

The Theory of Numbers.<sup>1</sup>

By Prof. G. H. HARDY, M.A., F.R.S.

I FIND myself to-day in the same embarrassing position in which a predecessor of mine at Oxford found himself at Bradford in 1875, the president of a Section, probably the largest and most heterogeneous in the Association, which is absorbed by a multitude of divergent professional interests, none of which agree with his or mine.

There are two courses possible in such circumstances. One is to take refuge, as Prof. Henry Smith did then, with visible reluctance, in a series of general propositions to which mathematicians, physicists, and astronomers may all be expected to return a polite assent. The importance of science and scientific method, the need for better organisation of scientific education and research, are all topics on which I could no doubt say something without undue strain either on my own honesty or on your credulity. That there is no finer education and discipline than natural science; that it is, as Dr. Campbell has said, "the noblest of the arts"; that the crowning achievements of science lie in those directions with which this Section is professionally concerned: all this I could say with complete sincerity, and, if I were the head of a deputation approaching a Government Department, I suppose that I would not shirk even so unprofitable a task.

It is unfortunate that these essential and edifying truths, important as it is that they should be repeated as loudly as possible from time to time, are, to the man whose interest in life lies in scientific work and not in propaganda, unexciting, and in fact quite intolerably dull. I could, if I chose, say all these things, but, even if I wanted to, I should scarcely increase your respect for mathematics and mathematicians by repeating to you what you have said yourselves, or read in the newspapers, a hundred times already. I shall say them all some day; the time will come when we shall none of us have anything more interesting to say. We need not anticipate our inevitable end.

I propose therefore to adopt the alternative course suggested by my predecessor, and try to say something to you about the one subject about which I have anything to say. It happens, by a fortunate accident, that the particular subject which I love the most, and which presents most of the problems which occupy my own researches, is by no means overwhelmingly recondite or obscure, and indeed is sharply distinguished from almost every other branch of pure mathematics, in that it makes a direct, popular, and almost irresistible appeal to the heart of the ordinary man.

There is, however, one preliminary remark which I cannot resist the temptation of making. The present is a particularly happy moment for a pure mathematician, since it has been marked by one of the greatest recorded triumphs of pure mathematics. This triumph is the work, as it happens, of a man who probably would not describe himself as a mathematician, but who has done more than any mathematician to vindicate the dignity of mathematics, and to put that obscure and perplexing construction,

commonly described as "physical reality," in its proper place.

There is probably less difference between the methods of a physicist and a mathematician than is generally supposed. The most striking among them seems to me to be this, that the mathematician is in much more direct contact with reality. This may perhaps seem to you a paradox, since it is the physicist who deals with the subject-matter to which the epithet "real" is commonly applied. But a very little reflection will show that the "reality" of the physicist, whatever it may be (and it is extraordinarily difficult to say), has few or none of the attributes which common-sense instinctively marks as real. A chair may be a collection of whirling atoms, or an idea in the mind of God. It is not my business to suggest that one account of it is obviously more plausible than the other. Whatever the merits of either of them may be, neither draws its inspiration from the suggestions of common-sense.

Neither the philosophers, nor the physicists themselves, have ever put forward any very convincing account of what physical reality is, or of how the physicist passes, from the confused mass of fact or sensation with which he starts, to the construction of the objects which he classifies as real. We cannot be said, therefore, to know what the subject-matter of physics is; but this need not prevent us from understanding the task which a physicist is trying to perform. That, clearly, is to correlate the incoherent body of facts confronting him with some definite and orderly scheme of abstract relations, the kind of scheme, in short, which he can borrow only from mathematics.

A mathematician, on the other hand, fortunately for him, is not concerned with this physical reality at all. It is impossible to prove, by mathematical reasoning, any proposition whatsoever concerning the physical world, and only a mathematical crank would be likely now to imagine it his function to do so. There is plainly one way only of ascertaining the facts of experience, and that is by observation. It is not the business of a mathematician to suggest one view of the universe or another, but merely to supply the physicists with a collection of abstract schemes, which it is for them to select from, and to adopt or discard at their pleasure.

