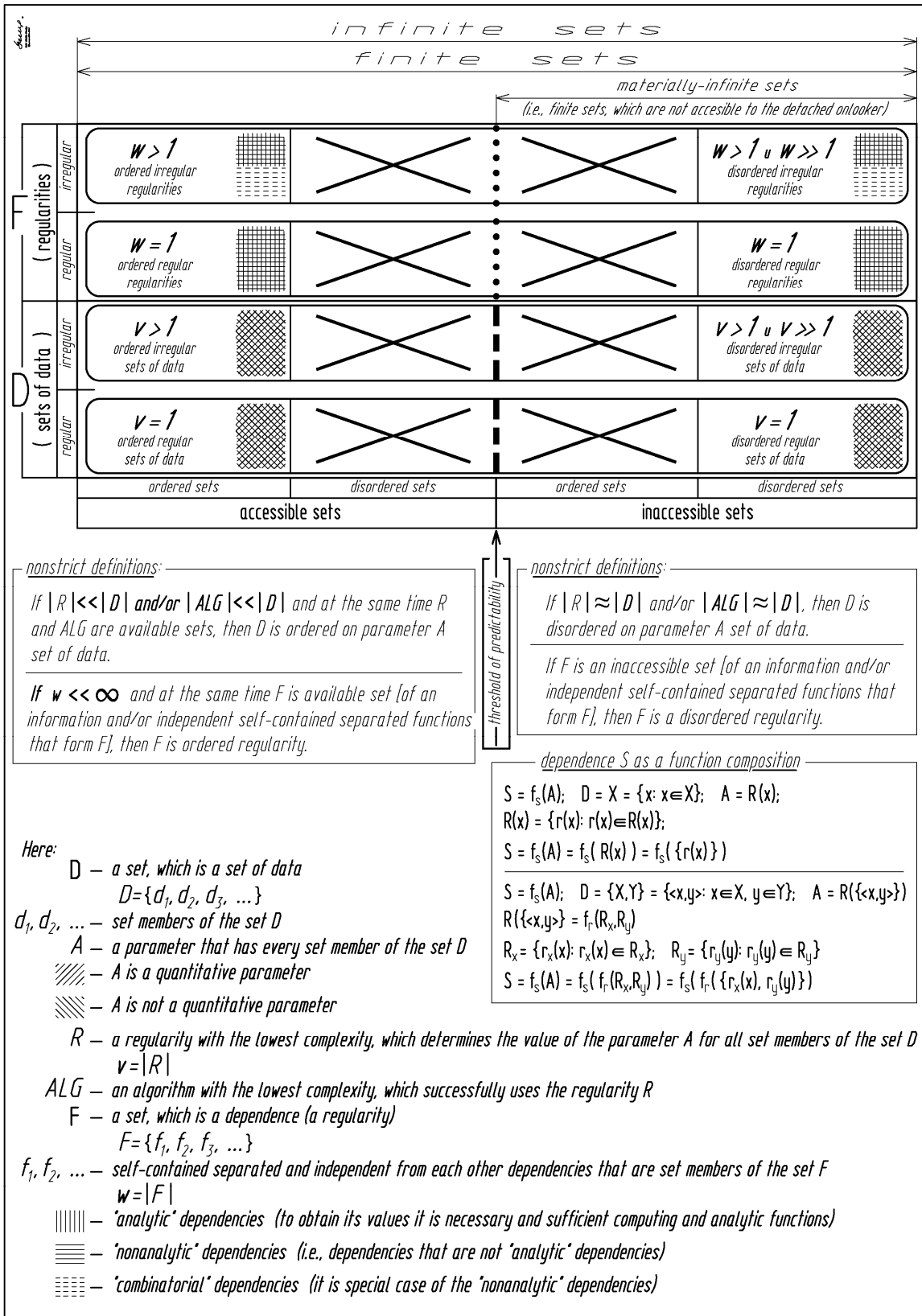
