AN INTRODUCTION TO THE THEORY OF NUMBERS*

BY G. H. HARDY

PART I

1. *Farey Series.* The theory of numbers has always occupied a peculiar position among the purely mathematical sciences. It has the reputation of great difficulty and mystery among many who should be competent to judge; I suppose that there is no mathematical theory of which so many well-qualified mathematicians are so much afraid. At the same time it is unique among mathematical theories in its appeal to the uninstructed imagination and in its fascination for the amateur. It would hardly be possible in any other subject to write books like Landau's *Vorlesungen* or Dickson's *History*, six great volumes of overwhelming erudition, better than the football reports for light breakfast table reading.

The excursions of amateur mathematicians into mathematics do not usually produce interesting results. I wish to draw your attention for a moment to one very singular exception. Mr. John Farey, Sen., who lived in the Napoleonic era, has a notice of twenty lines in the *Dictionary of National Biography*, where he is described as a geologist. He received as a boy "a good mathematical training". He was at one time agent to the Duke of Bedford, but afterwards came to London, where he acquired an extensive practice as a consulting surveyor, which led him to travel much about the country and "collect minerals and rocks". His principal work was a geological survey of Derbyshire, undertaken for the Board of Agriculture, but he also wrote papers in the *Philosophical Magazine*, on geology and on many other subjects, such as

* The sixth Josiah Willard Gibbs Lecture, read at New York City, December 28, 1928, before a joint session of the American Mathematical Society and the American Association for the Advancement of Science.

music, sound, comets, carriage wheels and decimal coinage. As a geologist, Farey is apparently forgotten, and, if that were all there were to say about him, I doubt that he would find his way into the *Dictionary of National Biography* today.

It is really very astonishing that Farey's official biographer should be so completely unaware of his subject's one real title to fame. For, in spite of the *Dictionary of National Biography*, Farey is immortal; his name stands prominently in Dickson's *History* and in the German encyclopaedia of mathematics, and there is no number-theorist who has not heard of "Farey's series". Just once in his life Mr. Farey rose above mediocrity and made an original observation. He did not understand very well what he was doing, and he was too weak a mathematician to prove the quite simple theorem he had discovered. It is evident also that he did not consider his discovery, which is stated in a letter of about half a page, at all important; the editor of the Philosophical Magazine printed a very stupid criticism in the next volume, and Farey, usually a rather acrid controversialist, ignored it completely. He had obviously no idea that this casual letter was the one event of real importance in his life. We may be tempted to think that Farey was very lucky; but a man who has made an observation that has escaped Fermat and Euler deserves any luck that comes his way.*

Farey's observation was this. The *Farey series of order* n is the series, in order of magnitude, of the irreducible rational fractions between 0 and 1 whose denominators do not exceed n. Thus

$$\frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2},$$
$$\frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{1}{1}$$

* It should be added that Farey's discovery had been anticipated 14 years before by C. Haros: see Dickson's *History*, vol. 1, p. 156. Cauchy happened to see Farey's note and attributed the theorem to him, and everyone else has followed Cauchy's example.

is the Farey series of order 7. There are two simple theorems about Farey series; (1) if p/q and p'/q' are two consecutive terms, then

$$p'q - pq' = 1,$$

and (ii) if p/q, p'/q', p''/q'' are three consecutive terms, then

$$\frac{p'}{q'} = \frac{p + p''}{q + q''}.$$

The second theorem (which is that actually stated by Farey) is an immediate consequence of the first, as we see by solving the equations

$$p'q - pq' = 1, \quad p''q' - p'q'' = 1,$$

for p' and q'.

The theorems are not of absolutely first class importance, but they are not trivial, and all of the many proofs have some feature of real interest. One of the simplest uses the language of elementary geometry. We consider the *lattice* or *Gitter* L in a plane formed by drawing parallels to the axes at unit distance from each other; the intersections, the points (x, y) with integral coordinates, are called the *points of the lattice*. It is obvious that the properties of the lattice are independent of the particular lattice point O selected as origin and symmetrical about any origin. The lattice is transformed into itself by the linear substitution

$$x' = \alpha x + \beta y, \quad y' = \gamma x + \delta y,$$

where α, β, γ, δ are integers and $\Delta = \alpha\delta - \beta\gamma = 1$, since then there is a pair x, y which give any assigned integral values for x', y'.

The area of the parallelogram P based on the origin and two lattice points (x_1, y_1), and (x_2, y_2), not collinear with O, is

$$\delta = \pm (x_1y_2 - x_2y_1).$$

We can construct a lattice L' (an oblique lattice) by producing and drawing parallels to the sides of P. A necessary and sufficient condition that L' should be equivalent to L, that is, that they should contain the same lattice points, is that $\delta=1$, that is, that δ should have its smallest possible value. It is clear that this is also a necessary and sufficient condition that *there should be no lattice point inside* P, and it is easy to see that if there is such a point inside P, there is one inside, or on the boundary of, the triangular half of P nearer to O.

We may call the lattice point (q,p) which corresponds to a fraction p/q in its lowest terms a *visible* lattice point; there is no other lattice point which obscures the view of it from O. Let us consider all the visible lattice points which lie inside, or on the boundary of, the triangle bounded by the lines $y=0$, $x=n$, $y=x$. It is plain that these points correspond one by one to the fractions of the Farey series of order n. When the ray R from O to (q, p) rotates from the x-axis to the line $y=x$, it passes through each of these points in turn. If we take two consecutive positions of R, corresponding to the points (q, p), (q', p'), the parallelogram based on these two points contains no lattice point inside it, since otherwise there would be a lattice point inside its nearer triangle, and therefore a Farey fraction between p/q and p'/q'. It follows that

$$\delta = p'q - pq' = 1,$$

which proves Farey's theorem.

2. *Purpose of this Lecture.* So much then for Farey's discovery; it is a curious theorem, and its history is still more curious; but I have no doubt allowed myself to dwell upon it a little longer than its intrinsic importance deserves. My discussion of it will, however, help me to explain what I am trying to do in this lecture.

I shall imagine my audience to be made up entirely of men like Farey. I know that most of them are very much better mathematicians, but I shall not assume so; I shall assume only that they possess the common school knowledge of arithmetic and algebra. But I shall also assume that, like Farey, they are curious about the properties of integral numbers; one need after all be no Ramanujan for that.

Let us then imagine such a man playing about with numbers (as so many retired officers in England do) and puzzling himself about the curious properties which they seem to possess. What odd properties would strike him? What are the first questions he would ask? We must not try to be very systematic; if we do, we shall make no progress in an hour. We must aim merely at a rough preliminary survey of the ground. If in the course of our survey, we find the opportunity for any illuminating remark, we may delay to make it, as I have already delayed over Mr. Farey, even if it does not seem to fall in quite its proper logical place. Then, if time permits, we may return to examine a little more closely any important difficulties which our preliminary survey has revealed.

3. *Congruences to a Modulus.* There is no doubt that the first general idea which we should have to explain is that of a *congruence.* Two numbers a and b are *congruent to modulus m* if they leave the same remainder when divided by m, that is, if m is a divisor of $a-b$. We write

$$a \equiv b \pmod{m}, \quad m \mid a - b.$$

It is obvious that congruences are of immense practical importance. Ordinary lite is governed by them; railway time tables and lists of lectures are tables of congruences. The absolute values of numbers are comparatively unimportant; we want to know what time it is, not how many minutes have passed since the creation.

A great many problems both of arithmetic and of common life depend upon the solution of congruences involving an unknown x, such as

$$a_0x^n + a_1x^{n-1} + \cdots + a_n \equiv 0 \qquad \pmod{m}.$$

Such congruences may be classified like algebraical equations, as linear, quadratic, $\cdots$, according to the value of n.

Our first instinct in dealing with congruences is to follow up the analogy with algebra. In algebra a linear equation has one root, a quadratic two, and so on. We find at once that there are obvious and striking contrasts; even the linear congruence suggests a whole series of problems, and a full discussion of quadratic congruences involves quite an imposing body of general ideas.