The most obvious example is to be found in the science of geometry. Mathematicians have constructed a very large number of different systems of geometry, Euclidean or non-Euclidean, of one, two, three, or any number of dimensions. All these systems are of complete and equal validity. They embody the results of mathematicians' observations of *their* reality, a reality far more intense and far more rigid than the dubious and elusive reality of physics. The old-fashioned geometry of Euclid, the entertaining seven-point geometry of Veblen, the space-times of Minkowski and Einstein, are all absolutely and equally real. When a mathematician has constructed, or, to be more accurate, when he has observed them, his professional interest in the matter ends. It may be the seven-point

<sup>1</sup> Presidential address delivered to Section A (Mathematics and Physics) of the British Association at Hull on Sept. 8.

geometry that fits the facts the best, for anything that mathematicians have to say. There may be three dimensions in this room and five next door. As a professional mathematician, I have no idea; I can only ask some competent physicist to instruct me in the facts.

The function of a mathematician, then, is simply to observe the facts about his own intricate system of reality, that astonishingly beautiful complex of logical relations which forms the subject-matter of his science, as if he were an explorer looking at a distant range of mountains, and to record the results of his observations in a series of maps, each of which is a branch of pure mathematics. Many of these maps have been completed, while in others, and these, naturally, are the most interesting, there are vast uncharted regions. Some, it seems, have some relevance to the structure of the physical world, while others have no such tangible application. Among them there is perhaps none quite so fascinating, with quite the same astonishing contrasts of sharp outline and mysterious shade, as that which constitutes the theory of numbers.

The number system of arithmetic is, as we know too well, not without its applications to the sensible world. The currency systems of Europe, for example, conform to it approximately; west of the Vistula, two and two make something approaching four. The practical applications of arithmetic, however, are tedious beyond words. One must probe a little deeper into the subject if one wishes to interest the ordinary man, whose taste in such matters is astonishingly correct, and who turns with joy from the routine of common life to anything strange and odd, like the fourth dimension, or imaginary time, or the theory of the representation of integers by sums of squares or cubes.

It is impossible for me to give you, in the time at my command, any general account of the problems of the theory of numbers, or of the progress that has been made towards their solution even during the last twenty years. I must adopt a much simpler method. I will merely state to you, with a few words of comment, three or four isolated questions, selected in a haphazard way. They are seemingly simple questions, and it is not necessary to be anything of a mathematician to understand them; and I have chosen them for no better reason than that I happen to be interested in them myself. There is no one of them to which I know the answer, nor, so far as I know, does any mathematician in the world; and there is no one of them, with one exception which I have included deliberately, the answer to which any one of us would not make almost any sacrifice to know.

1. *When is a number the sum of two cubes, and what is the number of its representations?* This is my first question, and first of all I will elucidate it by some examples. The numbers  $2 = 1^3 + 1^3$  and  $9 = 2^3 + 1^3$  are sums of two cubes, while 3 and 4 are not: it is exceptional for a number to be of this particular form. The number of cubes up to 1,000,000 is 100, and the number of numbers, up to this limit and of the form required, cannot exceed 10,000, one-hundredth of the whole. The density of the distribution of such numbers tends to zero as the numbers tend to infinity. Is there, I am asking, any simple criterion by which such numbers can be distinguished?

Again, 2 and 9 are sums of two cubes, and can be expressed in this form in one way only. There are numbers so expressible in a variety of different ways. The least such number is 1729, which is  $12^3 + 1^3$  and also  $10^3 + 9^3$ . It is more difficult to find a number with *three* representations; the least such number is

$$175,959,000 = 560^3 + 70^3 = 552^3 + 198^3 = 525^3 + 315^3.$$

One number at any rate is known with *four* representations, namely,

$$19 \times 363510^3$$

(a number of 18 digits), but I am not prepared to assert that it is the least. No number has been calculated, so far as I know, with more than four, but theory, running ahead of computation, shows that numbers exist with five representations, or six, or any number.

A distinguished physicist has argued that the possible number of isotopes of an element is probably limited because, among the ninety or so elements at present under observation, there is none which has more isotopes than six. I dare not criticise a physicist in his own field; but the figures I have quoted may suggest to you that an arithmetical generalisation, based on a corresponding volume of evidence, would be more than a little rash.