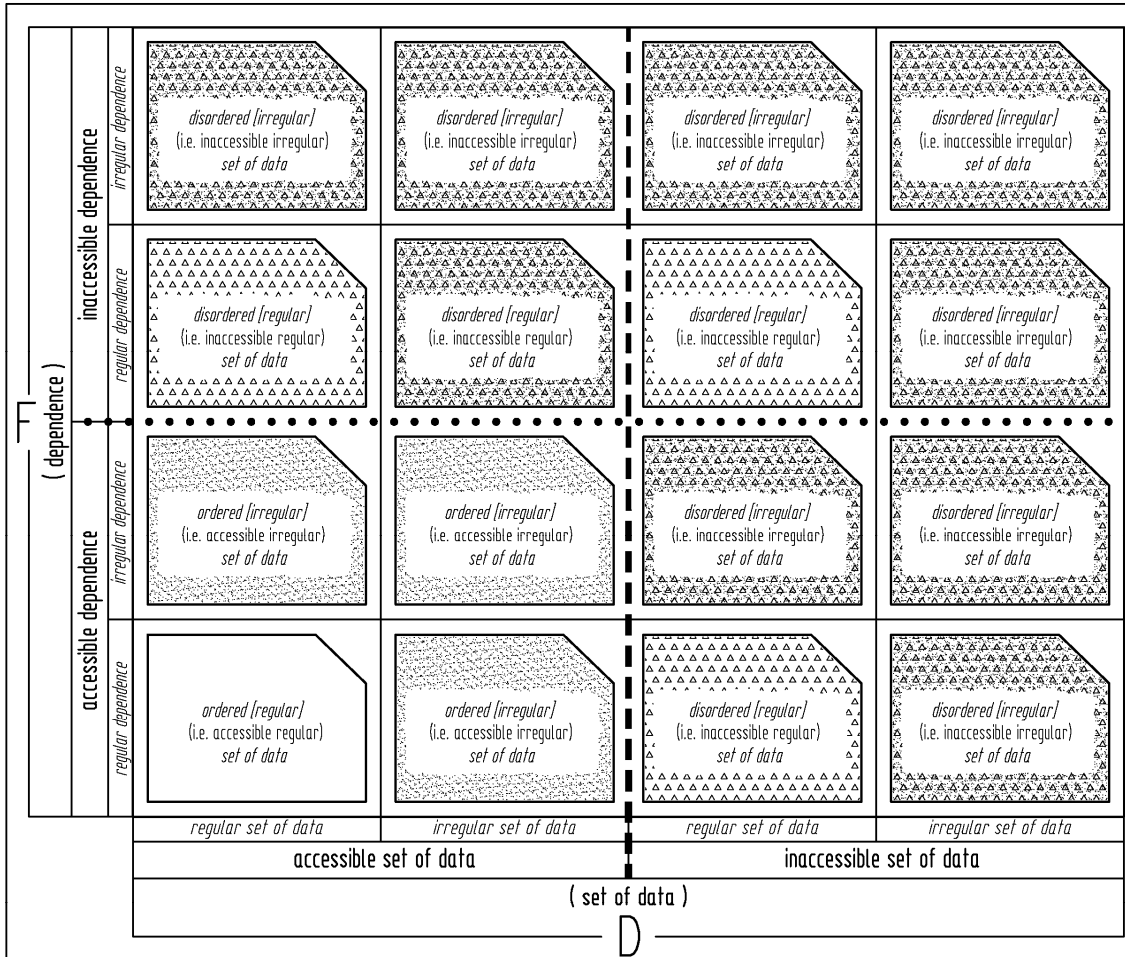