Let us take the simplest case, the linear congruence, and suppose first that we are concerned only with one particular modulus, such as 7 or 24. We have then an example of a genuinely finite mathematics. Congruent numbers have exactly the same properties and cannot be distinguished, and our mathematics contains only *a finite number of things.* In such a mathematics any problem can be solved by enumeration; we can solve $2x\equiv 5 \pmod 7$ by trying all possible values of x, and we find there is a unique solution, $x\equiv 6$. If we try to solve $2x\equiv 5 \pmod{24}$, we find that there is no solution; if I lecture every other day, I shall sooner or later lecture on Thursday, but if I lecture every other hour, I may never lecture at 5 P.M.

The difference is of course accounted for by the fact that 7 is *prime* and 24 is not. Here we encounter the notion of a prime, a number without factors, and all kinds of speculations suggest themselves. Can we tell, by any method short of trial of all possible divisors, whether any given number is prime or not? Are there formulas for primes? Are the primes infinite in number, and if so, what is the law of their distribution?

Again, it appears that all numbers are composed of primes, that primes are the ultimate material out of which the world of numbers is built up. We are bound to ask *how;* and here we meet our first big theorem, the "fundamental theorem of arithmetic," the theorem that factorization is unique. But we shall probably be wise to allow our enquirer to take this theorem for granted until he has acquired a little of the sophistication which comes with wider knowledge.

We may observe, however, before passing on, that the contrast between arithmetic and algebra becomes much more marked as soon as we consider congruences of higher degree. An equation of the fourth degree has, with appropriate conventions, just four roots. But

$$x^4 \equiv 1 \pmod{13}$$

has 4 roots, 1, 5, 8, and 12;

$$x^4 \equiv 1 \pmod{16}$$

has 8 roots, 1, 3, 5, 7, 9, 11, 13, and 15; and

$$x^4 \equiv 2 \pmod{16}$$

has none.

4. *Regarding Decimals.* I pass to another subject that has an irresistible fascination for amateurs, the subject of *decimals.* Some decimals are finite and some recurring, but it is easy to write down decimals, such as

(a) $0.10100100010 \cdots$ (b) $0.11010001000 \cdots$

which are neither. Here (a) the number of 0's increases by one at each stage, (b) the ranks of the 1's are $1, 2, 4, 8, \cdots$. More amusing examples are

(c) $0.01101010001010 \cdots$

(in which the 1's have prime rank) and

(d) $0.23571113171923 \cdots$

(formed by writing down the prime numbers in order). The proof for (c) demands the knowledge that there is an infinity of primes, and that for (d) rather more.*

The answer to some of the obvious questions is immediate. A finite decimal represents a rational fraction $p/(2^\alpha 5^\beta)$, a pure recurring decimal a fraction p/q, where q is not divisible by 2 or 5, and a mixed recurring decimal a fraction in which q is divisible by 2 or 5 and also by some other number. The converses of these theorems are also true, but the proof demands a little genuinely arithmetical reasoning. I shall state the proof in the simplest case, since it depends upon

* See Pólya and Szegö's *Aufgaben aus der Analysis*, vol. 2, pp. 160, 383.

the logical principle which is perhaps our most effective weapon in the elementary parts of the theory, where we are dealing with so simple a subject matter that our choice of arguments is naturally very restricted.

Suppose $p<q$ and q prime to 10. If we divide all powers 10^ν by q, there are only q possible remainders, and one at least must be repeated. It follows that there are a ν_1 and a $\nu_2>\nu_1$ such that

$$10^{\nu_2} \equiv 10^{\nu_1}, \quad 10^{\nu_1}(10^{\nu_2-\nu_1}-1) \equiv 0$$

to modulus q. It follows that, if we write $\nu_2-\nu_1=N$, we have $10^N\equiv 1$, so that $q \mid 10^N-1$ and

$$\frac{p}{q} = \frac{P}{10^N-1} = P\cdot 10^{-N} + P\cdot 10^{-2N} + \cdots .$$

Since $P<10^N$, this is a pure recurring decimal with a period of at most N. The principles which we have used are (a) that *if there are more than* q *things of at most* q *kinds, there must be two of them of the same kind*; (b) that if $10^\nu Q$ is divisible by q, and q is prime to 10, then Q is divisible by q. In the second we are of course appealing to the "fundamental theorem". The first is the general logical principle to which I referred just now.

Let us take a slightly more complicated variant of this principle. *If there are two sets of objects*

$$a_1, a_2, \cdots, a_m, \quad b_1, b_2, \cdots, b_m,$$

no two of either set being the same; and if every b *is equal to an* a; *then the* b'*s are the* a'*s arranged in a different order.* We may apply this principle to obtain further information about the period of our recurring decimal. I suppose now that q is prime. If q and a are given, and a is not a multiple of q, it is impossible that

$$ra \equiv sa \qquad (\text{mod } q)$$

unless $r\equiv s$. If (ra) is the remainder when ra is divided by q, the two sets

$$r, \quad (ra) \qquad (r = 1, 2, \cdots, q-1)$$

satisfy the conditions of our principle and are therefore the same except in order. It follows that

$$(q-1)!\,a^{q-1} \equiv \prod(ra) \equiv \prod r = (q-1)! \qquad (\text{mod } q),$$

and therefore that

$$a^{q-1} \equiv 1 \qquad (\text{mod } q)\ ;$$

Fermat's Theorem. In the particular case in which we are interested, a is 10, and Fermat's Theorem shows that we may take $N=q-1$, so that the period of p/q cannot exceed $q-1$ figures. Observe that we have appealed to the fundamental theorem twice in the proof.

It is familiar to everyone that $\frac{1}{7}$ has 6 figures, the maximum number. We are bound to ask what other primes q possess this property; the values of q less than 50 are in fact 7, 17, 19, 23, 29, and 47, but here we begin to get into deeper water. I cannot stop to discuss this question now, but before passing on I must mention another familiar text-book theorem which I shall have to quote later. This is Wilson's Theorem, that

$$(q-1)! + 1 \equiv 0 \qquad (\text{mod } q)$$

if and only if q is prime. Of the mass of proofs catalogued by Dickson, that of Dirichlet depends most directly on principles which we have used already. It is an immediate consequence of these principles that, if x is any one of the set $1, 2, \cdots, q-1$, there is just one other, y, such that $xy\equiv 1$ (mod q); we call y the *associate* of x. It is plain that 1 and $q-1$ are associated with themselves; and no other number can be, since $x_1^2\equiv x_2^2$ implies $x_1\equiv x_2$ or $x_1\equiv q-x_2$. It follows that the numbers $2, 3, \cdots, q-2$ are composed of $\frac{1}{2}(q-3)$ distinct pairs the product of each of which is congruent to 1. Hence

$$2\cdot 3 \cdots (q-2) \equiv 1^{(q-3)/2} = 1,$$
$$(q-1)! \equiv q-1 \equiv -1,$$

which is one half of Wilson's Theorem. The converse half is practically obvious, since $(q-1)!$ would be divisible by any factor of q.

5. *Algebraic and Transcendental Numbers.* The study of decimals leads directly to problems concerning *rationality and irrationality.* Our decimals such as $0.1010010001 \cdots$ must represent irrational numbers. What criteria are there for deciding whether a given number is rational or irrational? To ask this question is to go a little outside the theory of numbers proper, which is concerned first with integers, and then with rationals or irrationals of special forms, such as the form $a+b\sqrt{2}$, and not with irrationals as a whole or general criteria for irrationality. The problem is, however, one about which an amateur will certainly demand information.

The famous argument of Pythagoras shows that $\sqrt{2}$ is irrational; if a/b is in its lowest terms and $a^2=2b^2$, then a and b must both be even, a contradiction. It is obvious to us now that the Pythagorean argument extends at once to $\sqrt{3}$, $\sqrt{5}$, $\cdots$, $2^{1/3}$, $\cdots$, and generally to $N^{1/m}$, where N is any number which is not a perfect mth power. There is a curious and very instructive historical puzzle connected with this argument. There is a passage in Plato's *Theaetetus*, discussed at length by Heath in his *History of Greek Mathematics*, about the attempt of Theodorus to generalize Pythagoras's proof. Theodorus, working some 50 years after Pythagoras, proved the irrationality of $\sqrt{N}$ for all values of N (except square values) up to 17 inclusive. Why, ask the historians did he stop? Why in any case should it have taken mathematicians like the Greeks 50 years to make so obvious an extension? Zeuthen in particular expended a great deal of ingenuity upon this question, but I think that the ingenuity was misplaced, and that the answer is obvious.