There are similar questions, of course, for squares, but the answers to these were found long ago by Euler and by Gauss, and belong to the classical mathematics. Suppose, for simplicity of statement, that the number in question is *prime*. Then, if it is of the form  $4m + 1$ , it is a sum of squares, and in one way only, while if it is of the form  $4m + 3$  it is not so expressible; and this simple rule may readily be generalised so as to apply to numbers of any form. But there is no similar solution for our actual problem, nor, I need scarcely say, for the analogous problems for fourth, fifth, or higher powers. The smallest number known to be expressible in two ways by two biquadrates is

$$635318657 = 158^4 + 59^4 = 134^4 + 133^4;$$

and I do not believe that any number is known expressible in three. Nor, to my knowledge, has the bare existence of such a number yet been proved. When we come to fifth powers, nothing is known at all. The field for future research is unlimited and practically untrodden.

2. I pass to another question, again about cubes, but of a somewhat different kind. *Is every large number (every number, that is to say, from a definite point onwards) the sum of five cubes?* This is another exceptionally difficult problem. It is known that every number, without exception, is the sum of nine cubes; two numbers, 23 (which is  $2 \cdot 2^3 + 7 \cdot 1^3$ ) and 239, actually require so many. It seems that there are just fifteen numbers, the largest being 454, which need eight, and 121 numbers, the largest being 8042, which need seven; and the evidence suggests forcibly that the six-cube numbers also ultimately disappear. In a lecture which I delivered on this subject at Oxford I stated, on the authority of Dr. Ruckle, that there were two numbers, in the immediate neighbourhood of 1,000,000, which could not be resolved into fewer cubes than six; but Dr. A. E. Western has refuted this assertion by resolving each of them into five, and is of opinion,

I believe, that the six-cube numbers have disappeared entirely considerably before this point. It is conceivable that the five-cube numbers also disappear, but this, if it be so, is probably in depths where computation is helpless. The four-cube numbers must certainly persist for ever, for it is impossible that a number  $9n+4$  or  $9n+5$  should be the sum of three.

I need scarcely add that there is a similar problem for every higher power. For fourth powers the critical number is 16. There is no case, except the simple case of squares, in which the solution is in any sense complete. About the squares there is no mystery; every number is the sum of four squares, and there are infinitely many numbers which cannot be expressed by fewer.

3. I will next raise the question *whether the number  $2^{137}-1$  is prime*. I said that I would include one question which does not interest me particularly; and I should like to explain to you the kind of reasons which damp down my interest in this one. I do not know the answer, and I do not care greatly what it is.

The problem belongs to the theory of the so-called "perfect" numbers, which has exercised mathematicians since the times of the Greeks. A number is perfect if, like 6 or 28, it is the sum of all its divisors, unity included. Euclid proved that the number

$$2^m(2^{m+1}-1)$$

is perfect if the second factor is prime; and Euler, 2000 years later, that all *even* perfect numbers are of Euclid's form. It is still unknown whether a perfect number can be odd.

It would obviously be most interesting to know generally in what circumstances a number  $2^n-1$  is prime. It is plain that this can be so only if  $n$  itself is prime, as otherwise the number has obvious factors; and the 137 of my question happens to be the least value of  $n$  for which the answer is still in doubt. You may perhaps be surprised that a question apparently so fascinating should fail to arouse me more.

It was asserted by Mersenne in 1644 that the only values of  $n$ , up to 257, for which  $2^n-1$  is prime are

$$2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257;$$

and an enormous amount of labour has been expended on attempts to verify this assertion. There are no simple general tests by which the primality of a number chosen at random can be determined, and the amount of computation required in any particular case may be appalling. It has, however, been imagined that Mersenne perhaps knew something which later mathematicians have failed to rediscover. The idea is a little fantastic, but there is no doubt that, so long as the possibility remained, arithmeticians were justified in their determination to ascertain the facts at all costs. "The riddle as to how Mersenne's numbers were discovered remains unsolved," wrote Mr. Rouse Ball in 1891. Mersenne, he observes, was a good mathematician, but not an Euler or a Gauss, and he inclines to attribute the discovery to the exceptional genius of Fermat, the only mathematician of the age whom any one could suspect of being hundreds of years ahead of his time.