Figure 12. General Properties Of The Sets (On Parameter A)



Here:

- F – a dependence (any dependence is a set consisting of 1 or more [independent from each other] functions)
- D – a set of data (the value of the parameter A of all set members of this set determines the dependence R)
-  – codomain of a dependence S (of a function composition S), $S = F(D) = F_1(A) = F_2(R)$
- — — — — threshold of predictability of a set D on parameter A
- • • • • threshold of predictability of a dependence F on parameter "complexity of the dependence F"

Notes:

- This figure shows the "periodic table" for the simplest situations of "values of dependence F, the argument of which are some data D", i.e. for function compositions of rank 1. A similar situation is when instead of D such argument will be some other dependency. Any set of data can also be regarded as a participant in any function composition: in such cases, function as part of composition is dependence, which values of the parameter A for all set members of this set submits to.
- If in a function composition of any rank at least one its dependence is irregular on the parameter A, then comes the inevitable "contamination by irregularity": composition can also be only irregular dependence on parameter A.
- The same thing happens in cases when at least one such dependency is not accessible on parameter A: the function composition is also sure to be "infected by inaccessibility" on parameter A.
- At the same time both the irregularity and unavailability can be considered from the point of view of both quantitative and non-quantitative parameter A.
- The figure does not show numerous borderline situations that require a quantitative assessment of the complexity of the accessible dependencies and data sets. Complexities are summed up, so the composition of functions may become inaccessible.

Figure 13. Influence Of The General Properties Of An Independent Set On A Dependent Set

