

MATHEMATICAL PROBLEMS.*†

LECTURE DELIVERED BEFORE THE INTERNATIONAL CONGRESS OF MATHEMATICIANS AT PARIS IN 1900.

BY PROFESSOR DAVID HILBERT.

Who of us would not be glad to lift the veil behind which the future lies hidden; to cast a glance at the next advances of our science and at the secrets of its development during future centuries? What particular goals will there be toward which the leading mathematical spirits of coming generations will strive? What new methods and new facts in the wide and rich field of mathematical thought will the new centuries disclose?

History teaches the continuity of the development of science. We know that every age has its own problems, which the following age either solves or casts aside as profitless and replaces by new ones. If we would obtain an idea of the probable development of mathematical knowledge in the immediate future, we must let the unsettled questions pass before our minds and look over the problems which the science of to-day sets and whose solution we expect from the future. To such a review of problems the present day, lying at the meeting of the centuries, seems to me well adapted. For the close of a great epoch not only invites us to look back into the past but also directs our thoughts to the unknown future.

The deep significance of certain problems for the advance of mathematical science in general and the important rôle which they play in the work of the individual investigator are not to be denied. As long as a branch of science offers an abundance of problems, so long is it alive; a lack of problems foreshadows extinction or the cessation of independent development. Just as every human undertaking pursues certain objects, so also mathematical research requires its problems. It is by the solution of problems that the investigator tests the temper of his steel; he finds new methods and new outlooks, and gains a wider and freer horizon.

It is difficult and often impossible to judge the value of a problem correctly in advance; for the final award depends upon the gain which science obtains from the problem. Nevertheless we can ask whether there are general criteria which mark a good mathematical problem. An old French mathematician said: "A mathematical theory is not to be considered complete until you have made it so clear that you can explain it to the first man whom you meet on the street." This clearness and ease of comprehension, here

* Translated for the BULLETIN, with the author's permission, by Dr. MARY WINSTON NEWSON. The original appeared in the *Göttinger Nachrichten*, 1900, pp. 253-297, and in the *Archiv der Mathematik und Physik*, 3d ser., vol. 1 (1901), pp. 44-63 and 213-237.

† Reprinted from the Bulletin of the American Mathematical Society, vol. 8 (1902), pp. 437-479.

insisted on for a mathematical theory, I should still more demand for a mathematical problem if it is to be perfect; for what is clear and easily comprehended attracts, the complicated repels us.

Moreover a mathematical problem should be difficult in order to entice us, yet not completely inaccessible, lest it mock at our efforts. It should be to us a guide post on the mazy paths to hidden truths, and ultimately a reminder of our pleasure in the successful solution.

The mathematicians of past centuries were accustomed to devote themselves to the solution of difficult particular problems with passionate zeal. They knew the value of difficult problems. I remind you only of the "problem of the line of quickest descent," proposed by John Bernoulli. Experience teaches, explains Bernoulli in the public announcement of this problem, that lofty minds are led to strive for the advance of science by nothing more than by laying before them difficult and at the same time useful problems, and he therefore hopes to earn the thanks of the mathematical world by following the example of men like Mersenne, Pascal, Fermat, Viviani and others and laying before the distinguished analysts of his time a problem by which, as a touchstone, they may test the value of their methods and measure their strength. The calculus of variations owes its origin to this problem of Bernoulli and to similar problems.

Fermat had asserted, as is well known, that the diophantine equation

$$x^n + y^n = z^n$$

(x , y and z integers) is unsolvable—except in certain self-evident cases. The attempt to prove this impossibility offers a striking example of the inspiring effect which such a very special and apparently unimportant problem may have upon science. For Kummer, incited by Fermat's problem, was led to the introduction of ideal numbers and to the discovery of the law of the unique decomposition of the numbers of a circular field into ideal prime factors—a law which to-day, in its generalization to any algebraic field by Dedekind and Kronecker, stands at the center of the modern theory of numbers and whose significance extends far beyond the boundaries of number theory into the realm of algebra and the theory of functions.

To speak of a very different region of research, I remind you of the problem of three bodies. The fruitful methods and the far-reaching principles which Poincaré has brought into celestial mechanics and which are to-day recognized and applied in practical astronomy are due to the circumstance that he undertook to treat anew that difficult problem and to approach nearer a solution.

The two last mentioned problems—that of Fermat and the problem of the three bodies—seem to us almost like opposite poles—the former a free invention of pure reason, belonging to the region of abstract number theory, the latter forced upon us by astronomy and necessary to an understanding of the simplest fundamental phenomena of nature.

But it often happens also that the same special problem finds application in the most unlike branches of mathematical knowledge. So, for example, the problem of the

shortest line plays a chief and historically important part in the foundations of geometry, in the theory of curved lines and surfaces, in mechanics and in the calculus of variations. And how convincingly has F. Klein, in his work on the icosahedron, pictured the significance which attaches to the problem of the regular polyhedra in elementary geometry, in group theory, in the theory of equations and in that of linear differential equations.

In order to throw light on the importance of certain problems, I may also refer to Weierstrass, who spoke of it as his happy fortune that he found at the outset of his scientific career a problem so important as Jacobi's problem of inversion on which to work.