Theodorus *did not know the fundamental theorem of arithmetic;* there is something of a puzzle about the history of that theorem, but it cannot have been known to the Greeks before Euclid's time. The triviality of the generalization to us is due entirely to our knowledge of this theorem. Suppose, for example, we wish to prove that

$$a^2 = 60b^2,$$

where a and b are integers without common factor, is impossible. We argue that a^2 cannot be divisible by 3 unless a is divisible by 3; hence $a=3c$, $a^2=9c^2$, $3c^2=20b^2$, and a repetition of the argument shows that b also is divisible by 3. We can prove that $3 \mid a^2$ implies $3 \mid a$ *without the fundamental theorem*, by enumeration of possible cases, considering separately the cases ın which $a \equiv 0, 1, 2 \pmod 3$. If it were 17 instead of 3, the process would be a little tedious; and in any case such a classification of numbers would have been very novel in Theodorus's time. I am so far from being puzzled by the limitations of his work that I regard what he did as a very remarkable achievement.

There are very few types of numbers which present themselves at all naturally in analysis and which can be proved to be irrational. It is obvious that a number like $\log_{10} 2$ is irrational, for a power of 2 cannot be a power of 10. The proof for e, from the exponential series, is quite easy, and that for e^2 not very much more difficult. That for π is decidedly more so, and when we come to numbers like e^3 and π^2, it ceases to be worth while to worry about elementary proofs; we may as well go the whole way and prove e and π are transcendental. The most famous constant in analysis, after e and π, is Euler's constant γ; and the proof of the irrationality of γ is one of the classical unsolved problems of mathematics. It has never been proved that $2^{\sqrt{2}}$, $3^{\sqrt{2}}$, and similar numbers are irrational; no plausible method for attacking such problems has even been suggested. I am inclined to think that the number which holds out the best hopes for new discovery is the number e^{π}, which presents itself so naturally in the formulas of elliptic functions.

I said just now that e and π were "transcendental". I must not stop to talk at length about this famous theorem of Lindemann,* which contains the final proof that the

* See for example Hobson's *Trigonometry*, third edition, p. 305, or the same author's *Squaring the Circle.*

quadrature of the circle, in the classical sense, is impossible; but the *statement* of the theorem introduces a notion that we shall require, that of an *algebraic number*. An algebraic number is the root of an equation

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0,$$

where the a's are integers. An *algebraic integer* is an algebraic number whose characteristic equation has unity for its leading coefficient. Thus $\sqrt{2}$ and $1+\sqrt{(-5)}$ are algebraic integers. A *transcendental* number is a number which is not algebraic; and Lindemann's Theorem is that π *is transcendental*. It is easy to show that all lengths which can be constructed by euclidean methods are algebraic, and indeed algebraic numbers of a quite special kind. If follows that the quadrature of the circle by any euclidean construction is impossible.

There is another direction in which we may be tempted to digress at this point, the theory of the approximation of irrationals by rationals, what is now called "diophantine approximation". There is just one theorem in this field that I shall mention, because it is connected so directly with what I have just been saying, and because it depends upon another of the stock arguments of number theory, the principle that *an integer numerically less than* 1 *is* 0. This is Liouville's theorem, that *there are transcendental numbers*. It is naturally much easier to prove this than to prove that a given number such as π is transcendental.

Liouville proves first that *it is impossible to approximate rationally to an algebraic number with more than a certain accuracy*. It is quite easy to see why. Suppose that ξ is an algebraic number defined by

$$f(\xi) = a_0\xi^n + a_1\xi^{n-1} + \cdots + a_n = 0.$$

We may suppose that the equation is irreducible, that is to say that $f(\xi)$ cannot be resolved into simpler algebraic factors of similar form; in this case we say that ξ is *of degree* n. We can obviously find a number M, depending only on ξ, such that

$$|f'(x)| < M$$

for x near ξ. Suppose now that p/q is a rational, near ξ. Then

$$f\left(\frac{p}{q}\right) = \frac{N}{q^n},$$

where N is an integer not zero. It follows from our general principle that $|N| \geqq 1$ and

$$\left|f\left(\frac{p}{q}\right)\right| \geqq \frac{1}{q^n}.$$

But

$$f\left(\frac{p}{q}\right) = f\left(\frac{p}{q}\right) - f(\xi) = \left(\frac{p}{q} - \xi\right)f'(\eta),$$

where η lies between p/q and ξ. Hence, for all q,

$$\left|\frac{p}{q} - \xi\right| = \left|\frac{f(p/q)}{f'(\eta)}\right| > \frac{1}{Mq^n}.$$

It is impossible to approximate rationally to an algebraic number of degree n with an order of accuracy higher than q^{-n}.

On the other hand it is easy to write down numbers which have rational approximations of much higher accuracy than this; we have only to take a decimal of 0's and 1's in which the 1's are spaced out sufficiently widely. Thus

$$\xi = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots = .11000100000 \cdots$$

is approximated by its first k terms, that is, by a fraction

$$\frac{p}{q} = \frac{p}{10^{k!}}$$

with an error of order $10^{-(k+1)!} = q^{-k-1}$. Hence it is not an algebraic number of degree k and, since k is arbitrary, it must be transcendental. Obviously Liouville's argument enables us to *construct* transcendental numbers as freely as we please.

6. *Arithmetic. Forms.* The theory of irrationals starts from Pythagoras, and there is another great branch of the theory of numbers which also starts from him and about which I must now say something. This is the theory of *forms.*

Our interest in the theory of forms begins when we observe that there are Pythagorean triangles with integral sides; thus $3^2+4^2=5^2$. The first problem which suggests itself is that of determining all such triangles, and the solution given in substance by Diophantus, is easy. All the integral solutions of

$$x^2 + y^2 = z^2$$

are given by

$$x = \lambda(\xi^2 - \eta^2), \qquad y = 2\lambda\xi\eta, \qquad z = \lambda(\xi^2 + \eta^2),$$

where the letters are integers and ξ and η are coprime and of opposite parity. This problem is trivial, but it suggests an infinity of others.

It is natural to begin by a generalization of the problem. Let us discard the hypothesis that the hypotenuse z is integral; then

$$n = z^2 = x^2 + y^2$$

is the sum of two squares, and we are led to ask what numbers n possess this property. This is the first and simplest problem in the theory of *quadratic forms,* and the answer to it shows that no such problem can be quite easy. Even linear forms are not quite trivial; the solution of $ax+by=n$ in integers is a quite interesting elementary problem. When we consider quadratic forms, we come up against difficulties of a different order.

The first theorem in the subject is another theorem of Fermat, that *$x^2+y^2=n$ is soluble when n is a prime $p=4m+1$* and, apart from trivial variations of the sign and order of x and y, uniquely. It is to be observed that the equation is plainly insoluble when n is $4m+3$, since any square is congruent to 0 or 1 to modulus 4. This theorem is one of the most famous in the theory of numbers, and very rightly so, since it was the first really difficult theorem in the subject proved by any mathematician. There is no really simple proof, and the most natural, that which depends on the Gaussian numbers $a+bi$, introduces a whole series of ideas of revolutionary importance.

The first stage of the proof consists in proving that *there is a number x such that*

$$x^2 \equiv -1 \qquad (\text{mod } p),$$

or $p|1+x^2$. Let us go back for a moment to the proof I sketched of Wilson's Theorem. Let us associate the numbers $x=1, 2, \cdots, p-1$ in pairs x, y not, as then, so that $xy\equiv 1$, but so that

$$xy \equiv -1 \qquad (\text{mod } p).$$

If any x is associated with itself, our proposition is established. If not, we have arranged the numbers from 1 to $p-1$ in $\frac{1}{2}(p-1)$ pairs of different numbers each satisfying the condition. Hence

$$(p-1)! \equiv \prod xy \equiv (-1)^{(p-1)/2} = 1;$$

which is false, since, by Wilson's Theorem,

$$(p-1)! \equiv -1.$$

We thus obtain our proposition by reductio ad absurdum.