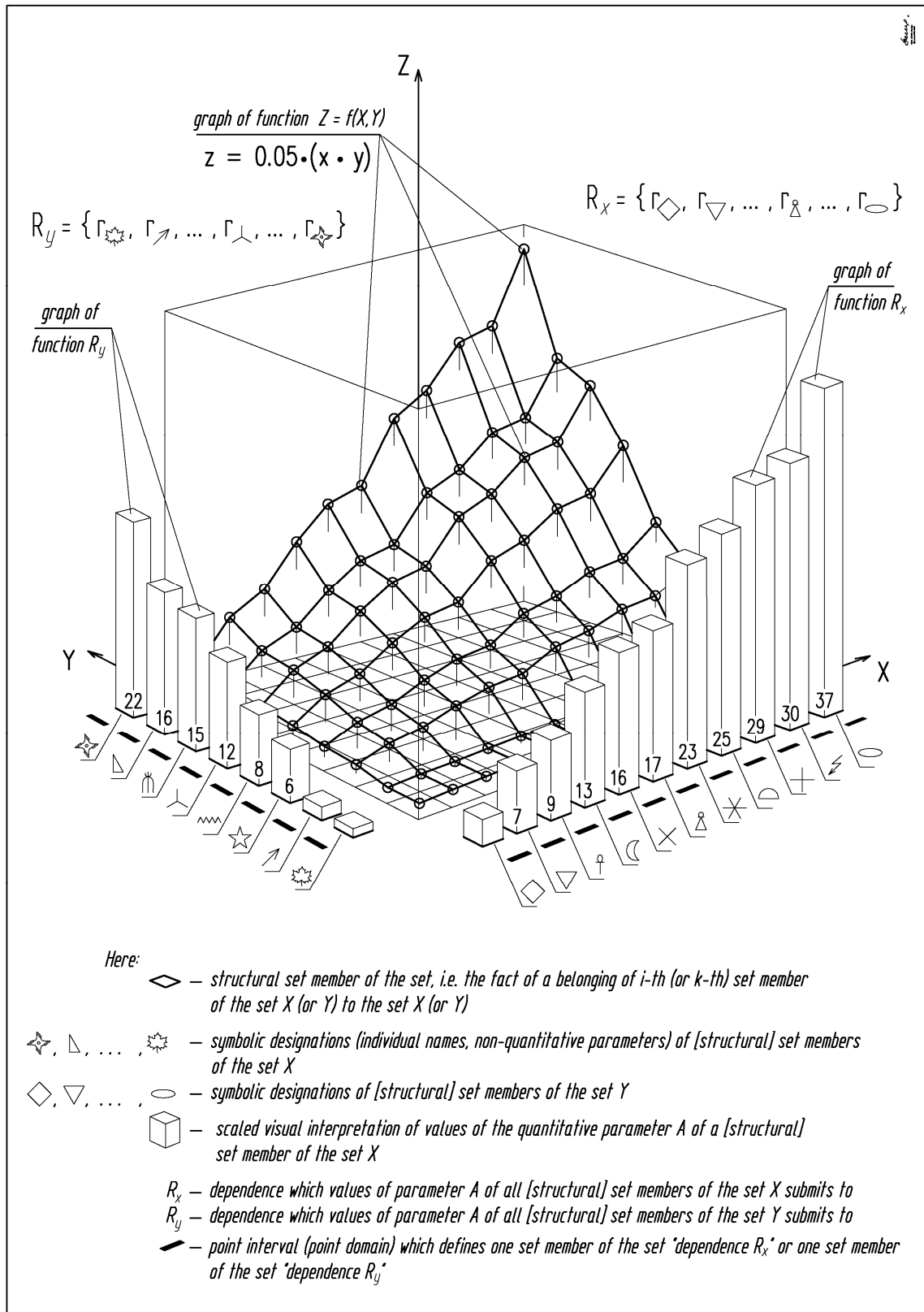


Figure 14. Example Of The Graph Of Regular Function Of Two Irregular Variables