Having now recalled to mind the general importance of problems in mathematics, let us turn to the question from what sources this science derives its problems. Surely the first and oldest problems in every branch of mathematics spring from experience and are suggested by the world of external phenomena. Even the rules of calculation with integers must have been discovered in this fashion in a lower stage of human civilization, just as the child of to-day learns the application of these laws by empirical methods. The same is true of the first problems of geometry, the problems bequeathed us by antiquity, such as the duplication of the cube, the squaring of the circle; also the oldest problems in the theory of the solution of numerical equations, in the theory of curves and the differential and integral calculus, in the calculus of variations, the theory of Fourier series and the theory of potential—to say nothing of the further abundance of problems properly belonging to mechanics, astronomy and physics.

But, in the further development of a branch of mathematics, the human mind, encouraged by the success of its solutions, becomes conscious of its independence. It evolves from itself alone, often without appreciable influence from without, by means of logical combination, generalization, specialization, by separating and collecting ideas in fortunate ways, new and fruitful problems, and appears then itself as the real questioner. Thus arose the problem of prime numbers and the other problems of number theory, Galois's theory of equations, the theory of algebraic invariants, the theory of abelian and automorphic functions; indeed almost all the nicer questions of modern arithmetic and function theory arise in this way.

In the meantime, while the creative power of pure reason is at work, the outer world again comes into play, forces upon us new questions from actual experience, opens up new branches of mathematics, and while we seek to conquer these new fields of knowledge for the realm of pure thought, we often find the answers to old unsolved problems and thus at the same time advance most successfully the old theories. And it seems to me that the numerous and surprising analogies and that apparently prearranged harmony which the mathematician so often perceives in the questions, methods and ideas of the various branches of his science, have their origin in this ever-recurring interplay between thought and experience.

It remains to discuss briefly what general requirements may be justly laid down for the solution of a mathematical

problem. I should say first of all, this: that it shall be possible to establish the correctness of the solution by means of a finite number of steps based upon a finite number of hypotheses which are implied in the statement of the problem and which must always be exactly formulated. This requirement of logical deduction by means of a finite number of processes is simply the requirement of rigor in reasoning. Indeed the requirement of rigor, which has become proverbial in mathematics, corresponds to a universal philosophical necessity of our understanding; and, on the other hand, only by satisfying this requirement do the thought content and the suggestiveness of the problem attain their full effect. A new problem, especially when it comes from the world of outer experience, is like a young twig, which thrives and bears fruit only when it is grafted carefully and in accordance with strict horticultural rules upon the old stem, the established achievements of our mathematical science.

Besides it is an error to believe that rigor in the proof is the enemy of simplicity. On the contrary we find it confirmed by numerous examples that the rigorous method is at the same time the simpler and the more easily comprehended. The very effort for rigor forces us to find out simpler methods of proof. It also frequently leads the way to methods which are more capable of development than the old methods of less rigor. Thus the theory of algebraic curves experienced a considerable simplification and attained greater unity by means of the more rigorous function-theoretical methods and the consistent introduction of transcendental devices. Further, the proof that the power series permits the application of the four elementary arithmetical operations as well as the term by term differentiation and integration, and the recognition of the utility of the power series depending upon this proof contributed materially to the simplification of all analysis, particularly of the theory of elimination and the theory of differential equations, and also of the existence proofs demanded in those theories. But the most striking example for my statement is the calculus of variations. The treatment of the first and second variations of definite integrals required in part extremely complicated calculations, and the processes applied by the old mathematicians had not the needful rigor. Weierstrass showed us the way to a new and sure foundation of the calculus of variations. By the examples of the simple and double integral I will show briefly, at the close of my lecture, how this way leads at once to a surprising simplification of the calculus of variations. For in the demonstration of the necessary and sufficient criteria for the occurrence of a maximum and minimum, the calculation of the second variation and in part, indeed, the wearisome reasoning connected with the first variation may be completely dispensed with—to say nothing of the advance which is involved in the removal of the restriction to variations for which the differential coefficients of the function vary but slightly.

While insisting on rigor in the proof as a requirement for a perfect solution of a problem, I should like, on the other hand, to oppose the opinion that only the concepts of analysis, or even those of arithmetic alone, are susceptible of a fully

rigorous treatment. This opinion, occasionally advocated by eminent men, I consider entirely erroneous. Such a one-sided interpretation of the requirement of rigor would soon lead to the ignoring of all concepts arising from geometry, mechanics and physics, to a stoppage of the flow of new material from the outside world, and finally, indeed, as a last consequence, to the rejection of the ideas of the continuum and of the irrational number. But what an important nerve, vital to mathematical science, would be cut by the extirpation of geometry and mathematical physics! On the contrary I think that wherever, from the side of the theory of knowledge or in geometry, or from the theories of natural or physical science, mathematical ideas come up, the problem arises for mathematical science to investigate the principles underlying these ideas and so to establish them upon a simple and complete system of axioms, that the exactness of the new ideas and their applicability to deduction shall be in no respect inferior to those of the old arithmetical concepts.

To new concepts correspond, necessarily, new signs. These we choose in such a way that they remind us of the phenomena which were the occasion for the formation of the new concepts. So the geometrical figures are signs or mnemonic symbols of space intuition and are used as such by all mathematicians. Who does not always use along with the double inequality $a > b > c$ the picture of three points following one another on a straight line as the geometrical picture of the idea "between"? Who does not make use of drawings of segments and rectangles enclosed in one another, when it is required to prove with perfect rigor a difficult theorem on the continuity of functions or the existence of points of condensation? Who could dispense with the figure of the triangle, the circle with its center, or with the cross of three perpendicular axes? Or who would give up the representation of the vector field, or the picture of a family of curves or surfaces with its envelope which plays so important a part in differential geometry, in the theory of differential equations, in the foundation of the calculus of variations and in other purely mathematical sciences?