The second stage of the proof depends on much more novel ideas. We are concerned with the simplest case of an *algebraic field*. The field $K(i)$ is the aggregate of numbers

$$\xi = r + si = r + s\sqrt{(-1)},$$

where r and s are rational. This number satisfies the equation

$$\xi^2 - 2r\xi + r^2 + s^2 = 0,$$

and is an algebraic integer, in the sense I defined before, when $2r$ and r^2+s^2 are integers, that is, when r and s are integers. We may denote by $K^*(i)$ the aggregate of all the integers

$$\alpha = a + bi$$

of $K(i)$; a and b are ordinary integers. The numbers of $K^*(i)$ reproduce themselves by addition and multiplication, and we can define division in this field just as we define it in ordinary arithmetic. We can also define a *prime* of $K^*(i)$, and factorization of numbers into primes. There are four numbers, ± 1 and $\pm i$, which play a part in the new arithmetic similar to that of 1 and -1 in ordinary arithmetic. These are the "unities" or divisors of 1. If we define the *norm* of $\alpha = a + bi$ as

$$N(\alpha) = a^2 + b^2,$$

then the unities are characterized by the fact that their norm is 1. We do not count them as primes, just as, in the ordinary theory, we do not count 1 as a prime.

We now make an assumption, namely that *the analog of the fundamental theorem holds in the field* $K^*(i)$, that is to say that, apart from any trivial complications which may be introduced by the unities, *the factorization of a number of* $K^*(i)$ *into primes is unique.* This assumption is in fact correct. Returning now to the first stage of our proof, there is an x such that

$$p \mid 1 + x^2 = (1 + ix)(1 - ix).$$

It is obvious that p does not divide $1+ix$ or $1-ix$, so that *p divides the product of two numbers without dividing either of them.* Hence p cannot be a prime in $K^*(i)$. We may therefore write

$$p = \pi\lambda,$$

where $N(\pi) > 1$ and $N(\lambda) > 1$. But

$$N(\pi)N(\lambda) = N(p) = p^2,$$

so that $N(\pi)$ and $N(\lambda)$ must each be p. If we write

$$\pi = a + ib,$$

it follows that

$$p = N(\pi) = a^2 + b^2,$$

which is Fermat's theorem.

We may be tempted by our success to further efforts in the same direction. It is easy to satisfy ourselves, by considering particular cases, that *any prime* $p=20m+1$ *is of the form* a^2+5b^2: thus $61=4^2+5\cdot 3^2$. Let us try to prove this theorem by a similar method. We must evidently consider now the field $K^*[\sqrt{(-5)}]$ formed of the algebraic integers of the form

$$\alpha = a + b\sqrt{(-5)} \ ;$$

it is easy to show that such a number is an algebraic integer if and only if a and b are ordinary integers. There is no difficulty in defining divisibility and primality in this field also.

The first step in our proof must plainly be to prove the existence of an x for which $p\,|\,1+5x^2$. This is not difficult, but it demands a little more knowledge of quadratic congruences than I can assume, and I must take it for granted.

We define the norm $N(\alpha)$ of a number of this field as a^2+5b^2. We then argue as before; we have

$$p\,|\,1 + 5x^2 = (1 + x\sqrt{(-5)})(1 - x\sqrt{(-5)}),$$

so that p divides a product without dividing either factor and is therefore not a prime. Hence, as before $p=\pi\lambda$, where $N(\pi)>1$ and $N(\lambda)>1$, and $N(\pi)$ and $N(\lambda)$ must each be p. It follows that

$$p = N(\pi) = a^2 + 5b^2,$$

the theorem we set out to prove.

At this point, however, there is a shock in store for us; we find that we can prove *too much*. The number

$$q = (2 + \sqrt{(-5)})(2 - \sqrt{(-5)})$$

is divisible by 3, while neither factor is so. Hence 3 is not a prime. Hence

$$3=\pi\lambda, \quad 9=N(\pi)N(\lambda),$$

and $N(\pi)$ and $N(\lambda)$ are each 3. It follows that

$$3 = N(\pi) = a^2 + 5b^2.$$

Similarly we can prove that

$$7 = a_2 + 5b_2;$$

and both of these theorems are obviously false.

There must therefore be a mistake somewhere in our argument, and if you examine it, and are prepared to believe that I have not been misleading you wilfully, you will see that there is only one step which can be questioned. In all three cases I concluded the argument by an appeal to the same theorem; *a number which divides the product of two numbers without dividing either of them cannot be prime.* This is true in ordinary arithmetic, because of the fundamental theorem; if 7 were a divisor of $15 = 3 \cdot 5$, 15 would be factorable into primes in two distinct manners. It follows that *the analog of the fundamental theorem in the field* $K^*[\sqrt{(-5)}]$ *must be false*; and this is easily verified when once our suspicions have been excited; thus

$$2 \cdot 3 = (1 + \sqrt{(-5)})(1 - \sqrt{(-5)}),$$

$$3 \cdot 7 = (1 + 2\sqrt{(-5)})(1 - 2\sqrt{(-5)}),$$

and all of these numbers are prime in $K^*[\sqrt{(-5)}]$. The proof which I gave of the theorem concerning primes $20m+1$ was therefore fallacious, although the theorem is true. The proof of Fermat's theorem, on the other hand, was correct, since factorization *is* unique in $K^*(i)$.

7. *Further Problems.* It is clear that we must go back to the beginning and study the theory of primes a little more closely; but before I do this I should like to call your attention to a series of further problems suggested by Fermat's theorem. We know now when a *prime* is the sum of two squares, and we have to consider the same problem for general n. Here in fact there are three different problems.

The first and most obvious problem is that of determining the necessary and sufficient conditions that n should be representable. This problem may be solved quite easily with the aid of the Gaussian numbers; n must be $2^\alpha M^2 N$, where α is 0 or 1 and N contains prime factors of the form

$4m+1$ only. We are then led naturally to the corresponding problem for other forms, first for the general binary quadratic form

$$ax^2 + bxy + cy^2,$$

then for quadratic forms in a larger number of variables, such as

$$x^2 + y^2 + z^2, \quad x^2 + y^2 + z^2 + t^2,$$

and then for forms of higher degree, such as x^3+y^3 and x^4+y^4. There is a highly developed theory of the general quadratic form; the most famous theorem is perhaps Lagrange's theorem, that *every number is the sum of four squares.* But as soon as we begin to consider cubic or higher forms we find ourselves on the boundary of knowedge. There is for example no criterion analogous to Fermat's by which we can decide whether a given number is the sum of two cubes.

The second problem about the form x^2+y^2 suggested by Fermat's theorem is that of determining the *number of representations.* This problem may be interpreted in two different ways. We may want an exact formula, in terms of the factors of n, and in this case the Gaussian theory again gives what we want; $r(n)$, the number of representations, is given by the formula

$$r(n) = 4\{d_1(n) - d_3(n)\},$$

where $d_1(n)$ and $d_3(n)$ are the numbers of divisors of n of the forms $4m+1$ and $4m+3$ respectively. This is, however, not the most interesting interpretation of the problem. We may want, not a formula like this, but information concerning the *order of magnitude* of $r(n)$, whether $r(n)$ is generally large when n is large, whether numbers are usually representable freely or with difficulty. In this case our formula gives us very little help, and the solution of the problem requires quite different methods.

It is here that we come into contact for the first time with a new branch of the theory, the modern "analytic" theory.

This theory has two special characteristics. The first is one of method; it uses, besides the methods of the classical theory, the methods of the modern theory of functions of a complex variable. The second is that it is concerned primarily with problems of order of magnitude and asymptotic distribution. The distinction is not a perfectly sharp one; there are "exact", "finite" theorems which have only been solved by "analytic" methods. For example, *every number greater than* $10^{10^{10}}$ *is expressible as the sum of* 8 *cubes*; this theorem includes no reference to "order of magnitude", and is a "finite" theorem in just the same sense as Fermat's theorem about the squares, but the only known proof is analytic. On the whole, however, it is the problems of asymptotic distribution which dominate the theory.

The answer given by the analytic theory to the special question which I raised is roughly as follows. The average value of $r(n)$ is π. It must be observed that representations which differ only trivially, that is, in the sign or order of x and y, are reckoned as distinct. If we allow for this, the average number of representations is rather less than a half; this is explained by the fact that, as we shall see, *most* numbers are not representable. On the other hand $r(n)$ tends to infinity with n with tolerable rapidity for numbers of appropriate forms, more rapidly for example than any power of $\log n$. The corresponding problems for cubes or higher powers present difficulties which are at present quite insuperable, and all that I can do is to mention a few curiosities. The smallest number representable by two cubes in two really distinct ways is

$$1729 = 1^3 + 12^3 = 9^3 + 10^3,$$

and the smallest representable in three ways is probably

$$175959000 = 70^3 + 560^3 = 198^3 + 552^3 = 315^3 + 525^3.$$

It can be proved that there exist numbers with as many different representations as we please. A. E. Western has carried out very heavy computations concerning representations by cubes; he has for example found 6 numbers, of which the smallest is 1,259,712, representable as the sum of *three* cubes in *six* different ways. The smallest number doubly representable by two fourth powers is probably

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

there is, so far as I know, no known example of a number with three such representations, nor any proof that such a number exists.