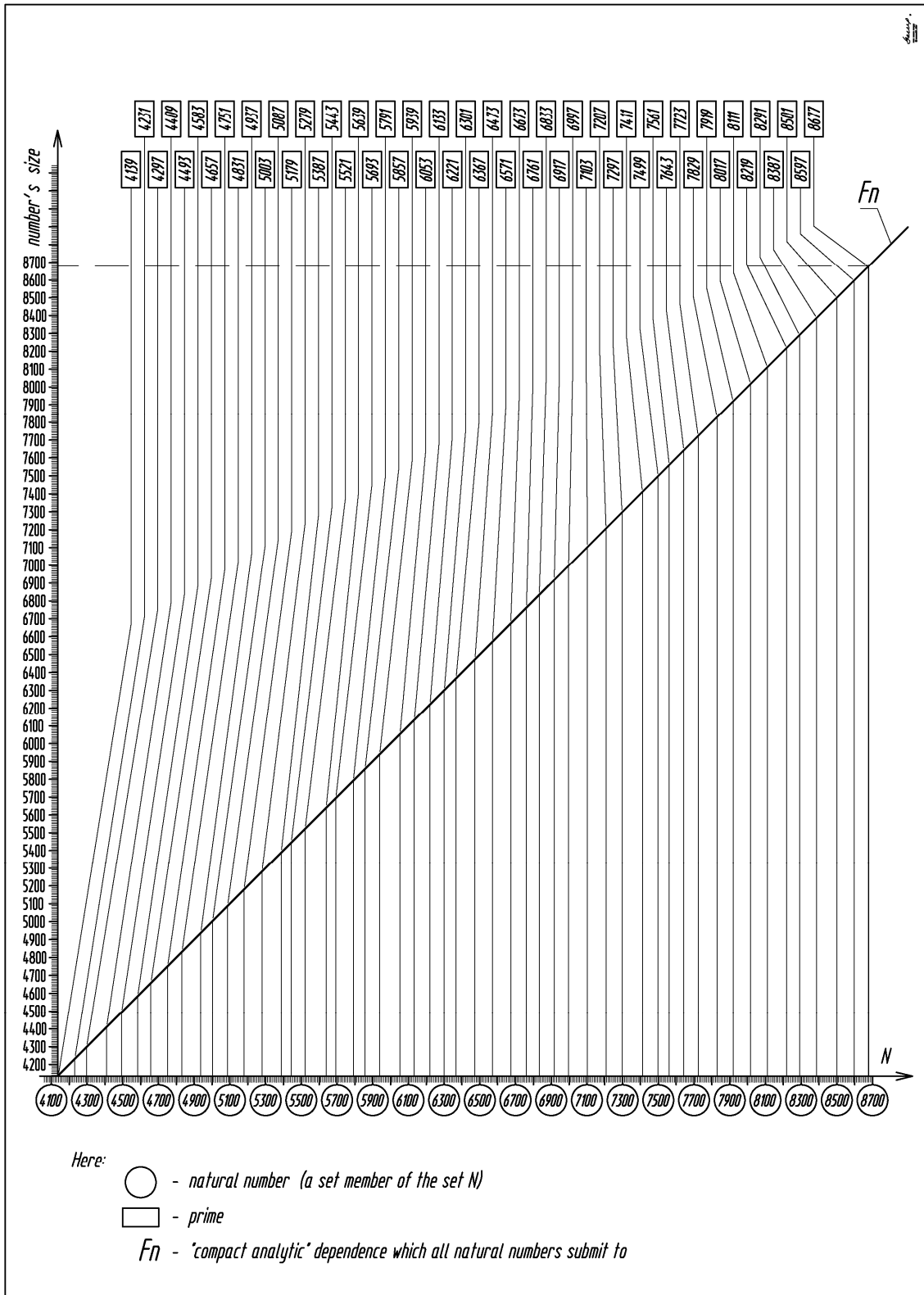


Figure 15. Natural Numbers And Primes In The Range Between 4135 And 8680

