The Present State of Some Problems in the Theory of Numbers.[1]

By Prof. L. J. MORDELL, F.R.S.

THE theory of numbers, which was called the queen of mathematics by Gauss, the originator of the modern theory, still remains supreme. The present era is pre-eminently one in which she dominates the mathematical world. Her willing, loyal, and devoted subjects include the foremost mathematicians in every land. Their recent achievements bear comparison in difficulty and significance with those of any other period. Their propaganda in the last few years includes a surprisingly large number of thrilling treatises, which deal with most aspects of her conquests, and far exceed in number and importance those dealing with any other advanced mathematical subject. There is no lack of effort to present the most recent developments in as inviting and attractive a form as possible. One need only mention recent books in the last few years by Bachmann, Hecke, Landau, and Feuter. No small part of their subject-matter is closely related to or perhaps had its foundations in one or more of the six problems I have selected for discussion, which are associated with such distinguished names, namely :

1. Euler's Three Biquadrate Problem.
2. Fermat's Last Theorem.
3. The Cubic Indeterminate Equation.
4. Gauss' Class Number Problem.
5. Dirichlet's Divisor Problem.
6. Minkowski's Theorem on the Product of Linear Forms.

Some of these problems are comparatively new, such as (5) and (6), and testify to the wonderful freshness and vitality of the theory of numbers. The age of the others can be measured in centuries, particularly (3), special examples of which have been known for about two thousand years.

Their solutions are in every state of completion or rather incompletion, except perhaps for (3), which I solved a few years ago. Although some progress has been made with most of the others, except (1), they present difficulties which severely tax and seem beyond the powers of present-day mathematics. The slightest advances are made only by the most venturesome and heroic efforts, how much so can be easily appreciated by those who have even the slightest interest in the subject. These advances prove both useful and stimulating in many other fields, and it is difficult to exaggerate their importance and influence in the history of mathematics.

There are many striking features about these problems which have been noticed by all workers in this field. A simplicity of enunciation is combined with the fact that many of its most beautiful and startling results are proved originally in most unexpected and complicated ways. It is generally after many years that the simple and apparently natural method is discovered. It is only then that the proofs can be appreciated by greater numbers, just perhaps as the rough diamond only reveals its beauty after it has been polished and cut.

EULER'S THREE BIQUADRATE THEOREM.

This states that the sum of three biquadrates cannot be another biquadrate unless two of them are zero; *i.e.* if integers a, b, c, d satisfy the equation,

$$a^4+b^4+c^4=d^4,$$

then two of a, b, c must be zero.

It is truly remarkable that this simple theorem, the truth of which was conjectured by Euler more than 150 years ago, has neither been proved nor disproved. Further, it has been found absolutely impossible to make any headway with this problem. Indeed, it would be difficult to mention any other which has yielded so little to the efforts of those who have attempted its solution. Hence only some half-dozen references are to be found in the mathematical literature to papers dealing with it. The most important result known is a numerical verification by Aubry, in 1912, that the theorem is true for $|d| \leqq 1040$.

The theorem cannot be extended to four fourth powers, as Norrie in 1911 showed that

$$30^4+120^4+272^4+315^4=353^4.$$

The particular case when one of a, b, c is zero, so that the equation is

$$a^4+b^4=c^4,$$

dates back from Fermat. It is proved by his method of infinite descent, *i.e.* if this equation or the less restricted one

$$a^4+b^4=c^2,$$

admits of integer solutions where abc is not equal to zero, then it must have other integer solutions a_1, b_1, c_1 where $a_1b_1c_1$ is not equal to zero, and where c_1 is numerically less than c. By continuing this process we are led to the existence of a solution wherein c is not zero and is numerically less than some definite number (here 1), and it can be easily verified by trial whether this is so. This example is a particular case of the second problem.

FERMAT'S LAST THEOREM.

This states that if integers x, y, z satisfy the equation

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

where n is a given integer greater than 2, then x or y equals zero.

