CARMICHAEL'S MONOGRAPHS ON BRANCHES OF THE THEORY OF NUMBERS.

The Theory of Numbers. By R. D. CARMICHAEL. New York, John Wiley and Sons, 1914. 8vo. 94 pages. Price $1.

Diophantine Analysis. By R. D. CARMICHAEL. New York, John Wiley and Sons, 1915. 8vo. 6+118 pages. Price $1.25.

THE various series of tracts or monographs on mathematics which are in course of publication in several European countries are so well known and the arguments in favor of them are so generally conceded that it is not surprising that several series of tracts have been recently begun in America. In view of the purpose of such a tract, the editor of a series naturally imposes a definite upper limit to its length. Frequently the tract relates to a very extensive field of mathematics and the problem of the selection of topics presents a serious difficulty to the author.

There is an added difficulty in the case of a tract for beginners in the theory of numbers (and the same point would apply to the case of the theory of groups): the subject is somewhat abstract and the nature of the theorems and proofs is quite different from that to which the reader is accustomed. Consequently the author of the tract on the Theory of Numbers has wisely adopted a very elementary and expansive style of presentation, even at the expense of a reduction of the number of topics treated. A like motive, combined with the desire to emphasize methods rather than results, doubtless led the author to give several proofs of Fermat's theorem and Euler's generalization, although the space used could have been utilized for the presentation of further results.

Chapter I deals (in 23 pages) with the uniqueness of factorization into primes, the greatest common divisor and least common multiple of two or more integers, the highest power of a prime which divides $n!$, and the simplest properties of prime numbers.

Chapter II devotes 7 pages to Euler's ϕ-function or indicator. Two methods of evaluating $\phi(m)$ are given in detail, and a third method is suggested.

Chapter III gives in 10 pages the formal properties of congruences, a proof that a congruence of degree n with respect

to a prime modulus has at most n (real) roots, and the simpler theorems on linear congruences.

Chapter IV treats (in 14 pages) of Fermat's theorem and its extensions and converse, its application to linear congruences and to Euler's criterion for quadratic residues; also Wilson's theorem and its converse.

Chapter V devotes 15 pages to a rather full account of the theory of primitive roots. Concerning the important function $\lambda(m)$, the maximum indicator of Cauchy, it is proved that there exist integers belonging to the exponent $\lambda(m)$ modulo m. Thus $x^{\lambda(m)} \equiv 1 \pmod{m}$ is satisfied by every integer x prime to m, while this is not true for an exponent less than $\lambda(m)$.

Chapter VI gives (in 17 pages) a brief first view of various additional topics such as the theory of quadratic residues, including a statement of the law of reciprocity; Galois imaginaries, from the intuitive point of view of Galois; rational right triangles.

In view of its great clearness and elementary character, this book will prove a boon to the general reader desirous of an introduction to the "queen of the sciences," as well as to those students of mathematics who wish to acquire quickly and easily a working knowledge of the theory of numbers sufficient for its ordinary applications in other fields of mathematics. For the latter purpose, the text should have contained numerous exercises involving quadratic residues. On the other topics treated, the exercises are numerous and well selected. Having examined the full reports from a beginner in this subject who used this text for private reading, the reviewer is confident that the text is well suited for the two classes of readers mentioned above. In view of the limited range of topics, the book would have to be supplemented by lectures if adopted for a major course in the theory of numbers, as usually presented at the universities.

The author has deviated from custom in his definition of three or more relatively prime numbers. This term is used (page 9) when the numbers have no common factor except unity. According to Dirichlet,* numbers are relatively prime only when every pair of them are relatively prime. While Carmichael is consistent in the use of his definition, a student who was reading the text occasionally made errors by falling back upon the older (and perhaps more natural) definition.

In exercise 7, page 17, the word two should be inserted before

* Vorlesungen über Zahlentheorie, ed. 4, 1894, p. 11.

" relatively prime factors." There is an evident misprint in exercise 3, page 20.