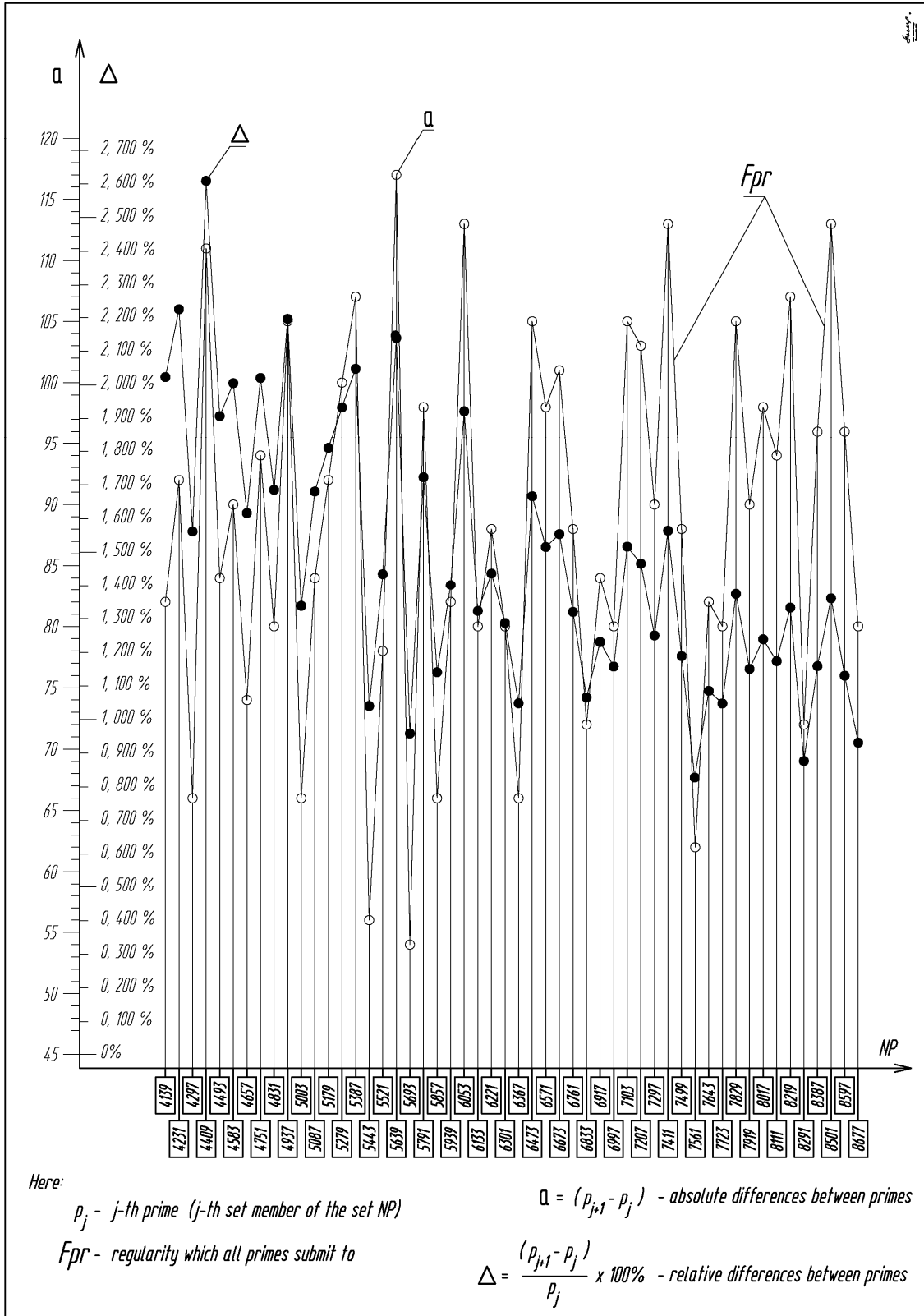


Figure 16. Absolute And Relative Differences Between Primes In The Range Between 4139 And 8677