This theorem was discovered about 1637 by Fermat, who wrote upon the margin of his copy of the works of Diophantos, " I have discovered a truly remarkable proof which this margin is too small to contain." The theorem has attained world-wide celebrity because of the Wolfskell prize of 100,000 marks established in 1907 for the first demonstration of its proof. The prize has not yet been won.

The most important results are due to Kummer

[1] A lecture given to the Manchester Literary and Philosophical Society on Nov. 15, 1927.

who spent a great part of his life upon it. Assuming that n is an odd prime p, which involves no loss of generality, he proved the truth of the theorem for values of n included in certain general classes, *e.g.* when n is not a divisor of the numerator of one of the first $\frac{n-1}{2}$ Bernouillian numbers, B_r being defined as the coefficient of $(-1)^{r-1}x^{2r}/2r!$ in the expansion in ascending power of x of $x/e^x - 1$, and in particular for $3 \leq n \leq 100$, though his proof was not complete for a few values of n. It is not known whether the values of n for which Kummer proved his results are infinite in number. Though his papers were written about the middle of the last century, no further important results were obtained until 1909. Kummer and his successors in the discussion of the problem divided it into two cases, according as xyz is not or is divisible by p. The first case is the easiest, and for the theorem to hold for this one, Wieferich showed in 1909 that $2^{p-1} \equiv 1 \pmod{p^2}$, that is, $2^{p-1} - 1$ is exactly divisible by p^2.

The first value of p for which this is true was shown by Meissner in 1913 to be 1093. But Wieferich's theorem is a particular case of the more general one that if r is any prime less than p, then $r^{p-1} \equiv 1 \pmod{p^2}$ if the equation $x^p + y^p = z^p$ holds with xyz prime to p. This was proved for $r=3$ by Mirimanoff, for $r=5$ by Vandiver, and by Frobenius for $r=11$, 17, and when $p \equiv 1 \pmod 6$, for $r=7$, 13, 19. The proofs except when $r=2$ or 3 are very complicated and suggest that the real source of these results is still to be found.

Fermat's last theorem is the most important of all the problems that I shall mention, as the efforts made in attempting its solution led Kummer to discoveries that marked the beginning of the theory of algebraic numbers. This discovery later revealed wonderful and beautiful relations between the theory of numbers, elliptic functions, automorphic functions, and many other parts of the theory of functions of a complex variable.

In no other part of the theory of numbers as in Fermat's last theorem are the investigator and reader called upon to deal with such abstract conceptions, such involved results, many of which are arrived at by a long chain of reasoning; and such general theories, *e.g.* laws of reciprocity, which have their foundations deep in the arithmetical theory. No other problem has been attempted by so many distinguished mathematicians, and very few can have led to such remarkable developments.

CUBIC INDETERMINATE EQUATIONS.

This problem is to find the rational values of x, y, satisfying the general equation of the third degree in x, y with rational coefficients, namely,

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + ky + i = 0,$$

i.e. to find the rational points on this cubic curve which it is supposed has no double point, as then the problem is comparatively simple.

It is the oldest of those with which I am dealing, and particular cases of this question have been considered so long as two thousand years ago. Its solution proved intractable until six years ago, when I discovered the general solution, which is now so obvious that it is given in lectures at some universities.

A great deal of what was done on this question for many years can be explained in a few sentences. Any straight line meets the curve in three points. If two of these points are rational, the third is found from a simple equation, so that its co-ordinates will certainly be rational. In particular the tangent to the cubic at a rational point will meet it in another rational point.

Now suppose we have already found, perhaps by trial, n rational points on the curve say P_1, P_2 . . . P_n, *e.g.* if $x^3+y^3=9$, $x=2$, $y=1$ is an obvious point. The tangent to the curve at P_1 will meet it again in another rational point P'_1, distinct from P_1 unless P_1 is a point of inflexion. So the tangent at P'_1 meets the curve in general in another point P''_1, etc., and we may expect to find an infinite number of rational points starting from P_1, though it is conceivable that we may find only a finite number of points forming a closed polygon. Similarly, we may expect to find an infinite number starting from P_2 if P_2 is not included in the group arising from P_1, and so for P_3, etc. But we can find another rational point, $Q_{1,2}$ from the intersection of the line $P_1 P_2$ . . . and the curve. We may now either draw a tangent to the curve at $Q_{1,2}$, or draw the secants joining $Q_{1,2}$ and the points P_2, P_3, etc., and find their intersections with the curve.