The nature of the problems of the analytic theory becomes clearer when we consider the third problem suggested by Fermat's theorem. This is the problem of determining the *distribution* of the representable numbers. We want to know *how many numbers are representablε*, or, to put it more precisely, how many numbers less than a large assigned number x are representable. If $Q(x)$ is the number of such numbers, what is the order of magnitude of $Q(x)$? Are nearly all numbers representable, or just a majority, or only a few? The answer is in fact that $Q(x)$ is approximately

$$\frac{Ax}{(\log x)^{1/2}},$$

where A is a constant; to put it roughly, quite a lot of numbers are representable, but strictly an infinitesimal proportion of the whole. This explains why the average number of representations turned out to be less than one.

This problem about $Q(x)$ is a very interesting one, but there is another of the same kind which is obviously still more interesting and much more fundamental. This is the problem of the distribution of the primes themselves; *how many primes are there less than x?* I shall say something about this problem in a moment; it is in any case time for us to return to the theory of primes, since all our enquiries have ended in questions about them, and it is obviously impossible to make serious progress until we know more both of their elementary properties and of the laws which govern their distribution.

PART II

8. *The Fundamental Theorem.* The *fundamental theorem* of arithmetic is the beginning of the theory of numbers, and it is plain that our first task must be to make this theorem secure.

There is another historical puzzle about the fundamental theorem. Who first stated the theorem, explicitly and generally? The natural answer is *Euclid*, since the *Elements* contain all the materials for the proof. Everything rests on Euclid's famous algorithm for the greatest common divisor. Given two numbers a, b, of which a is the greater, we form ιhe table

$$a = bc + b_1, \qquad b = b_1c_1 + b_2, \qquad b_1 = b_2c_2 + b_3, \cdots$$

where $b_1, b_2, \cdots$, are the remainders in the ordinary sense of elementary arithmetic. Since

$$b > b_1 > b_2 > \cdots,$$

b_n must sooner or later be zero. The last positive remainder δ has the properties implied by the words *greatest common divisor*, and it follows from the process by which δ is formed that any number which divides both a and b divides δ.

Let us note in passing that there is an analogous process in $K^*(i)$, but that the analogy fails in $K^*[\surd(-5)]$. In ordinary arithmetic, given a and b, we can find a number congruent to a mod b and less than b. There is a similar theorem for the Gaussian numbers. Here there is no strict order of magnitude between different numbers, and we have to use the order of magnitude of their norms. Given α and β, there is a number, congruent to α mod β, whose norm is less than that of β. There is no such theorem in $K^*[\surd(-5)]$, and the process analogous to Euclid's fails.

When the existence of δ is once established, the proof of the fundamental theorem is easy. We write

$$\delta = (a, b)$$

and we say that a is prime to b when $(a, b) = 1$. The crucial lemma is that *if* $(a, b) = \lambda$ *and* $b \mid ac$, *then* $b \mid c$; in particular, *a prime cannot divide a product without dividing one or other of* *the factors.* This once granted, anybody can construct the proof of the fundamental theorem for himself; and you will remember that it was just this proposition which led to our troubles in $K^*[\sqrt{(-5)}]$.

The lemma itself may be proved as follows. We construct the euclidean algorithm for a and b, with the final remainder 1. If we multiply it throughout by c, we have the algorithm for ac and bc, and the final remainder is c. It follows that

$$(ac, bc) = c.$$

Since b divides ac, by hypothesis, and also bc, it divides c.

This is Euclid's own argument, and with it he had proved what is essential in the fundamental theorem. It is a very singular thing that he should then omit to state the magnificent theorem that he has proved. He is over the line and free, but apparently disdains the formality of touching down. I do not know of any formal statement of the theorem earlier than Gauss. The substance of the theorem, however, is in the *Elements*; it was plainly unknown, as I explained before, to the Greeks from 50 to 100 years before Euclid's time; and I see no particular reason for questioning the obvious view that it is Euclid's own.

As soon as we have proved the fundamental theorem our elementary knowledge falls into line. The theory of linear congruences, the theorems of Fermat and Wilson and all their consequences, the elementary theory of decimals and of the divisors of numbers, may be developed straightforwardly and without the introduction of essentially new ideas. I can now say something about the more modern side of the theory of primes.

9. *Problems Concerning Primes.* What are the most natural questions to ask about primes? I say deliberately the most *natural*; we must remember that a natural question does not always seem, on fuller reflection, to have been a *reasonable* one. It is natural to an engineer to ask us for a finite formula for

$$\int e^{-x^2}dx,$$

or for a solution of some simple looking differential equation in finite terms. If we fail to satisfy him, it is not because of our stupidity, but because the world does not happen to have been made that way.

So, if any one asks us (1) *to give a general formula for the nth prime* p_n, a formula in the sense in which

$$p_n = n^2, \quad p_n = n^2 + 1, \quad p_n = [e^n],$$

where $[x]$ denotes the integral part of x, would be a formula, I can only reply that it is not a reasonable question. It is, I will not say demonstrably impossible, but wildly improbable, that any such formula exists. The distribution of the primes is not like what it would have to be on any such hypothesis. I should make the same reply to a good many other questions which an amateur might be likely to ask, for example if he asked me (2) *to give a rule for finding the prime which immediately follows a given prime.* It would of course be perfectly reasonable that he should press me for the reasons why I gave so purely a negative a reply. On the other hand the problem (3) *to find the number of primes below a given limit* is, if interpreted properly, an entirely reasonable and a soluble problem. The problems (4) *to prove that there are infinitely many pairs of primes differing by* 2, and (5) *to prove that there are infinitely many primes of the form* n^2+1, are also entirely reasonable, and if (as is the case) we cannot solve them, it is quite reasonable to condemn our lack of ingenuity.

10. *The Distribution of Primes.* If we wish to classify these problems and to decide which of them are reasonable and which are not, the first essential is to understand broadly the present state of knowledge about the distribution, the distribution *in the large* or *asymptotic* distribution, of the primes. It is this theory which gives the solution of problem (3).

We denote by $\pi(x)$ the number of primes not exceeding

x. The first step is to prove that (a) *the number of primes is infinite*; $\pi(x)$ *tends to infinity with* x. This is another of Euclid's great contributions to knowledge, and Euclid's proof is perhaps the classical example of proof by reductio ad absurdum. If the theorem is false, we may denote the primes by $2, 3, 5, \cdots, P$, and all numbers are divisible by one of these. On the other hand the number

$$(2\cdot 3\cdot 5 \cdots P) + 1$$

is obviously not divisible by any of $2, 3, \cdots, P$, and this is a contradiction.

Another very interesting proof is due to Pólya.* It is easy to see that any two of the numbers

$$2 + 1, 2^2 + 1, 2^4 + 1, \cdots, u_n = 2^{2^n} + 1$$

are prime to each other. For suppose that p is an odd prime and that $p \mid u_n$, $p \mid u_{n+k}$. Then also

$$p \mid 2^{2^{n+k}} - 1 = u_{n+k} - 2,$$

since

$$x^{2^k m} - 1$$

is algebraically divisible by $x^m + 1$, and therefore

$$p \mid u_{n+k} - (u_{n+k} - 2) = 2,$$

which is absurd. It follows that the number of primes less than u_n is at least n, and therefore that the number of primes is infinite. In fact the argument shows not merely that $\pi(x) \to \infty$ but that

$$\pi(x) > A \log \log x,$$

where A is a constant. Something in this direction, though a little less, can be proved by a refinement of Euclid's argument.

There is a third line of argument which is a little less elementary but may be made to prove a good deal more.†

* See Pólya and Szegö, loc. cit., pp. 133, 342.

† See Dickson's *History*, vol. 1, p. 414, where the proof is attributed to Auric.