These speculations appear extremely fanciful now, for the bubble has at last been pricked. It seems now that Mersenne's assertion, so far from hiding un-plumbed depths of mathematical profundity, was a

conjecture based on inadequate empirical evidence, and a somewhat unhappy one at that. It is now known that there are at least four numbers about which Mersenne is definitely wrong; he should have included at any rate 61, 89, and 107, and he should have left out 67. The mistake as regards 61 and 67 was discovered so long ago as 1886, but could be explained with some plausibility, so long as it stood alone, as a merely clerical error. But when Mr. R. E. Powers, in 1911 and 1914, proved that Mersenne was also wrong about 89 and 107, this line of defence collapsed, and it ceased to be possible to take Mersenne's assertion seriously.

The facts may be summed up as follows. Mersenne makes fifty-five assertions, for the fifty-five primes from 2 to 257. Of these assertions forty are true, four false, and eleven still doubtful. Not a bad result, you may think; but there is more to be said. Of the forty correct assertions many, half at least, are trivial, either because the numbers in question are comparatively small, or because they possess quite small and easily detected divisors. The test cases are those in which the numbers are prime, or Mersenne asserts that they are so; there are only four of these cases which are difficult and in which the truth is known; and in these Mersenne is wrong in every case but one.

It seems to me, then, that we must regard Mersenne's assertion as exploded; and for my part it interests me no longer. If he is wrong about 89 and 107, I do not care greatly whether he is wrong about 137 as well, and I should regard the computations necessary to decide as very largely wasted. There are so many much more profitable calculations which a computer could undertake.

I hope that you will not infer that I regard the problem of perfect numbers as uninteresting in itself; that would be very far from the truth. There are at least two intensely interesting problems. The first is the old problem, which so many mathematicians have failed to solve, whether a perfect number can be odd. The second is whether the number of perfect numbers is infinite or not. If we assume that all perfect numbers are even, we can state this problem in a still more arresting form. *Are there infinitely many primes of the form  $2^n-1$ ?* I find it difficult to imagine a problem more fascinating or more intricate than that. It is plain, though, that this is a question which computation can never decide, and it is very unlikely that it can ever give us any data of serious value. And the problem itself really belongs to a different chapter of the theory, to which I should like next to direct your attention.

4. *Are there infinitely many primes of the form  $n^2+1$ ?* Let me first remind you of some well-known facts in regard to the distribution of primes.

There are infinitely many primes; their density decreases as the numbers increase, and tends to zero when the numbers tend to infinity. More accurately, the number of primes less than  $x$  is, to a first approximation,

$$\frac{x}{\log x}$$

The chance that a large number  $n$ , selected at random, should be prime is, we may say, about  $\frac{1}{\log n}$ .

Still more precisely, the "logarithm-integral"

$$\text{Li } x = \int_2^x \frac{dt}{\log t}$$

gives a very good approximation to the number of primes. This number differs from  $\text{Li } x$  by a function of  $x$  which oscillates continually, as Mr. Littlewood, in defiance of all empirical evidence to the contrary, has shown, between positive and negative values, and is sometimes large, of the order of magnitude  $\sqrt{x}$  or thereabouts, but always small in comparison with the logarithm-integral itself.

Except for one lacuna, which I must pass over in silence now, this problem of the general distribution of primes, the first and central problem of the theory, is in all essentials solved. But a variety of most interesting problems remain as to the distribution of primes among numbers of special forms. The first and simplest of these is that of the arithmetical progressions: *How are the primes distributed among all possible arithmetical progressions  $an+b$ ?* We may leave out of account the case in which  $a$  and  $b$  have a common factor; this case is trivial, since  $an+b$  is then obviously not prime.

The first step towards a solution was made by Dirichlet, who proved for the first time, in 1837, that any such arithmetical progression contains an infinity of primes. It has since been shown that the primes are, to a first approximation at any rate, distributed evenly among all the arithmetical progressions. When we pursue the analysis further, differences appear; there are on the average, for example, more primes  $4n+3$  than primes  $4n+1$ , though it is not true, as the evidence of statistics has led some mathematicians to conclude too hastily, that there is always an excess to whatever point the enumeration is carried.