The arithmetical symbols are written diagrams and the geometrical figures are graphic formulas; and no mathematician could spare these graphic formulas, any more than in calculation the insertion and removal of parentheses or the use of other analytical signs.

The use of geometrical signs as a means of strict proof presupposes the exact knowledge and complete mastery of the axioms which underlie those figures; and in order that these geometrical figures may be incorporated in the general treasure of mathematical signs, there is necessary a rigorous axiomatic investigation of their conceptual content. Just as in adding two numbers, one must place the digits under each other in the right order, so that only the rules of calculation, *i. e.*, the axioms of arithmetic, determine the correct use of the digits, so the use of geometrical signs is

determined by the axioms of geometrical concepts and their combinations.

The agreement between geometrical and arithmetical thought is shown also in that we do not habitually follow the chain of reasoning back to the axioms in arithmetical, any more than in geometrical discussions. On the contrary we apply, especially in first attacking a problem, a rapid, unconscious, not absolutely sure combination, trusting to a certain arithmetical feeling for the behavior of the arithmetical symbols, which we could dispense with as little in arithmetic as with the geometrical imagination in geometry. As an example of an arithmetical theory operating rigorously with geometrical ideas and signs, I may mention Minkowski's work, *Die Geometrie der Zahlen*.*

Some remarks upon the difficulties which mathematical problems may offer, and the means of surmounting them, may be in place here.

If we do not succeed in solving a mathematical problem, the reason frequently consists in our failure to recognize the more general standpoint from which the problem before us appears only as a single link in a chain of related problems. After finding this standpoint, not only is this problem frequently more accessible to our investigation, but at the same time we come into possession of a method which is applicable also to related problems. The introduction of complex paths of integration by Cauchy and of the notion of the IDEALS in number theory by Kummer may serve as examples. This way for finding general methods is certainly the most practicable and the most certain; for he who seeks for methods without having a definite problem in mind seeks for the most part in vain.

In dealing with mathematical problems, specialization plays, as I believe, a still more important part than generalization. Perhaps in most cases where we seek in vain the answer to a question, the cause of the failure lies in the fact that problems simpler and easier than the one in hand have been either not at all or incompletely solved. All depends, then, on finding out these easier problems, and on solving them by means of devices as perfect as possible and of concepts capable of generalization. This rule is one of the most important levers for overcoming mathematical difficulties and it seems to me that it is used almost always, though perhaps unconsciously.

Occasionally it happens that we seek the solution under insufficient hypotheses or in an incorrect sense, and for this reason do not succeed. The problem then arises: to show the impossibility of the solution under the given hypotheses, or in the sense contemplated. Such proofs of impossibility were effected by the ancients, for instance when they showed that the ratio of the hypotenuse to the side of an isosceles right triangle is irrational. In later mathematics, the question as to the impossibility of certain solutions plays a preëminent part, and we perceive in this way that old and

* Leipzig, 1896.

difficult problems, such as the proof of the axiom of parallels, the squaring of the circle, or the solution of equations of the fifth degree by radicals have finally found fully satisfactory and rigorous solutions, although in another sense [than that originally intended. It is probably this important fact along with other philosophical reasons that gives rise to the conviction (which every mathematician shares, but which no one has as yet supported by a proof) that every definite mathematical problem must necessarily be susceptible of an exact settlement, either in the form of an actual answer to the question asked, or by the proof of the impossibility of its solution and therewith the necessary failure of all attempts. Take any definite unsolved problem, such as the question as to the irrationality of the Euler-Mascheroni constant C , or the existence of an infinite number of prime numbers of the form $2^n + 1$. However unapproachable these problems may seem to us and however helpless we stand before them, we have, nevertheless, the firm conviction that their solution must follow by a finite number of purely logical processes.

Is this axiom of the solvability of every problem a peculiarity characteristic of mathematical thought alone, or is it possibly a general law inherent in the nature of the mind, that all questions which it asks must be answerable? For in other sciences also one meets old problems which have been settled in a manner most satisfactory and most useful to science by the proof of their impossibility. I instance the problem of perpetual motion. After seeking in vain for the construction of a perpetual motion machine, the relations were investigated which must subsist between the forces of nature if such a machine is to be impossible;* and this inverted question led to the discovery of the law of the conservation of energy, which, again, explained the impossibility of perpetual motion in the sense originally intended.

This conviction of the solvability of every mathematical problem is a powerful incentive to the worker. We hear within us the perpetual call: There is the problem. Seek its solution. You can find it by pure reason, for in mathematics there is no *ignorabimus*.

The supply of problems in mathematics is inexhaustible, and as soon as one problem is solved numerous others come forth in its place. Permit me in the following, tentatively as it were, to mention particular definite problems, drawn from various branches of mathematics, from the discussion of which an advancement of science may be expected.

Let us look at the principles of analysis and geometry. The most suggestive and notable achievements of the last century in this field are, as it seems to me, the arithmetical formulation of the concept of the continuum in the works of Cauchy, Bolzano and Cantor, and the discovery of non-euclidean geometry by Gauss, Bolyai, and Loba-

*See Helmholtz, "Ueber die Wechselwirkung der Naturkräfte und die darauf bezüglichen neuesten Ermittlungen der Physik"; Vortrag, gehalten in Königsberg, 1854.

hevsky. I therefore first direct your attention to some problems belonging to these fields.