If 2, 3, 5, $\cdots$, P were the only primes, then every number would be of the form

$$2^a 3^b 5^c \cdots P^k.$$

If this number is less than x, then a fortiori 2^a is less than x, so that a is less than a constant multiple of $\log x$, and the same argument applies to b, c, $\cdots$, k. The number of possible choices of a, b, $\cdots$, k is therefore less than a multiple of $(\log x)^\pi$, where π is the total number of primes. In other words the number of numbers less than x is less than

$$A(\log x)^\pi,$$

where A is a constant, and this is impossible, since x tends to infinity more rapidly than any power of log x. A refinement of the argument leads to the inequality

$$\pi(x) > A\frac{\log x}{\log\log x};$$

and the underlying principle may be stated roughly thus, that *if the number of primes were finite, there would not be enough numbers to go round.*

We are still a very long way from the ultimate truth. It is in fact possible to prove, and by comparatively elementary methods, that *the order of magnitude of* $\pi(x)$ *is* $x(\log x)^{-1}$. This theorem, conjectured by Legendre and Gauss, was first proved by Tchebycheff in 1848.

There are two much earlier theorems of Euler which point in this direction. The first is the theorem that (b) *the series*

$$\sum\frac{1}{p}$$

extended over all prime numbers p, *is divergent.* The proof of this theorem depends upon an identity, also due to Euler, upon which the whole of the modern theory of primes is founded. The identity is

$$1^{-s} + 2^{-s} + 3^{-s} + \cdots = \sum n^{-s}$$
$$= \frac{1}{(1-2^{-s})(1-3^{-s})(1-5^{-s})\cdots}$$
$$= \prod\left(\frac{1}{1-p^{-s}}\right)$$

and is valid for $s > 1$; it is at bottom merely the analytical expression of the fundamental theorem, and its importance arises from the fact that it asserts the equivalence of two expressions of which one contains the primes explicitly while the other does not. From Euler's identity we deduce (b) roughly as follows: if $\sum p^{-1}$ were convergent, then

$$\prod\left(\frac{1}{1-p^{-1}}\right)$$

would be convergent, and therfore $\sum n^{-1}$ would be convergent, which is false. Of course the proof really needs a rather more careful statement.

Euler's second theorem is (c) *the quotient of* $\pi(x)$ *by* x *tends to zero*; or in symbols

$$\frac{\pi(x)}{x} \rightarrow 0\,,$$

or, as we write it now

$$\pi(x) = o(x).$$

The proportion of primes is ultimately infinitesimal, "*almost all*" *numbers are composite.* The theorem is a quite simple corollary of (b); roughly, if we remove from the numbers less than x all multiples of the primes $2, 3, \cdots, p$, other than these primes themselves, we are left something like

$$x\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\cdots\left(1-\frac{1}{p}\right)$$

numbers. The product multiplying x tends to zero when

$p \to \infty$, because of (b), and from this we can deduce Euler's second theorem.

It is rather curious that, although Euler's second theorem is a corollary of the first, the lessons which we learn from the two theorems concerning the distribution of the primes have exactly opposite tendencies. The second theorem tells us that the number of primes below a given limit is *not too great*, that the primes are in the end rather liberally spaced out; it is in fact exactly equivalent to the theorem that (d) *the nth prime p_n has an order of magnitude greater than n*, or

$$\frac{p_n}{n} \to \infty .$$

If on the other hand the order of magnitude of p_n were *much* greater than n, if it were for example n^2 or $n^{10/9}$ or $n(\log n)^2$, then the series $\sum p_n^{-1}$ would be *convergent*, which is just what Euler's first theorem denies. What we learn from the two theorems together is something like this. If, as we hope, the true order of magnitude of p_n can be measured by some simple function $\phi(n)$, then that function must be of order higher than n, but somewhere near the boundary of convergence of the series

$$\sum \frac{1}{\phi(n)} \cdot$$

The' most obvious function which satisfies these requirements is $n \log n$, and to say that p_n is of order $n \log n$ is the same thing as to say that $\pi(x)$ is of order $x(\log x)^{-1}$. This is just what is asserted by Tchebycheff's theorem.

11. *Tchebycheff's Theorem.* The formal statement of Tchebycheff's theorem is (e) *the order of magnitude of $\pi(x)$ is $x(\log x)^{-1}$; there are constants A and B such that*

$$\frac{Ax}{\log x} < \pi(x) < \frac{Bx}{\log x} \cdot$$

This theorem is precisely equivalent to (f) *the order of magnitude of p_n is $n \log n$; there are constants A and B such that*

$$An \log n < p_n < Bn \log n.$$

The proofs of these theorems given by Tchebycheff have been simplified a good deal by Landau, and I can give you a sketch of one half of the proof which should enable you to understand without much difficulty the general character of the whole.

We begin by replacing $\pi(x)$ by another function. We can write $\pi(x)$ in the form

$$\pi(x) = \sum_{p \leqq x} 1 ;$$

count one for every prime up to x. A more convenient and really a more natural function is

$$\theta(x) = \sum_{p \leqq x} \log p,$$

the logarithm of the product of all primes up to x. This function seems at first sight a more complicated function, but it is easy enough to see why it is more convenient to work with. The most natural operation to perform on primes is *multiplication*, and this is the operation which we employ in forming $\theta(x)$. It is because it is natural to multiply primes and not to add or subtract them that problems like the problem of the prime pairs $(p, p+2)$, or Goldbach's problem of expressing numbers as sums of primes, turn out to be so terribly difficult.

Since $x/x^{1-\delta}$ tends to infinity, for any positive value of δ, we may expect that nearly all the primes which contribute to $\theta(x)$ will lie in the interval $(x^{1-\delta}, x)$, so that their logarithms lie between $(1-\delta) \log x$ and $\log x$. Hence we may expect $\theta(x)$ to be very much the same function as $\pi(x) \log x$, and in fact there is no difficulty in proving that

$$\theta(x) \sim \pi(x) \log x,$$

that is, that the ratio of the two functions tends to 1. It follows that the inequalities in (e) are equivalent to

$$Ax < \theta(x) < Bx.$$

I shall sketch the proof of the second inequality, which is rather the simpler.

Suppose that x is a power of 2, say 2^m. The primes between $x/2$ and x divide $x!$ but not $(x/2)!$, so that

$$\prod_{x/2<p\leqq x} p \,\Big|\, \frac{x!}{(x/2)!(x/2)!}.$$

The expression on the right is *one term* in the binomial expansion of $(1+1)^x=2^x$, and therefore

$$\prod_{x/2<p\leqq x} p \leqq 2^x.$$

Replacing x by

$$x/2,\ x/4;\ x/8,\ \cdots$$

and multiplying the results, we find that

$$\prod_{p\leqq x} p \leqq 2^{x+x/2+x/4+\cdots} \leqq 2^{2x},$$

and

$$\theta(x) \leqq 2\log 2\cdot x.$$

This proves the theorem when $x=2^m$. If

$$2^m<x<2^{m+1}$$

we have

$$\theta(x) \leqq \theta(2^{m+1}) \leqq 4\log 2\cdot 2^m < 4\log 2\cdot x.$$

Hence we may take $B=4 \log 2$. The proof of the second inequality is, as I said, not quite so simple, but does not involve essentially more difficult ideas. We have thus determined the order of magnitude of $\pi(x)$ and of p_n, and it is perhaps a little astonishing that a problem which sounds so abstruse should have so comparatively simple a solution.

12. *The Prime Number Theorem.* Tchebycheff's solution of the problem is, however, one with which it is impossible to remain content for long, since the whole trend of our discussion has been to suggest that much more is true than we have proved. In fact Tchebycheff's work, fine as it is, is the record of a failure; it is what survives of an unsuccessful attempt to prove what is now called the *Prime Number Theorem.*

This is the theorem that (g) *$\pi(x)$ and $x(\log x)^{-1}$ are asymptotically equivalent; the ratio of the two functions tends to unity.* We express this by writing

$$\pi(x) \sim \frac{x}{\log x} \cdot$$

The Prime Number Theorem is equivalent to

$$p_n \sim n \log n,$$

and we may express it very roughly by saying that *the odds are* log *x to* 1 *that a large number x is not prime.*

The Prime Number Theorem, the central theorem of the analytic theory of numbers, was proved independently by Hadamard and by de la Vallée-Poussin in 1896. The empirical evidence for its truth had for long been overwhelming, and I suppose that every number-theorist since Legendre had tried to prove it. The theorem differs from all those which I have discussed so far in that it is apparently impossible to prove it by properly elementary methods; there is no proof known which does not depend essentially on complex function theory. I do not mean to imply that there is any terrible difficulty in the proof; there are considerable difficulties of detail, but the fundamental ideas on which it depends are tolerably straightforward. They are, however, quite unlike any of those of which I have spoken, and I should require a whole lecture to explain them even to a strictly mathematical audience. Actually, a good deal more is known; it can be proved that $\pi(x)$ is approximated still more closely by the "logarithm-integral" of x,

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

that in fact

$$\pi(x) = \mathrm{Li}\, x + O\left\{\frac{x}{(\log x)^k}\right\}$$

for every k, the error being of lower order than the quotient of x by *any* power of $\log x$; and it is probable, though not yet proved, that the order of the error does not very materially exceed that of $\sqrt{x}$.