The text on Diophantine analysis is of much greater scientific importance than the book just reviewed, since there exists no other single book in any language which presents so much of the material on Diophantine equations, and certainly no earlier book which undertakes such a systematic presentation of important aspects of the theory. From the time of Pythagoras there has been an uninterrupted interest in the subject now known as Diophantine equations. In particular, there has been for three centuries a special interest in Fermat's last theorem, that perpetual challenge to mathematical combat, that impenetrable armor upon which has been shattered the lance of many a gallant trained soldier, that lure which has fascinated only to repel the uncouth advances of many a camp follower and raw recruit. If only to satisfy a reasonable curiosity, the general mathematical public is entitled to a clear exposition of the problems, methods and results achieved in an ancient subject in which the theorems appear to be so simple and yet are often so difficult to prove.

Chapter I deals with the general nature of Diophantine analysis, the lack of general methods of investigation, rational oblique and right triangles, and Fermat's method of infinite descent.

Chapter II is an introduction to the application in this subject of a principle, discussed later in this review, which is really only the theorem that, in a given algebraic domain, the norm of a product equals the product of the norms of the factors. The applications here are to Pell's equation $x^2 - Dy^2 = \sigma^2$ (especially the case $\sigma = 1$), to $x^2 + ay^2 + bu^2 + abv^2 = t^2$, to the complete solution of $x^2 + y^2 + z^2 = t^2$ in integers, to the derivation of a second solution of $x^4 + by^4 + bz^4 = t^2$ from a given solution, and to a like result for $x^4 + ay^4 = \mu^2 + bv^2$.

Chapters III and IV are devoted to Diophantine equations of the third and fourth degrees in two or more variables.

Chapter V devotes 19 pages to Fermat's last theorem: If n is an integer greater than 2, there are no integers x, y, z all different from zero, such that $x^n + y^n = z^n$. The formulas given by Abel and Legendre are proved. There is a presentation of the method of Sophie Germain as developed by

Legendre and recent writers. Four pages are used to give a summary of further results known about Fermat's last theorem, many of the results being stated in the form of exercises.

Chapter VI directs attention to the possibility of using rational solutions of functional equations as a means of classifying isolated problems on Diophantine equations. The illustration employed is the functional equation

$$(a^2 + 1)(u_a^2 + 1) = v_a^2 + 1.$$

Various solutions of this are employed in a treatment of Fermat's problem to find three squares such that the product of any two of which, added to the sum of those two, gives a square.

The chief aim of the author is set forth in the preface as follows. "The task of the author has been to systematize, as far as possible, a large number of isolated investigations and to organize the fragmentary results into a connected body of doctrine. The principal single organizing idea here used and not previously developed systematically in the literature is that connected with the notion of a multiplicative domain introduced in Chapter II" (that of applying the multiplicative property of norms of algebraic numbers). Again on page 50, the author says "The method of extending this set (of numbers $x_1^n + a_1x_1^{n-1}x_2 + \cdots + a_nx_2^n$) so that the resulting set shall form a domain closed with respect to multiplication grows out of a remark due to Lagrange (Oeuvres, 7, pages 164–179), though Lagrange seems nowhere to have utilized it in connection with Diophantine problems. A partial use of it has been made by Legendre (Théorie des Nombres, volume 2, ed. 3, pages 134–141); but its consequences seem nowhere to have been systematically developed."

This programme has been carried out so admirably that it does not detract from the value of the work to point out that Lagrange did apply the idea to Diophantine equations and that later writers developed the theory quite systematically.

Lagrange* proved that, if a is a fixed nth root of unity, the product of two functions of the type

$$p = t + ua\sqrt[n]{A} + xa^2\sqrt[n]{A^2} + \cdots + za^{n-1}\sqrt[n]{A^{n-1}}$$

is of like form. Hence if we replace a by the different nth

* *Mém. Ac. R. Sc. Berlin*, vol. 23, 1769; Oeuvres 2, 527.