1. CANTOR'S PROBLEM OF THE CARDINAL NUMBER OF THE CONTINUUM.

Two systems, *i. e.*, two assemblages of ordinary real numbers or points, are said to be (according to Cantor) equivalent or of equal *cardinal number*, if they can be brought into relation to one another such that to every number of the one assemblage corresponds one and only one definite number of the other. The investigations of Cantor on such assemblages of points suggest a very plausible theorem, which nevertheless, in spite of the most strenuous efforts, no one has succeeded in proving. This is the theorem :

Every system of infinitely many real numbers, *i. e.*, every assemblage of numbers (or points), is either equivalent to the assemblage of natural integers, 1, 2, 3, ... or to the assemblage of all real numbers and therefore to the continuum, that is, to the points of a line; *as regards equivalence there are, therefore, only two assemblages of numbers, the countable assemblage and the continuum.*

From this theorem it would follow at once that the continuum has the next cardinal number beyond that of the countable assemblage; the proof of this theorem would, therefore, form a new bridge between the countable assemblage and the continuum.

Let me mention another very remarkable statement of Cantor's which stands in the closest connection with the theorem mentioned and which, perhaps, offers the key to its proof. Any system of real numbers is said to be ordered, if for every two numbers of the system it is determined which one is the earlier and which the later, and if at the same time this determination is of such a kind that, if *a* is before *b* and *b* is before *c*, then *a* always comes before *c*. The natural arrangement of numbers of a system is defined to be that in which the smaller precedes the larger. But there are, as is easily seen, infinitely many other ways in which the numbers of a system may be arranged.

If we think of a definite arrangement of numbers and select from them a particular system of these numbers, a so-called partial system or assemblage, this partial system will also prove to be ordered. Now Cantor considers a particular kind of ordered assemblage which he designates as a well ordered assemblage and which is characterized in this way, that not only in the assemblage itself but also in every partial assemblage there exists a first number. The system of integers 1, 2, 3, ... in their natural order is evidently a well ordered assemblage. On the other hand the system of all real numbers, *i. e.*, the continuum in its natural order, is evidently not well ordered. For, if we think of the points of a segment of a straight line, with its initial point excluded, as our partial assemblage, it will have no first element.

The question now arises whether the totality of all numbers may not be arranged in another manner so that every partial assemblage may have a first element, *i. e.*, whether the continuum cannot be considered as a well ordered assemblage—a question which Cantor thinks must be an-

swered in the affirmative. It appears to me most desirable to obtain a direct proof of this remarkable statement of Cantor's, perhaps by actually giving an arrangement of numbers such that in every partial system a first number can be pointed out.

2. THE COMPATIBILITY OF THE ARITHMETICAL AXIOMS.

When we are engaged in investigating the foundations of a science, we must set up a system of axioms which contains an exact and complete description of the relations subsisting between the elementary ideas of that science. The axioms so set up are at the same time the definitions of those elementary ideas; and no statement within the realm of the science whose foundation we are testing is held to be correct unless it can be derived from those axioms by means of a finite number of logical steps. - Upon closer consideration the question arises: *Whether, in any way, certain statements of single axioms depend upon one another, and whether the axioms may not therefore contain certain parts in common, which must be isolated if one wishes to arrive at a system of axioms that shall be altogether independent of one another.*

But above all I wish to designate the following as the most important among the numerous questions which can be asked with regard to the axioms: *To prove that they are not contradictory, that is, that a finite number of logical steps based upon them can never lead to contradictory results.*

In geometry, the proof of the compatibility of the axioms can be effected by constructing a suitable field of numbers, such that analogous relations between the numbers of this field correspond to the geometrical axioms. Any contradiction in the deductions from the geometrical axioms must thereupon be recognizable in the arithmetic of this field of numbers. In this way the desired proof for the compatibility of the geometrical axioms is made to depend upon the theorem of the compatibility of the arithmetical axioms.

On the other hand a direct method is needed for the proof of the compatibility of the arithmetical axioms. The axioms of arithmetic are essentially nothing else than the known rules of calculation, with the addition of the axiom of continuity. I recently collected them* and in so doing replaced the axiom of continuity by two simpler axioms, namely, the well-known axiom of Archimedes, and a new axiom essentially as follows: that numbers form a system of things which is capable of no further extension, as long as all the other axioms hold (axiom of completeness). I am convinced that it must be possible to find a direct proof for the compatibility of the arithmetical axioms, by means of a careful study and suitable modification of the known methods of reasoning in the theory of irrational numbers.

To show the significance of the problem from another point of view, I add the following observation: If contradictory attributes be assigned to a concept, I say, that *mathematically the concept does not exist*. So, for example, a real number whose square is -1 does not exist mathe-

* *Jahresbericht der Deutschen Mathematiker-Vereinigung*, vol. 8 (1900), p. 180.