The problem of the arithmetical progressions, then, may also be regarded as solved; and the same is true of the problem of the primes of a given quadratic form, say  $am^2+2bmn+cn^2$ , homogeneous in the two variables  $m$  and  $n$ . To take, for example, the simplest and most striking case, there is the natural and obvious number of primes  $m^2+n^2$ . A prime is of this form, as I have mentioned already, if, and only if, it is of the form  $4k+1$ . The quadratic problem reduces here to a particular case of the problem of the arithmetical progressions.

When we pass to cubic forms, or forms of higher degree, we come to the region of the unknown. This, however, is not the field of inquiry which I wish now to commend to your attention. The quadratic forms of which I have spoken are forms in two independent variables  $m$  and  $n$ ; the form  $n^2+1$  of my question is a non-homogeneous form in a single variable  $n$ , the simplest case of the general form  $an^2+2bn+c$ . It is clear that one may ask the same question for forms of any degree: are there, for example, infinitely many primes  $n^3+2$  or  $n^4+1$ ? I do not choose  $n^3+1$ , naturally, because of the obvious factor  $n+1$ .

This problem is one in which computation can still play an important part. You will remember that I stated the same problem for perfect numbers. There a computer is helpless. For the numbers  $2^n-1$ , which dominate the theory, increase with unmanageable

rapidity, and the data collected by the computers appear, so far as one can judge, to be almost devoid of value. Here the data are ample, and, though the question is still unanswered, there is really strong statistical evidence for supposing a particular answer to be true. It seems that the answer is affirmative, and that there is a definite approximate formula for the number of primes in question. This formula is

$$\frac{1}{2} \text{Li } \sqrt{x} \times \left(1 + \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 + \frac{1}{7}\right) \left(1 + \frac{1}{11}\right) \dots,$$

where the product extends over all primes  $p$ , and the positive sign is chosen when  $p$  is of the form  $4n+3$ . Dr. A. E. Western has submitted this formula to a most exhaustive numerical check. It so happens that Colonel Cunningham some years ago computed a table of primes  $n^2+1$  up to the value 15,000 of  $n$ , a limit altogether beyond the range of the standard factor tables, and Cunningham's table has made practicable an unusually comprehensive test. The actual number of primes is 1199, while the number predicted is 1219. The error, less than 1 in 50, is much less than one could reasonably expect. The formula stands its test triumphantly, but I should be deluding you if I pretended to see any immediate prospect of an accurate proof.

5. The last problem I shall state to you is this: *Are there infinitely many prime-pairs  $p, p+2$ ?* One may put the problem more generally: *Does any group of primes, with assigned and possible differences, recur indefinitely, and what is the law of its recurrence?*

I must first explain what I mean by a "possible" group of primes. It is possible that  $p$  and  $p+2$  should both be prime, like 3, 5, or 101, 103. It is not possible (unless  $p$  is 3) that  $p, p+2$  and  $p+4$  should all be prime, for one of them must be a multiple of 3: but  $p, p+2, p+6$  or  $p, p+4, p+6$  are possible triplets of primes. Similarly

$$p, p+2, p+6, p+8, p+12$$

can all be prime, so far as any elementary test of divisibility shows, and in fact 5, 7, 11, 13 and 17 satisfy the conditions. It is easy to define precisely what we understand by a "possible" group. We mean a group the differences in which, like 0, 2, 6, have at least one missing residue to every possible modulus. The "impossible" group 0, 2, 4 does not satisfy the condition, for the remainders after division by 3 are 0, 2, 1, a complete set of residues to modulus 3. There is no difficulty in specifying possible groups of any length we please.

We define in this manner, then, a "possible" group of primes, and we put the questions: Do all possible groups of primes actually occur, do they recur indefinitely often, and how often on the average do they recur? Here again it would seem that the answers are affirmative, that all possible groups occur, and continue to occur for ever, and with a frequency the law of which can be assigned. The order of magnitude of the number of prime-pairs,  $p, p+2$ , or  $p, p+4$ , or  $p, p+6$ , both members of which are less than a large number  $x$ , is, it appears,

$$\frac{x}{(\log x)^2}$$

The order of magnitude of the corresponding number of triplets, of any possible type, is

$$\frac{x}{(\log x)^3}$$

and so on generally. Further, we can assign the relative frequencies of pairs or triplets of different types; there are, for example, about twice as many pairs the difference of which is 6 as there are pairs with the difference 2. All these results have been tested by actual enumeration from the factor tables of the first million numbers; and a physicist would probably regard them as proved, though we of course know very well that they are not.