roots of unity and form the product of the functions so obtained from p, we obtain a rational function P of $t, u, \cdots, z, A$, such that the product of two functions of type P is a third function of type P. It is shown how P can be found by elimination. The theory is applied to the solution of

$$r^n - As^n = q^m. \tag{1}$$

We desire to express each factor $r - asA^{1/n}$ as an mth power p^m, where $a^m = 1$, and p is the above linear function. Then

$$p^m = T + Ua\sqrt[n]{A} + Xa^2\sqrt[n]{A^2} + \cdots + Za^{n-1}\sqrt[n]{A^{n-1}}.$$

Hence we take $r = T$, $s = -U$, $X = 0, \cdots, Z = 0$. Thus (1) is solvable by this method if $X = 0, \cdots, Z = 0$ are solvable. Although we have only $n - 2$ equations in n variables, they do not always have rational solutions. For the case $n = 3$, $m = 2$, the single condition $X = 0$ gives $x = -u^2/2t$; then

$$r = T = t^2 + 2Aux = t^2 - \frac{Au^3}{t},$$

$$-s = U = Ax^2 + 2tu = \frac{Au^4}{4t^2} + 2tu,$$

$$q = P = t^3 + Au^3 - 3Atux + A^2x^3.$$

For $n = m = 3$, the condition is $tu^2 + t^2v = Auv^2$; but Lagrange did not complete the discussion of this case.

The method just applied to the two cases having $n = 3$ was later extended by Lagrange* from the special case $a^3 = 1$ to the case in which a is a root of any cubic equation. This work is reproduced by Carmichael on pages 55, 56, where a reference to Lagrange would have been in place. For, although this reference was given five pages earlier, it was there stated (see quotation above) that Lagrange had not applied the idea to Diophantine problems. Carmichael reproduced Lagrange's use of the idea to obtain a set of solutions, involving two parameters, of

$$x^3 + ax^2y + bxy^2 + cy^3 = v^2. \tag{2}$$

Lagrange remarked that his solution of (2) "is well worthy of notice on account of its generality and the manner in which

* Addition IX to Euler's Algebra, vol. 2, 1774, pp. 644–9; Oeuvres de Lagrange, vol. 7, pp. 170–9.

it was derived, which is perhaps the only way which can lead to it easily."

Carmichael attempts to apply the idea to the similar equation in which v^2 is replaced by v^3, but finds (page 58) that the condition $X = 0$ is so complicated that a complete solution is hardly to be expected; he then gives the recent methods by Schaewen, based on other principles.

Lagrange* made much use of the property

$$(p^2 - Bq^2)(p_1^2 - Bq_1^2) = (pp_1 \pm Bqq_1)^2 - B(pq_1 \pm qp_1)^2$$

in his various investigations on Diophantine equations of the second degree, especially in his work on Pell's equation and in the solution of $u^2 - Bt^2 = A$ in rational numbers. The corresponding formula (page 525) concerning

$$F = p^2 - Bq^2 - Cr^2 + BCs^2$$

was used by him in the proof that every number is expressible as a sum of four squares. G. Libri† used this property of F and gave a formula stated to give all the ways of reducing a product FF_1 of two such functions to a like form F_2; he gave (page 292) an identity expressing the product of two sums of four cubes as a sum of cubes of four rational expressions, and remarked that also

$$3x^4 + y^4 - z^4 - 3u^4$$

repeats under multiplication and represents rationally all rational numbers.

Lagrange‡ stated that "the simplest and most general method for equations like $x^4 + ay^4 = z^2$ is perhaps that by factors in his additions (final chapter) to Euler's algebra."

It is therefore clear that Lagrange was fully aware of the applications of the multiplicative property of norms to Diophantine problems. Moreover, it is rather evident that he developed this property of norms for the purpose of applying it to Diophantine equations.

As to Carmichael's remark that the consequences of this idea of Lagrange's "seem nowhere to have been systematically developed," it should be noted that the series of papers by

* Oeuvres, 2, p. 386, p. 523.
† *Journal für Math.*, vol. 9, 1832, p. 287.
‡ Oeuvres, 4, p. 395.