matically. But if it can be proved that the attributes assigned to the concept can never lead to a contradiction by the application of a finite number of logical processes, I say that the mathematical existence of the concept (for example, of a number or a function which satisfies certain conditions) is thereby proved. In the case before us, where we are concerned with the axioms of real numbers in arithmetic, the proof of the compatibility of the axioms is at the same time the proof of the mathematical existence of the complete system of real numbers or of the continuum. Indeed, when the proof for the compatibility of the axioms shall be fully accomplished, the doubts which have been expressed occasionally as to the existence of the complete system of real numbers will become totally groundless. The totality of real numbers, *i. e.*, the continuum according to the point of view just indicated, is not the totality of all possible series in decimal fractions, or of all possible laws according to which the elements of a fundamental sequence may proceed. It is rather a system of things whose mutual relations are governed by the axioms set up and for which all propositions, and only those, are true which can be derived from the axioms by a finite number of logical processes. In my opinion, the concept of the continuum is strictly logically tenable in this sense only. It seems to me, indeed, that this corresponds best also to what experience and intuition tell us. The concept of the continuum or even that of the system of all functions exists, then, in exactly the same sense as the system of integral, rational numbers, for example, or as Cantor's higher classes of numbers and cardinal numbers. For I am convinced that the existence of the latter, just as that of the continuum, can be proved in the sense I have described; unlike the system of *all* cardinal numbers or of *all* Cantor's alephs, for which, as may be shown, a system of axioms, compatible in my sense, cannot be set up. Either of these systems is, therefore, according to my terminology, mathematically non-existent.

From the field of the foundations of geometry I should like to mention the following problem :

3. THE EQUALITY OF THE VOLUMES OF TWO TETRAHEDRA OF EQUAL BASES AND EQUAL ALTITUDES.

In two letters to Gerling, Gauss* expresses his regret that certain theorems of solid geometry depend upon the method of exhaustion, *i. e.*, in modern phraseology, upon the axiom of continuity (or upon the axiom of Archimedes). Gauss mentions in particular the theorem of Euclid, that triangular pyramids of equal altitudes are to each other as their bases. Now the analogous problem in the plane has been solved.† Gerling also succeeded in proving the equality of volume of symmetrical polyhedra by dividing them into congruent parts. Nevertheless, it seems to me probable that a general proof of this kind for the theorem of Euclid just mentioned is impossible, and it should be our task to give a rigor-

* Werke, vol. 8, pp. 241 and 244.

† Cf., beside earlier literature, Hilbert, Grundlagen der Geometrie, Leipzig, 1899, ch. 4. [Translation by Townsend, Chicago, 1902.]

ous proof of its impossibility. This would be obtained, as soon as we succeeded in specifying two tetrahedra of equal bases and equal altitudes which can in no way be split up into congruent tetrahedra, and which cannot be combined with congruent tetrahedra to form two polyhedra which themselves could be split up into congruent tetrahedra. †

4. PROBLEM OF THE STRAIGHT LINE AS THE SHORTEST DISTANCE BETWEEN TWO POINTS.

Another problem relating to the foundations of geometry is this: If from among the axioms necessary to establish ordinary euclidean geometry, we exclude the axiom of parallels, or assume it as not satisfied, but retain all other axioms, we obtain, as is well known, the geometry of Lobachevsky (hyperbolic geometry). We may therefore say that this is a geometry standing next to euclidean geometry. If we require further that that axiom be not satisfied whereby, of three points of a straight line, one and only one lies between the other two, we obtain Riemann's (elliptic) geometry, so that this geometry appears to be the next after Lobachevsky's. If we wish to carry out a similar investigation with respect to the axiom of Archimedes, we must look upon this as not satisfied, and we arrive thereby at the non-archimedean geometries which have been investigated by Veronese and myself. The more general question now arises: Whether from other suggestive standpoints geometries may not be devised which, with equal right, stand next to euclidean geometry. Here I should like to direct your attention to a theorem which has, indeed, been employed by many authors as a definition of a straight line, viz., that the straight line is the shortest distance between two points. The essential content of this statement reduces to the theorem of Euclid that in a triangle the sum of two sides is always greater than the third side—a theorem which, as is easily seen, deals solely with elementary concepts, *i. e.*, with such as are derived directly from the axioms, and is therefore more accessible to logical investigation. Euclid proved this theorem, with the help of the theorem of the exterior angle, on the basis of the congruence theorems. Now it is readily shown that this theorem of Euclid cannot be proved solely on the basis of those congruence theorems which relate to the application of segments and angles, but that one of the theorems on the congruence of triangles is necessary. We are asking, then, for a geometry in which all the axioms of ordinary euclidean geometry hold, and in particular all the congruence axioms except the one of the congruence of triangles (or all except the theorem of the equality of the base angles in the isosceles triangle), and in which, besides, the proposition that in every triangle the sum of two sides is greater than the third is assumed as a particular axiom.

† Since this was written Herr Dehn has succeeded in proving this impossibility. See his note: "Ueber raumgleiche Polyeder," in *Nachrichten d. K. Gesellsch. d. Wiss. zu Göttingen*, 1900, and a paper soon to appear in the *Math. Annalen* [vol. 55, pp. 465-478].

One finds that such a geometry really exists and is no other than that which Minkowski constructed in his book, *Geometrie der Zahlen*,* and made the basis of his arithmetical investigations. Minkowski's is therefore also a geometry standing next to the ordinary euclidean geometry; it is essentially characterized by the following stipulations:

1. The points which are at equal distances from a fixed point O lie on a convex closed surface of the ordinary euclidean space with O as a center.

2. Two segments are said to be equal when one can be carried into the other by a translation of the ordinary euclidean space.