There is a great deal of mathematics the purport of which is quite impossible for any amateur to grasp, and which, however beautiful and important it may be, must always remain the possession of a narrow circle

of experts. It is the peculiarity of the theory of numbers that much of it could be published broadcast, and would win new readers for the *Daily Mail*. The positive integers do not lie, like the logical foundations of mathematics, in the scarcely visible distance, nor in the uncomfortably tangled foreground, like the immediate data of the physical world, but at a decent middle distance, where the outlines are clear and yet some element of mystery remains. There is no one so blind that he does not see them, and no one so sharp-sighted that his vision does not fail; they stand there a continual and inevitable challenge to the curiosity of every healthy mind. I have merely directed your attention for a moment to a few of the less immediately conspicuous features of the landscape, in the hope that I may sharpen your curiosity a little, and that some may feel tempted to walk a little nearer and take a closer view.

### The Organisation of Research.<sup>1</sup>

By Principal J. C. IRVINE, C.B.E., D.Sc., LL.D., F.R.S.

THE British Association was the product of an age rather than the inspiration of any one man, yet of those who first gave practical effect to the movement which has spread scientific learning and has bound its devotees in a goodly fellowship there was no more eager spirit than Sir David Brewster. It is not an exaggerated claim that it was he who founded the British Association. One may trace his enlightened action to a desire to combat the apathy and distrust shown by the Government of his day towards scientific work and even scientific workers. Only in the historical sense can I claim any relationship with Brewster. It is my privilege to occupy the Principalship he once held, and I cannot escape from the thought that the daily tasks now mine were once his.

It is thus inevitable that to-day a name often in my mind should spring once more into recollection, especially as my distinguished predecessor was present at the first Hull meeting in 1853, when he contributed two papers to Section A. Chemists should be among the first to pay grateful tribute to Brewster's efforts on behalf of science, and I propose, therefore, to include in my address a review of the position scientific chemistry has won since his day in public and official estimation. Moreover, at the express suggestion of some of our members whose opinions cannot be disregarded, I am induced to add the consideration of the new responsibilities chemists have incurred now that so many of Brewster's hopes have been realised. These were recently submitted by me to another audience and, through the medium of an article in *NATURE* (July 22, p. 131), are possibly known to you already, but I agree with my advisers that their importance warrants further elaboration and wider discussion.

It would be idle to recall the lowly position of chemistry as an educative force in this country, or to reconstruct the difficulties with which the scientific chemist was confronted during the first thirty years of the nineteenth century. Present difficulties are

serious enough, and press for all our attention, without dwelling unduly on troubles of the past. But we must at least remember that in the early days of the British Association "schools" of chemistry were in their infancy, and that systematic instruction in the science was difficult to obtain. Another point of fundamental importance which has to be borne in mind is that the masters of the subject were then for the most part solitary workers.

It is difficult for us, looking back through the years, to realise what it must have meant to search for truth under conditions which were discouraging, if not actually hostile. Yet, although his labours were often thankless and unrewarded, the chemist of the time was probably a riper philosopher and a finer enthusiast than his successor of to-day. He pursued his inquiries amid fewer distractions, and in many ways his lot must have been happy, save when tormented by the thought that a subject so potent as chemistry in developing the intellectual and material welfare of the community should remain neglected to an extent which to us seems incredible.

Public sympathy was lacking, Government support was negligible or grudgingly bestowed, and there was little or no co-operation between scientific chemistry and industry. As an unaided enthusiast the chemist was left to pursue his way without the stimulus, now happily ours, which comes from the feeling that work is supported by educated and enlightened appreciation.

Let me quote from one of Faraday's letters now in my possession and, so far as I can trace, unpublished. Writing to a friend immediately before the foundation of the British Association, he relates that a manufacturer had adopted a process developed in the course of an investigation carried out in the Royal Institution. The letter continues: "He" (the manufacturer) "writes me word that, having repeated our experiments, he finds the product very good, and as our information was given openly to the world he, as a matter of compliment, has presented me with some pairs of razors to give away." If ever there was a compliment

<sup>1</sup> From Part I. of the presidential address delivered to Section B (Chemistry) of the British Association at Hull on Sept. 7.