Desboves* give such a systematic development, perhaps as extensive as Carmichael's. Among the equations treated by this method by Desboves are

$$X^3 + rY^3 = Z^2, Z^3, Z^4; \quad \xi^4 + k\eta^4 = \zeta^2.$$

In this connection should be cited a general theorem of importance due to Dirichlet:† If at least one of the roots $\alpha, \beta, \cdots, \omega$ of an equation $s^n + as^{n-1} + \cdots + h = 0$ is real and if $a, \cdots, h$ are integers, while $s^n + \cdots$ has no rational divisor, and if

$$\phi(\alpha) = x + \alpha y + \cdots + \alpha^{n-1}z,$$

then the Diophantine equation

$$F(x, y, \cdots, z) \equiv \phi(\alpha)\phi(\beta) \cdots \phi(\omega) = 1$$

has an infinity of integral solutions. If the corresponding Lagrangian function P can assume a given value N, it takes the same value N for an infinitude of sets of values of $x, y, \cdots, z$. Poincaré‡ noted that, under the same conditions, the solution of $F = N$ reduces to the problem of forming all complex ideals of norm N, and discussed the latter question.

Carmichael (pages 44–48) has applied Lagrange's method to two new types of Diophantine equations

$$x^4 + ay^4 + bz^4 = t^2, \quad x^4 + ay^4 = \mu^2 + b\nu^2,$$

obtaining a second set of solutions from a given set. When applied to another equation (page 62), the method led to a solution which "unfortunately lacks generality," so that a special method was devised. The author himself of course recognizes that Lagrange's method is not a universal panacea.

If the strict limitations of space had not made it necessary for the author to develop a considerable body of classic results from a single central point of view, he would doubtless have given an exposition of other methods of considerable generality. For example, the elegant method in the joint paper§ by Hilbert and Hurwitz to obtain all sets of rational solutions of

* *Nouv. Ann. Math.*, ser. 2, vol. 18, 1879, pp. 265–279, 398–410, 433–444, 481–499.

† *Comptes Rendus*, Paris, vol. 10, 1840, pp. 285–8.

‡ Ibid., vol. 92, 1881, p. 777.

§ *Acta Mathematica*, vol. 14, 1890–1, pp. 217–224.

$f(x, y, z) = 0$, where f is a homogeneous polynomial of degree n with integral coefficients such that the curve $f = 0$ is of genus (or deficiency or Geschlecht) zero. Again, Poincaré,* with the aim to find a bond between various problems of Diophantine analysis, has treated homogeneous polynomials $f(x, y, z)$ with integral coefficients from the standpoint of classes of curves $f = 0$ under birational transformations with rational coefficients. Finally, C. Runge† and E. Maillet‡ have given conditions for an infinitude of sets of solutions of any Diophantine equation in two variables. References to papers of this type would have been in place in such a brief text.

The reference (page 68) to Euler alone is rather generous, as Euler, in his proof of the impossibility of integral solutions, all different from zero, of $x^3 + y^3 = z^3$, did not give a rigorous proof of the vital point that, if $p^2 + 3q^2$ is a cube, it is the cube of a number $t^2 + 3u^2$ and that $p + q\sqrt{-3}$ is the cube of $t + u\sqrt{-3}$. For a proof, see Pepin.§

The numerous exercises are of three types with distinguishing marks. There are 133 exercises intended to develop facility in the handling of the subject; 53 additional exercises are of more difficulty and are intended primarily as a summary of known results not otherwise included in the text; while 35 further exercises are intended to suggest investigations. With many of the exercises are affixed names of writers and dates, but no journal references. The author evidently made a thorough examination of the extensive literature of the subject.

In view of its undoubted scientific merits, the book should be very useful to the student of Diophantine analysis. In view of its clear and attractive style of presentation, its emphasis on important results and methods, and its proper subordination of minor or more technical matters, the text should appeal strongly to the general reader desirous of obtaining in a brief time a clear view of this attractive branch of the theory of numbers.

L. E. DICKSON.

---

* *Jour. de Math.*, ser. 5, vol. 7 (1901), 161–233.
† *Jour. für Math.*, vol. 100 (1887), pp. 425–435.
‡ *Jour. de Math.*, ser. 5, vol. 6 (1900), pp. 261–277.
§ *Jour. de Math.*, ser. 3, vol. 1 (1875), p. 317.