In Minkowski's geometry the axiom of parallels also holds. By studying the theorem of the straight line as the shortest distance between two points, I arrived* at a geometry in which the parallel axiom does not hold, while all other axioms of Minkowski's geometry are satisfied. The theorem of the straight line as the shortest distance between two points and the essentially equivalent theorem of Euclid about the sides of a triangle, play an important part not only in number theory but also in the theory of surfaces and in the calculus of variations. For this reason, and because I believe that the thorough investigation of the conditions for the validity of this theorem will throw a new light upon the idea of distance, as well as upon other elementary ideas, *e. g.*, upon the idea of the plane, and the possibility of its definition by means of the idea of the straight line, *the construction and systematic treatment of the geometries here possible seem to me desirable.*

5. LIE'S CONCEPT OF A CONTINUOUS GROUP OF TRANSFORMATIONS WITHOUT THE ASSUMPTION OF THE DIFFERENTIABILITY OF THE FUNCTIONS DEFINING THE GROUP.

It is well known that Lie, with the aid of the concept of continuous groups of transformations, has set up a system of geometrical axioms and, from the standpoint of his theory of groups, has proved that this system of axioms suffices for geometry. But since Lie assumes, in the very foundation of his theory, that the functions defining his group can be differentiated, it remains undecided in Lie's development, whether the assumption of the differentiability in connection with the question as to the axioms of geometry is actually unavoidable, or whether it may not appear rather as a consequence of the group concept and the other geometrical axioms. This consideration, as well as certain other problems in connection with the arithmetical axioms, brings before us the more general question: *How far Lie's concept of continuous groups of transformations is approachable in our investigations without the assumption of the differentiability of the functions.*

Lie defines a finite continuous group of transformations as a system of transformations

* Leipzig, 1896.

* *Math. Annalen*, vol. 46, p. 91.

of an order not greater than $\frac{1}{2}$ in x .* Further, we should determine whether the occasional condensation of prime numbers which has been noticed in counting primes is really due to those terms of Riemann's formula which depend upon the first complex zeros of the function $\zeta(s)$.

After an exhaustive discussion of Riemann's prime number formula, perhaps we may sometime be in a position to attempt the rigorous solution of Goldbach's problem,† viz., whether every integer is expressible as the sum of two positive prime numbers; and further to attack the well-known question, whether there are an infinite number of pairs of prime numbers with the difference 2, or even the more general problem, whether the linear diophantine equation

$$ax + by + c = 0$$

(with given integral coefficients each prime to the others) is always solvable in prime numbers x and y .

But the following problem seems to me of no less interest and perhaps of still wider range: *To apply the results obtained for the distribution of rational prime numbers to the theory of the distribution of ideal primes in a given number-field k —* a problem which looks toward the study of the function $\zeta_k(s)$ belonging to the field and defined by the series

$$\zeta_k(s) = \sum \frac{1}{n(j)^s},$$

where the sum extends over all ideals j of the given realm k , and $n(j)$ denotes the norm of the ideal j .

I may mention three more special problems in number theory: one on the laws of reciprocity, one on diophantine equations, and a third from the realm of quadratic forms.

9. PROOF OF THE MOST GENERAL LAW OF RECIPROCITY IN ANY NUMBER FIELD.

For any field of numbers the law of reciprocity is to be proved for the residues of the l th power, when l denotes an odd prime, and further when l is a power of 2 or a power of an odd prime.

The law, as well as the means essential to its proof, will, I believe, result by suitably generalizing the theory of the field of the l th roots of unity,* developed by me, and my theory of relative quadratic fields.†

10. DETERMINATION OF THE SOLVABILITY OF A DIOPHANTINE EQUATION.

Given a diophantine equation with any number of unknown quantities and with rational integral numerical

* Cf. an article by H. von Koch, which is soon to appear in the *Math. Annalen* [Vol. 55, p. 441].

† Cf. P. Stäckel: "Über Goldbach's empirisches Theorem," *Nachrichten d. K. Ges. d. Wiss. zu Göttingen*, 1896, and Landau, *ibid.*, 1900.

* *Jahresber. d. Deutschen Math.-Vereinigung*, "Ueber die Theorie der algebraischen Zahlkörper," vol. 4 (1897), Part V.

† *Math. Annalen*, vol. 51 and *Nachrichten d. K. Ges. d. Wiss. zu Göttingen*, 1898.

coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

11. QUADRATIC FORMS WITH ANY ALGEBRAIC NUMERICAL COEFFICIENTS.

Our present knowledge of the theory of quadratic number fields † puts us in a position to attack successfully the theory of quadratic forms with any number of variables and with any algebraic numerical coefficients. This leads in particular to the interesting problem: to solve a given quadratic equation with algebraic numerical coefficients in any number of variables by integral or fractional numbers belonging to the algebraic realm of rationality determined by the coefficients.

The following important problem may form a transition to algebra and the theory of functions:

12. EXTENSION OF KRONECKER'S THEOREM ON ABELIAN FIELDS TO ANY ALGEBRAIC REALM OF RATIONALITY.

The theorem that every abelian number field arises from the realm of rational numbers by the composition of fields of roots of unity is due to Kronecker. This fundamental theorem in the theory of integral equations contains two statements, namely:

First. It answers the question as to the number and existence of those equations which have a given degree, a given abelian group and a given discriminant with respect to the realm of rational numbers.

Second. It states that the roots of such equations form a realm of algebraic numbers which coincides with the realm obtained by assigning to the argument z in the exponential function e^{iz} all rational numerical values in succession.

The first statement is concerned with the question of the determination of certain algebraic numbers by their groups and their branching. This question corresponds, therefore, to the known problem of the determination of algebraic functions corresponding to given Riemann surfaces. The second statement furnishes the required numbers by transcendental means, namely, by the exponential function e^{iz} .