13. *Formulas for Primes.* I return now for a moment to a question which I discussed shortly before, the question whether it was reasonable to expect an "elementary formula" for the nth prime p_n. Let us imagine that my questioner was obstinate in his desire for such a formula; how could I refute his successive suggestions? If he suggested

$$p_n = n \log n,$$

I should have the obvious reply that $n \log n$ is not an integer. Suppose then that he modified his formula to

$$p_n = [n \log n].$$

I should reply that his formula did not agree with the known facts of the asymptotic theory. It agrees with $p_n \sim n \log n$, the first and most obvious deduction from the Prime Number Theorem itself; but the theory carries us much further; it enables us, for example, to show that

$$p_n = n \log n + n \log \log n + O(n),$$

which contradicts the formula. If, becoming more cautious, he asked me what ground I had for denying that p_n might be *some* elementary combination of

$$n,\ \log n,\ \log \log n,\ \cdots,$$

I should naturally find it harder to refute him, but I could advance three arguments which are enough in the aggregate to make up a tolerably convincing case. (i) Since Lix is a very good approximation to $\pi(x)$, the inverse function $\mathrm{Li}^{-1}n$ must be a very good approximation to p_n. Now it is demonstrable that neither the logarithm integral nor its inverse* is an elementary function. It is therefore very unlikely that there should be an elementary formula for p_n. (ii) If the "elementary formula" does not involve the symbol $[\cdots]$ of the "integral part", the function which it defines will generally not be integral for integral n. If it does, it loses all its simplicity and all its plausibility. (iii) An elementary function may be expected to behave with tolerable regularity at infinity, and so may all its *differences*. Now extremely little is known about the difference $p_{n+1}-p_n$ of two successive primes, but everything that is known, or seems probable from the evidence of the tables, suggests *extreme irregularity* in its behavior. The Prime Number Theorem shows that the *average* value of $p_{n+1}-p_n$ must be $\log n$, and tend to infinity with n. On the other hand there is overwhelming evidence that the smallest possible values of $p_{n+1}-p_n$, namely, 2, 4, 6, $\cdots$, recur indefinitely. It seems practically certain, not merely that there are infinitely many prime pairs $(p, p+2)$ but that there are infinitely many triplets $(p, p+2, p+6)$, and so with any combination of successive primes that is arithmetically possible; such a combination as $(p, p+2, p+4)$ is naturally not possible, since one of these numbers must be divisible by 3. All this seems hopelessly inconsistent with the existence of such a formula as was suggested, and it is clear that speculation in this direction is a waste of time.

There are, however, questions which have a somewhat similar tendency and which cannot be dismissed so summarily. There is one, for example, mentioned in Carmichael's little book. The problem, as he states it, is "*to find a prime greater than a given prime*," which might be interpreted as

* This may be deduced from general theorems proved recently by J. F. Ritt.

meaning either "*to find an elementary function $\phi(n)$ such that $\phi(n)\rightarrow\infty$ and $\phi(n)$ is prime for every n, or for all n beyond a certain limit*" or as meaning "*to find an elementary function $\phi(p)$ such that $\phi(p)>p$ and $\phi(p)$ is prime whenever p is prime.*" With either interpretation, it is a reasonable challenge, and the problem has not been solved.

Let us take the first form of the problem, which is perhaps the more natural, and let us begin by demanding *less*, namely that $\phi(n)$ shall be prime only for *an infinity of values of n*. In this case the problem becomes trivial, since n is a solution, by Euclid's theorem. It is, however, very interesting to observe that even then n, and certain simple linear functions such as $4n-1$ and $6n-1$, are the *only* trivial solutions. Dirichlet proved that *any* linear function $an+b$ has the property required, provided only that b is prime to a, or in other words that *every arithmetical progression* (subject to the last reservation) *contains an infinity of primes*. This theorem is quite difficult, except in a few special cases such as those which I mentioned, and it exhausts our knowledge in this particular direction. No one has ever proved that any of the functions

$$n^2+1,\quad 2^n-1,\quad 2^n+1$$

is prime for an infinity of values of n. With functions of *two* variables we can progress a good deal farther; we know for example that every quadratic form $am^2+bmn+cn^2$ contains an infinity of primes, provided of course that a, b, c have no common factor and that $b^2\neq 4ac$, and we can study the law of their distribution.

To find a $\phi(n)$ prime for *every* n is naturally still more difficult. Here linear functions are obviously useless, and no solution of any kind is known. Fermat conjectured that

$$2^{2^n}+1,$$

is always prime, but Euler proved that this is false, since

$$2^{32}+1 = 4294967297 = 641\cdot 6700417.$$

So far as I know, no one else has ever advanced any other suggestion which is even plausible.

In view of the apparently insuperable difficulties of this problem, there is a certain interest in *negative* results. It is plain, first, that $an+b$ cannot be prime for all n, or all large n. More generally, no polynomial

$$f(n) = a_0n^k + a_1n^{k-1} + \cdots + a_k$$

can be prime for all or all large n; for if $f(m) = M$ then $f(rn+m)$ is divisible by M for all r. There are entertaining curiosities in this field; thus

$$n^2 - n + 41$$

is prime for the first 41, and

$$n^2 - 79n + 1601$$

for the first 80 values of n. It is obvious that forms like

$$a^n - 1, \quad a^n + 1$$

cannot be prime for all large n, since, for example, $a^{3m}-1$ is divisible by a^m-1, and it is natural to suppose that the same is true for

$$P(n, 2^n, 3^n, 4^n, \cdots, k^n),$$

where P is any polynomial with integral coefficients.†

14. *The Fundamental Theorem in an Algebraic Field.* I must not allow myself to succumb to the temptation of talking too long about the theory of the distribution of primes, which is after all only one chapter in arithmetic. There are other topics about which our imaginary enquirer will certainly demand more information, and of these I think one stands out; it is certain that he will want fuller explanations about the field $K^*[\sqrt{(-5)}]$ and the other algebraic fields in which the analog of the fundamental theorem fails. All ordinary arithmetic depends, it seems, upon the fundamental theorem; how then can there *be* an arithmetic in a field in

† Morgan Ward of Pasadena has found a very simple proof of this theorem.

which it is false? It would seem that the arithmetic of such a field can bear no real resemblance to ordinary arithmetic. I shall spend the rest of my time in an attempt to explain, in the very broadest outline, how order is restored.

I shall begin by quoting a remark of Hilbert which is trivial in itself but which shows us at once the direction in which we must look for a solution. Consider the numbers

$$1,5,9,13,17,21,\cdots$$

of the form $4m+1$. These numbers form a group for multiplication (though naturally not for addition), and we can define divisibility and primality in the group. The "primes" are the numbers

$$5,9,13,17,21,29,33,37,41,49,\cdots$$

which are greater than 1, of the form $4m+1$, and not decomposable into factors of this form. Thus 21, 57, 77, and 209 are "primes"; but

$$4389 = 21\cdot 209 = 57\cdot 77,$$

so that a number of the group may be resolved into "prime" factors in different ways.