Clearly, in this way, we can find in general an infinite number of other rational points by starting from n known rational points, say primary points for short. From the time of Fermat onwards, mathematicians had to content themselves with doing little more than deriving for special equations explicit formulæ for the co-ordinates of the points found from one or more given ones, *e.g.*: for

$$ax^3 + by^3 = c, \; y^2 = px^3 + q.$$

Even prizes established by learned societies led to no solution.

Finally, I showed that all the rational solutions of the general equation could be found from a finite number of primary ones by drawing tangents and secants as above. In other words, the method of infinite descent gives all the solutions; and there is now no theoretical difficulty in finding them.

GAUSS' CLASS NUMBER PROBLEM.

Let $-D$ be a given negative number and let $ax^2 + bxy + cy^2$ be any quadratic form of determinant $-D$, *i.e.*, a, b, c are any integers for which $b^2 - 4ac = -D$. This requires that $D \equiv 0, 1 \pmod 4$, and then an infinity of integers a, b, c, can be found, and so an infinite number of quadratic forms of given determinant $-D$. It is a classic and elementary theorem that all these quadratic forms can be derived from a finite number, $H(D)$ say, by means of a linear transformation with integer coefficients and determinant unity. It was conjectured by Gauss more than 125 years ago that there are only a finite number of values of D for a given $H(D)$. This has not yet been proved, though a formula and many recurring formulæ are known for $H\ (D)$. Hecke, making use of an unproved hypothesis about the zeros of a function analogous to the Riemann Zeta function, has given a simple proof. But I wish to deal more particularly with what would appear to be the very simple case when $H\ (D)=1$. This is so for $D=3, 4, 7, 8, 11, 12, 16, 19, 27, 28, 43, 67, 163$. It is easily verified that for any others, D must be a prime of the form $8n+3$. It was shown in 1911 by Dickson that there is no other value of D less than 1,500,000.

It may seem surprising that the truth of the conjecture about $H\ (D)=1$, is equivalent to the fact that the formula $z^2+z+2n+1$ gives only prime numbers for the integers z satisfying $0 \leq z \leq 2n-1$ as was proved by Rabinovitch (Rainich), and this is easily verified for $D=43, 67, 163$, when $n=5, 8, 20$.

It is also equivalent to the statement that the only solutions in non-negative integers of

$$yz+zx+xy=D=8n+3$$

are given by

$$(x, y, z)=(0, 1, 8n+3),\ (1, 3, 2n),\ (1, 1, 4n+1),$$

and those derived from these by permuting x, y, z.

Neither of these simple facts has, however, proved of use in proving the theorem.

DIRICHLET'S DIVISOR PROBLEM.

The number of divisors $d\ (n)$ of a given integer n is a function of n which changes very irregularly with n, and is really the number of positive integer solutions of $xy=n$. If n is a prime number $d\ (n)=2$, while if $n=p^a q^b r^c\ .\ .\ .$ where $p, q, r\ .\ .\ .$ are different primes

$$d(n)=(a+1)(b+1)(c+1)\ .\ .\ .\ .$$

But though $d(n)$ does not depend so much upon the magnitude of n as upon its form, it is different with