Since the realm of the imaginary quadratic number fields is the simplest after the realm of rational numbers, the problem arises, to extend Kronecker's theorem to this case. Kronecker himself has made the assertion that the abelian equations in the realm of a quadratic field are given by the equations of transformation of elliptic functions with singular moduli, so that the elliptic function assumes here the same rôle as the exponential function in the former case. The proof of Kronecker's conjecture has not yet been

† Hilbert, "Ueber den Dirichlet'schen biquadratischen Zahlenkörper," *Math. Annalen*, vol. 45; "Ueber die Theorie der relativquadratischen Zahlkörper," *Jahresber. d. Deutschen Mathematiker-Vereinigung*, 1897, and *Math. Annalen*, vol. 51; "Ueber die Theorie der relativ-Abelschen Körper," *Nachrichten d. K. Ges. d. Wiss. zu Göttingen*, 1898; *Grundlagen der Geometrie*, Leipzig, 1899, Chap. VIII, § 83 [Translation by Townsend, Chicago, 1902]. Cf. also the dissertation of G. Rückle, Göttingen, 1901.

integral curves of equation (1) which pass through a fixed point, Kneser on the other hand makes use of any simple family of such curves and constructs for every such family a solution, characteristic for that family, of that partial differential equation which is to be considered as a generalization of the Jacobi-Hamilton equation.

The problems mentioned are merely samples of problems, yet they will suffice to show how rich, how manifold and how extensive the mathematical science of to-day is, and the question is urged upon us whether mathematics is doomed to the fate of those other sciences that have split up into separate branches, whose representatives scarcely understand one another and whose connection becomes ever more loose. I do not believe this nor wish it. Mathematical science is in my opinion an indivisible whole, an organism whose vitality is conditioned upon the connection of its parts. For with all the variety of mathematical knowledge, we are still clearly conscious of the similarity of the logical devices, the *relationship* of the *ideas* in mathematics as a whole and the numerous analogies in its different departments. We also notice that, the farther a mathematical theory is developed, the more harmoniously and uniformly does its construction proceed, and unsuspected relations are disclosed between hitherto separate branches of the science. So it happens that, with the extension of mathematics, its organic character is not lost but only manifests itself the more clearly.

But, we ask, with the extension of mathematical knowledge will it not finally become impossible for the single investigator to embrace all departments of this knowledge? In answer let me point out how thoroughly it is ingrained in mathematical science that every real advance goes hand in hand with the invention of sharper tools and simpler methods which at the same time assist in understanding earlier theories and cast aside older more complicated developments. It is therefore possible for the individual investigator, when he makes these sharper tools and simpler methods his own, to find his way more easily in the various branches of mathematics than is possible in any other science.

The organic unity of mathematics is inherent in the nature of this science, for mathematics is the foundation of all exact knowledge of natural phenomena. That it may completely fulfil this high mission, may the new century bring it gifted masters and many zealous and enthusiastic disciples.

I. Foundations (Yu. I. Manin). In accordance with Hilbert's prophecy, we are living in Cantor's paradise. So we are bound to be tempted.

Most mathematicians nowadays do not see any point in banning infinity, nonconstructivity, etc. Gödel made clear that it takes an infinity of new ideas to understand all about integers only. Hence we need a creative approach to creative thinking, not just a critical one. Two lines of research are naturally suggested.

(a) To find out new axioms of (more or less naive) set theory, demonstrably efficient in number theory. Most advanced new methods (l -adic cohomology) should be explored thoroughly. Are they readily formalized in Zermelo-Fraenkel or Gödel-Bernays systems? Can we use in necessary categorical constructions only known axioms, or has something new already slipped in?

(b) We should consider possibilities of developing a totally new language to speak about infinity. Classical critics of Cantor (Brouwer *et al.*) argued that, say, the general choice axiom is an illicit extrapolation of the finite case.

I would like to point out that this is rather an extrapolation of commonplace physics, where we can distinguish things, count them, put them in some order, etc. New quantum physics has shown us models of entities with quite different behavior. Even "sets" of photons in a looking-glass box, or of electrons in a nickel piece are much less cantorion than the "set" of grains of sand. In general, a highly probabilistic "physical infinity" looks considerably more complicated and interesting than a plain infinity of "things".

Certainly there are no *a priori* reasons to choose fundamental concepts of mathematics so as to make them parallel to those of physics. Nevertheless it happened constantly and proved extremely fruitful.

The twentieth century return to Middle Age scholastics taught us a lot about formalisms. Probably it is time to look outside again. Meaning is what really matters.

II. Number theory.

(A) *Decidability of classical problems* (E. Bombieri). There are very many old problems in arithmetic whose interest is practically nil, e.g. the existence of odd perfect numbers, problems about the iteration of numerical functions, the existence of infinitely many Fermat primes $2^{2^n} + 1$, etc. Some of these questions

Rules for the Millennium Prizes

The Clay Mathematics Institute (CMI) has named seven "Millennium Prize Problems." The Scientific Advisory Board of CMI (SAB) selected these problems, focusing on important classic questions that have resisted solution over the years. The Board of Directors of CMI designated a \$7 million prize fund for the solutions to these problems, with \$1 million allocated to each. The Directors of CMI, and no other persons or body, have the authority to authorize payment from this fund or to modify or interpret these stipulations. The Board of Directors of CMI makes all mathematical decisions for CMI, upon the recommendation of its SAB.