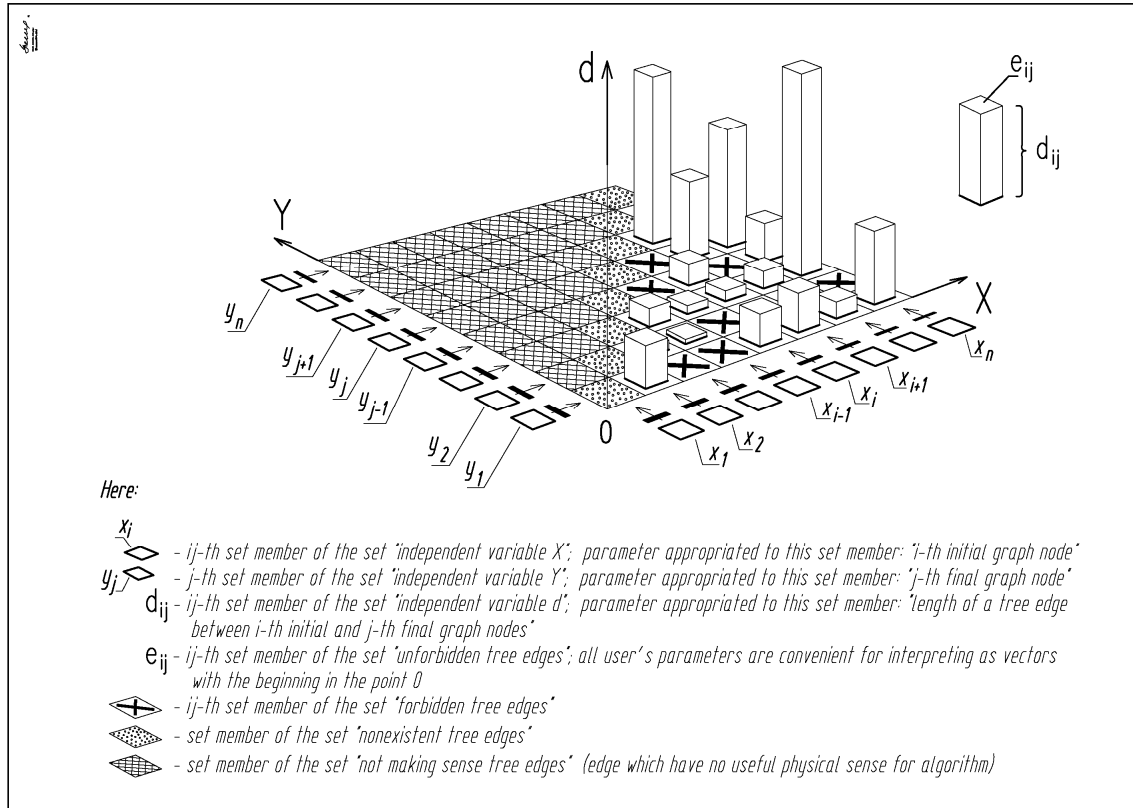


Figure17. Independent Variables Of The TSP (3-Dimensional Interpretation)

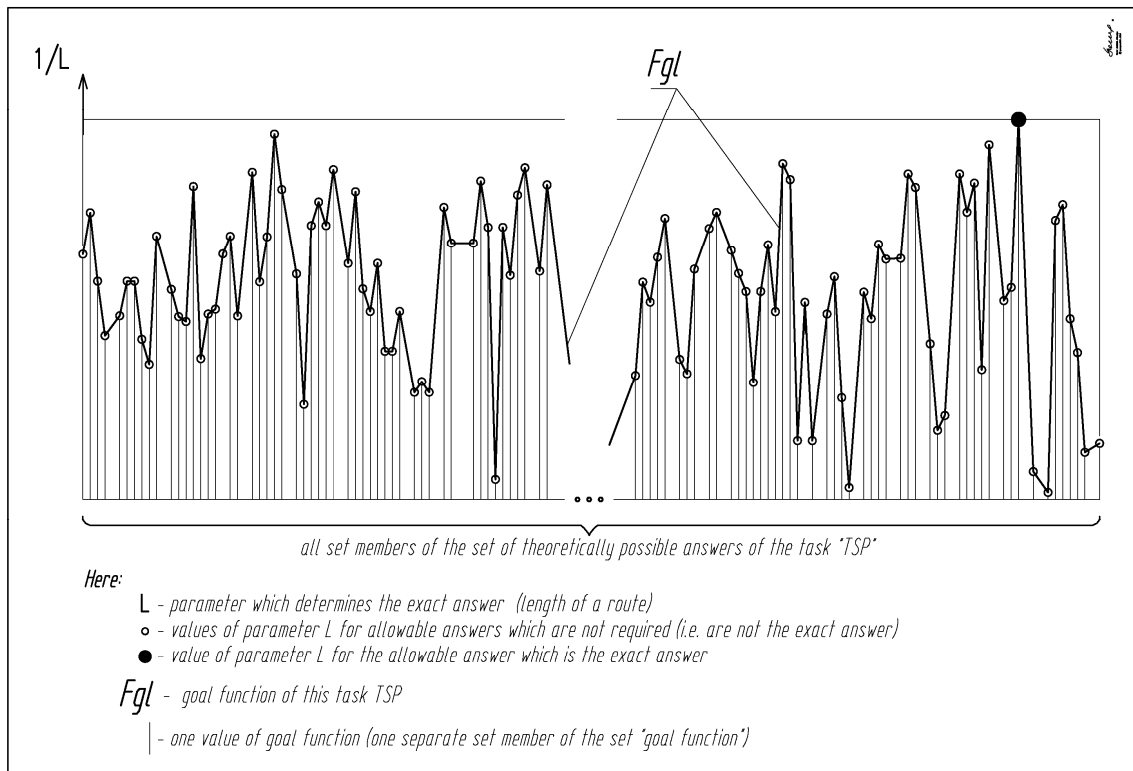


Figure18. Graph Of Goal Function Of The TSP (2-Dimensional Interpretation)