$$d(1)+d(2)+\ .\ .\ .\ d(n).$$

This really represents the number of positive integer solutions of $xy \leq n$, *i.e.* the number of points with positive integral co-ordinates lying in the area bounded by the rectangular hyperbola $xy=n$ and the lines $x=1$, $y=1$, including the boundary in the area. The irregularities are smoothed out as it were, in the sum. Dirichlet showed in 1849 that $d(1)+d(2)+\ .\ .\ .\ d(n)=n\ \log\ n+(2\gamma-1)n+R(n)$ where $\gamma=0{\cdot}577\ .\ .\ .$ is Euler's constant, and $R(n)$ the remainder or error term is less numerically than a constant multiple of $\sqrt{n}$. This is expressed by $R(n)=O(\sqrt{n})$. For many years this was thought to be the best approximation to $R(n)$. Voronoi proved, however, in 1903, that $R(n)=O\ (\sqrt[3]{n}\log n)$. Van der Corput showed next that $R(n)=O(n^{\alpha})$ with $\alpha=\frac{1}{3}$. This result was arrived at in many different ways, arithmetical, geometrical, by the real variable, and by the complex variable. These all led to $\alpha=\frac{1}{3}$ and seemed to suggest that $O\ (\sqrt[3]{n})$ was the best approximation to the error term; though it was known from Hardy's work of 1915 that in the error term, the index $\alpha \geq \frac{1}{4}$. Wonderful to relate, Van der Corput showed in 1922 by an exceedingly difficult and complicated method that $\alpha<33/100$. Simpler proofs have since been given by Littlewood, Walfisz, and Landau for the slightly less precise result $\alpha \leq 37/112$.

This extraordinary result appears not to be final; but to have arrived at it is one of the most startling achievements of the present day. The problem is one which has made the greatest demands upon many branches of mathematics. The most delicate questions of convergence, of the theory of functions, and the most adept manipulation of inequalities are all required.

In this problem, as opposed to the others, it is the methods of the analytical theory of numbers which have proved most successful. The most important stage in the proof depends upon Weyl's method of finding upper limits for large values of n to sums such as

$$\cos(f(1))+\cos(f(2))+\ .\ .\ .\ \cos(f(n)).$$

These approximations have also played a vital part in Waring's problem and in the recent theory of the Riemann Zeta function.

MINKOWSKI'S THEOREM ON THE PRODUCT OF LINEAR FORMS.

This is the most recent of these problems, but it has features that mark it out as a worthy companion to those that have preceded it.

Let

$$\begin{aligned} L_1&=a_{11}x_1+a_{12}x_2+\ .\ .\ .\ a_{1n}x_n-c_1,\\ L_2&=a_{21}x_1+a_{22}x_2+\ .\ .\ .\ a_{2n}x_n-c_2,\\ &.\ .\ .\ .\ .\ .\\ L_n&=a_{n1}x_1+a_{n2}x_2+\ .\ .\ .\ a_{nn}x_n-c_n, \end{aligned}$$

be n linear non-homogeneous forms where the a's and c's are any real constants subject to the restriction that the determinant $|a_{rs}|=1$, which it may be noted in no wise detracts from the generality of the following theorem. Then it is supposed that there are integer values for $x_1, x_2, \ldots x_n$, for which the product $|L_1L_2\ .\ .\ .\ L_n| \leq 2^{-n}$.

The proof for $n=2$ was first given by Minkowski. Remak has given another, and I am now publishing one which proves it in a very simple way. But a different state of affairs arises for $n=3$. Remak gave in 1921 an extraordinarily complicated and intricate proof in fifty pages. It depends upon the arithmetic theory of the definite ternary quadratic, and involves ideas closely allied to those occurring in the problem of the closest packing of spheres. Unfortunately, it appears to be exceedingly difficult to extend the proof to the case $n=4$, and it is not known whether the theorem is true for $n \geq 4$, although it seems very likely. It is very rarely that the proof of the generalisation of a question to n dimensions proves so unattainable, especially when in similar questions, for example, in dealing with linear forms in which $c_1=c_2=.\ .\ .\ c_n=0$, the results for n variables are proved as easily as for two.

It is fairly certain that in due course a very simple general proof will be found, making the truth of the theorem almost intuitive. Such a one could be found by generalising to n variables the simple theorem that if $|\,a\,| \leq 1$, $|\,b\,| \leq 1$, there is a range of values of width at least two for x for which

$$|ax^2+bx| \leq 1.$$