The SAB of CMI will consider a proposed solution to a Millennium Prize Problem if it is a complete mathematical solution to one of the problems. (In the case that someone discovers a mathematical counterexample, rather than a proof, the question will be considered separately as described below.) **A proposed solution to one of the Millennium Prize Problems may not be submitted directly to CMI for consideration.**

Before consideration, a proposed solution must be published in a refereed mathematics publication of worldwide repute (or such other form as the SAB shall determine qualifies), and it must also have general acceptance in the mathematics community two years after. Following this two-year waiting period, the SAB will decide whether a solution merits detailed consideration. In the affirmative case, the SAB will constitute a special advisory committee, which will include (a) at least one SAB member and (b) at least two non-SAB members who are experts in the area of the problem. The SAB will seek advice to determine potential non-SAB members who are internationally-recognized mathematical experts in the area of the problem. As part of this procedure, each component of a proposed solution under consideration shall be verified by one or more members of this special advisory committee.

The special advisory committee will report within a reasonable time to the SAB. Based on this report and possible further investigation, the SAB will make a recommendation to the Directors. The SAB may recommend the award of a prize to one person. The SAB may recommend that a particular prize be divided among multiple solvers of a problem or their heirs. The SAB will pay special attention to the question of whether a prize solution depends crucially on insights published prior to the solution under consideration. The SAB may (but need not) recommend recognition of such prior work in the prize citation, and it may (but need not) recommend the inclusion of the author of prior work in the award.

If the SAB cannot come to a clear decision about the correctness of a solution to a problem, its attribution, or the appropriateness of an award, the SAB may recommend that no prize be awarded for a particular problem. If new information comes to light, the SAB may (but will not necessarily) reconsider a negative decision to recommend a prize for a proposed solution, but only after an additional two-year waiting period following the time that the new information comes to light. The SAB has the sole authority to make recommendations to the Directors of the CMI concerning the appropriateness of any award and the validity of any claim to the CMI Millennium Prize.

In the case of the P versus NP problem and the Navier-Stokes problem, the SAB will consider the award of the Millennium Prize for deciding the question in either direction. In the case of the other problems if a counterexample is proposed, the SAB will consider this counterexample after publication and the same two-year waiting period as for a proposed solution will apply. If, in the opinion of the SAB, the counterexample effectively resolves the problem then the SAB may recommend the award of the Prize. If the counterexample shows that the original problem survives after reformulation or elimination of some special case, then the SAB may recommend that a small prize be awarded to the author. The money for this prize

See also:

[Notes on the Rules](#)

[Publication Guidelines](#)

will not be taken from the Millennium Prize Problem fund, but from other CMI funds.

Any person who is not a disqualified person (as that term is defined in section 4946 of the Internal Revenue Code) in connection with the Institute, or a then serving member of the SAB, may receive the Millennium Prize.

All decision-making procedures concerning the CMI Millennium Prize Problems are private. This includes the deliberations or recommendations of any person or persons CMI has used to obtain advice on this question. No records of these deliberations or related correspondence may be made public without the prior approval of the Directors, the SAB, and all other living persons involved, unless fifty years time have elapsed after the event in question.

Notwithstanding the wording of the problem descriptions, the SAB will not consider recommending the award of a prize to any individual who has not, in the judgement of SAB, made a major personal contribution to the understanding of the field of the problem in their published solution; nor will it investigate in detail solutions that do not represent a major advance in the field. Conversely, the SAB may consider recommending the award of the prize to an individual who has published work that, in the judgement of the SAB, fully resolves the questions raised by one of the Millennium Prize Problems even if it does not exactly meet the wording in the official problem description.

Please send inquiries regarding the Millennium Prize Problems to admin@claymath.org.

Revision of September 25, 2012

Clay Mathematics Institute
10 Memorial Blvd.
Suite 902
Providence, RI 02903,
USA

CMI President's Office
Andrew Wiles Building
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG, UK

Last update: 25-Mar-2015 12:36 pm

P vs NP Problem



Suppose that you are organizing housing accommodations for a group of four hundred university students. Space is limited and only one hundred of the students will receive places in the dormitory. To complicate matters, the Dean has provided you with a list of pairs of incompatible students, and requested that no pair from this list appear in your final choice. This is an example of what computer scientists call an NP-problem, since it is easy to check if a given choice of one hundred students proposed by a coworker is satisfactory (i.e., no pair taken from your coworker's list also appears on the list from the Dean's office), however the task of generating such a list from scratch seems to be so hard as to be completely impractical. Indeed, the total

number of ways of choosing one hundred students from the four hundred applicants is greater than the number of atoms in the known universe! Thus no future civilization could ever hope to build a supercomputer capable of solving the problem by brute force; that is, by checking every possible combination of 100 students. However, this apparent difficulty may only reflect the lack of ingenuity of your programmer. In fact, one of the outstanding problems in computer science is determining whether questions exist whose answer can be quickly checked, but which require an impossibly long time to solve by any direct procedure. Problems like the one listed above certainly seem to be of this kind, but so far no one has managed to prove that any of them really are so hard as they appear, i.e., that there really is no feasible way to generate an answer with the help of a computer. Stephen Cook and Leonid Levin formulated the P (i.e., easy to find) versus NP (i.e., easy to check) problem independently in 1971.

This problem is: **Unsolved**

Rules:

[Rules for the Millennium Prizes](#)

Related Documents:

 [Official Problem Description](#)

 [Minesweeper](#)

Related Links:

[Lecture by Vijaya Ramachandran](#)