In this case the solution of the mystery is obvious. The "fundamental theorem" fails *because of the absence from the group of the numbers* $4m+3$ *of ordinary arithmetic.* In fact

$$21 = 3\cdot 7,\quad 57 = 3\cdot 19,\quad 77 = 7\cdot 11,\quad 209 = 11\cdot 19$$

and

$$21\cdot 209 = (3\cdot 7)(11\cdot 19) = (3\cdot 19)(7\cdot 11) = 57\cdot 77.$$

We cannot give a proper account of the properties of the numbers $4m+1$ so long as we insist on excluding the numbers $4m+3$; *the numbers* $4m+1$ *do not form by themselves an adequate basis for arithmetic.* This observation has of course no intrinsic interest, since no reasonable person would expect that they would do so. It is trivial in itself, but it is not at all trivial in its suggestion, since it suggests that the troubles of the field $K^*[\surd(-5)]$ may be remedied *by considering the field as part of some larger field.*

This is in fact the solution found by Kummer. We consider the field $L[\surd(-5)]$ of numbers

$$\xi = \surd(a + b\surd(-5)),$$

where a and b are ordinary integers. This is only an approximate statement; we do not actually consider all such numbers, but only those satisfying certain further conditions; the greatest common divisor of a and b must be a square or five times a square, and a^2+5b^2 must be a square. The field L includes K^*. The numbers of L form a group for multiplication, and we can define divisibility and primality in the field. Finally, the analog of the fundamental theorem is valid; *factorization is unique in L.* The proof of this is quite simple, but requires a little attention to detail, and I must refer you for the details to Mordell's tract on *Fermat's Last Theorem.*

We can now give a simple account of the equations in $K^*(\surd(-5))$ which puzzled us before. Consider for example the equation

$$3\cdot 7 = (1 + 2\surd(-5))(1 - 2\surd(-5)).$$

It is easily verified that

$$3^2=(2+\surd(-5))(2-\surd(-5)),$$

$$7^2=(2+3\surd(-5))(2-3\surd(-5)),$$

$$(1+2\surd(-5))^2=-19+4\surd(-5)=-(2-\surd(-5))(2+3\surd(-5)),$$

$$(1-2\surd(-5))^2=-19-4\surd(-5)=-(2+\surd(-5))(2-3\surd(-5)).$$

Hence, if we write

$$\alpha = \surd(2 + \surd(-5)), \qquad \alpha' = \surd(2 - \surd(-5)),$$

$$\beta = \surd(2 + 3\surd(-5)), \qquad \beta' = \surd(2 - 3\surd(-5)),$$

we have

$$3 = \alpha\alpha',\ 7 = \beta\beta',\ 1 + 2\sqrt{(-5)} = -\alpha'\beta,\ 1 - 2\sqrt{(-5)} = -\alpha\beta',$$

$$3 \cdot 7 = \alpha\alpha' \cdot \beta\beta' = \alpha'\beta \cdot \alpha\beta' = (1 + 2\sqrt{(-5)})(1 - 2\sqrt{(-5)})\ ;$$

and all of these equations are entirely natural. *In order to obtain a satisfactory theorem of factorization in K^*, we must conceive K^* as immersed in the larger field L.* The logic of the solution is exactly the same as that of the solution of the corresponding, but trivial, problem for the numbers $4m+1$.

On the other hand there is an obvious contrast between the two solutions. It is *natural* to think of the field "$4m+1$" as part of the field "m"; "m" is the more obvious and simpler field. It is not natural to think of K^* as part of L; K^* is a much simpler and more natural field than L, and we should like to do without the reference to the latter if we could. It will be very tiresome if, whenever we consider an algebraic field, we are to be compelled to construct some more elaborate field of which it is a part. We should prefer to tidy up the house without going out of doors.

We may look for a hint once more in the numbers $4m+1$. Some of these numbers are divisible by 7, a number outside the field; and these numbers stand in certain specific relations to one another inside the field. Could we give a rational account of these relations without explicit reference to the number 7? It is a very unnatural thing to try to do, since what is *important* about the numbers is precisely that they *are* divisible by 7, but we could do it; we could define the class

$$21, 49, 77, 105, \cdots,$$

of numbers $4m+1$ divisible by 7 in terms of the field $4m+1$ itself. For example, we could take the first two numbers 21 and 49, and say "the class in question is the class which begins with these two numbers and whose members recur at regular intervals in the field." It is of course an artificial definition, and it is impossible to conceal from ourselves what we are really doing.

It is often a very profitable exercise for a mathematician to force himself to solve some simple problem without the weapon obviously appropriate to the occasion, to throw away the key of the front door and insist on forcing himself in somehow through the window. The forced and unnatural solution of one problem will often turn out to contain the germ of a quite natural solution of another. So it proves in this case; it is natural to try to define the numbers of K^* divisible by ξ without going outside K^*; it is natural, and possible, and it gives us the key to what is, in the general case, the established method of constructing a satisfactory arithmetic.

It is obvious that, if α and β belong to K^*, and $\xi|\alpha$ and $\xi|\beta$, then $\xi|\lambda\alpha+\mu\beta$, where λ and μ are any numbers of K^*. The converse proposition is not true; it is not true that if I is any set of numbers of the field K^* which has the property "if α and β belong to I, then $\lambda\alpha+\mu\beta$ belongs to I, for every λ and μ of the field", then there exists a number ξ, belonging to K^* which divides every number of I. What *is* true is that every number of I is divisible by a ξ which belongs to L but not in general to K^*. The set I is identical with the set of numbers of K^* divisible by ξ. Such a set I, or the more general set based on any finite number of numbers $\alpha, \beta, \gamma, \cdots$, of K^*, is called an *ideal*, the numbers ξ, underlying K^* but not belonging to it, having been described by Kummer as "ideal numbers". In ordinary arithmetic ideals are simply the sets of numbers divisible by some special number such as 3, and there is nothing in particular to be gained by their introduction. In an algebraic field they are not, in general, the sets of numbers divisible by a number *of the field*, and their introduction is essential before arithmetic can get properly started. We can define multiplication and division of ideals, prime ideals, and so on, and when we have done this we find that the arithmetic of ideals has all the properties of ordinary multiplicative arithmetic. In particular, *every ideal can be resolved uniquely into prime ideals*; the fundamental theorem is true when stated in terms of ideals.

The proof of the fundamental theorem is not particularly difficult; Landau presents it, with all the preliminary definitions, in about a dozen pages of quite simple reasoning. But I would not commit the impertinence, even if I had the time, of assuming the airs of an expert in the algebraic theory of numbers, a subject which I admire only at a distance and in which I have never worked. It is ordinary rational arithmetic which attracts the ordinary man, and I have digressed outside it only because there is a good deal in it which it is impossible to appreciate properly without a little knowledge of the larger theory. It is impossible, for example, to appreciate Euclid's arithmetical achievements until we realize that there are arithmetics in which the most obvious analogs of his theorems are false.

15. *Conclusion. Pedagogy.* There are few things in the world for which I have less taste than I have for mathematical pedagogics, but I cannot resist the temptation of concluding with one pedagogic lesson. There was, and I fear still is, a popular English text book of algebra which I used at school and which contained a chapter on the theory of numbers. It might be expected that such a chapter would be among the most instructive in the book; we might suppose, for example, that Euclid's algorithm, with its elegance, its simplicity, and its far reaching consequences, would be an ideal text for the instruction of a bright young mathematician. In fact the algorithm was never mentioned; one was to find the highest common factor of 12091 and 14803, I suppose, by "trial"; and all that the authors had to say of the fundamental theorem was that "it is so evident that it may be regarded as a necessary law of thought." It is possible of course that all this may have been expunged from later editions. It is certain, however, that chapters on number theory in textbooks of algebra are usually quite intolerably bad, and it is conceivable that Oxford University may have been right in erasing the subject altogether from its more elementary examination schedule.

The elementary theory of numbers should be one of the very best subjects for early mathematical instruction. It demands very little previous knowledge; its subject matter is tangible and familiar; the processes of reasoning which it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity. A month's intelligent instruction in the theory of numbers ought to be twice as instructive, twice as useful, and at least ten times as entertaining as the same amount of "calculus for engineers". It is after all only a minority of us who are going to spend our lives in engineering workshops, and there is no particular reason why most of us should feel any overpowering interest in machines; nor is it in the least likely that, on those occasions when machines are of real importance to us, we shall require the power of dealing with them by methods more elaborate than the simplest rule of thumb. It is not engineering mathematics that is wanted for the understanding of modern physics, and still less is it wanted by most of us for the ordinary needs of life; we do not actually drive cars by solving differential equations. There may be a case for subordinating mathematics to the linguistic and literary studies which are so much more obviously useful to ordinary men, but there is none for sacrificing a splendid subject to meet a quite imaginary need.

PRINCETON UNIVERSITY