rand's own contributions, and a single reading will show that it is written by one who has not merely made a compilation of the works of others, but who possesses in addition that intimate acquaintance with the subject which is only obtained by those who have advanced it at least in some directions. Whatever the defects of the book may be, it will take a high rank amongst the many classic treatises on celestial mechanics. If we might venture to make a suggestion, it would be that a full alphabetical index of subjects and names be appended to the fourth volume, thus adding greatly to the value of the series as books of reference. The increasing labor of finding out what has been done in a subject makes such an index almost necessary.

ERNEST W. BROWN.

HAVERFORD COLLEGE, PA.

BACHMANN'S THEORY OF NUMBERS.

Die Elemente der Zahlentheorie. Von PAUL BACHMANN. Leipzig, Teubner, 1892. 8vo, xii + 264 pp.

"The most beautiful theorems of higher arithmetic have this peculiarity, that they are easily discovered by induction, while on the other hand their demonstrations lie in exceeding obscurity, and can be ferreted out only by very searching investigations. It is precisely this which gives to higher arithmetic that magic charm which has made it the favorite science of the first mathematicians, not to mention its inexhaustible richness, wherein it so far excels all other parts of pure mathematics."—GAUSS.

Interest in the theory of numbers has, perhaps naturally enough, not always remained at the high-water mark indicated in the above encomium, though there is not wanting a list of illustrious names, reaching down to the present generation, of those who have made important contributions to the theory. Within the last decade there have appeared translations of classic works of the highest importance, one at least grown well-nigh inaccessible in the original, as well as quite a number of text-books on the subject. During the last three years there have appeared text-books, each with its own points of merit, in the languages English, French, and German.* All these recent publications point to a strong interest in the theory of numbers now existent, and at the same time give promise that the increased facilities for study will give a fresh impetus to research in this field.

---

* Respectively by Mathews, Lucas, and Bachmann.

We consider in this review one of these recent text-books on the theory of numbers. This work is the beginning of a homogeneous presentation of the subject in its present status, the object being rather to make a synopsis or an outline of this branch of mathematics than a compendium containing all that has ever been written on it. The volume before us treats of the *elements* of the subject—congruences, quadratic residues, and forms, the last being restricted to *binary* forms. Consequently the division of classes into *genera* has been excluded, because the fundamental theorem proving the actual existence of the possible genera is based upon the consideration of ternary forms. Of course, all non-arithmetical proofs are also strictly excluded.

Regarding the work as a whole, the following points deserve especial remark:

I. *Clearness of Presentation.*—This is characteristic not only of the discussions, but also and especially of the formulations of the problems and the analyses of methods. This, together with the well-balanced mean preserved between excessive conciseness and too great diffuseness, makes the book unusually readable. It must be said, however, that the simpler presentation is not always preferred, but rather that which fits more consistently into the general plan of treatment. Instances of this will be noticed in the detailed sketch to follow.

II. *Introduction of Recent Results.*—Since the time of Gauss not much has been accomplished, relatively speaking, by elementary methods in the elementary field as outlined above, but still the author finds sufficient opportunity for presenting recent results to warrant the statement that he has given us, as proposed, not simply a sketch of the subject as Gauss left it, but of the elementary theory of numbers in its principal outlines as it stands to-day. Particular mention may be made of the application of the theory of groups, and the generalization of the Gaussian lemma by Schering and Kronecker. Throughout the book well-chosen references direct the reader to original sources.

III. *Historical Remarks.*—Concise sketches of the salient features of the historical development of the subjects considered are made as occasion arises and add materially to the interest and also to the clearness of the treatment. The author is usually scrupulous in crediting even simple and commonly current results to their original publisher (e.g., pp. 19, 25, 26). On this account only, it is worth mentioning that the proposition (p. 30) concerning the highest power of a prime contained in $m!$ was given by Legendre.*

We proceed now to a more detailed consideration of the

* Théorie des Nombres, Introd. xvi.

contents of the book, dwelling only upon points whose treatment differs from that usually found in other books.

In an introductory section the concept "number" is briefly taken up (pp. 1–4). It has been customary with writers of treatises on the theory of numbers tacitly to assume the system of positive integral numbers. It is questionable whether so abstract an idea as "number" can be adequately treated in four pages, and whether our author has really done more than to occupy himself throughout four pages in plausibly assuming the system of positive integral numbers. The operations, addition and multiplication, with their laws are also discussed in the introduction.

SECTION I. *The Divisibility of Numbers.* — The author begins by considering the least positive remainders which the entire system of positive and negative integers leave when divided by a given integer n, the latter being at once called the *modulus*. This brings into prominence the periodicity of the series of integers taken modulo n, and various elementary properties of numbers with regard to divisibility are deduced by considering the least positive residues (mod n) written at the corners of a regular n-gon inscribed in a circle, a well-known method which the author credits to Poinsot.* The resolution of numbers into prime factors is shown to be unique, the number of divisors of a given integer and their sum are found, and properties of the greatest common divisor and of the least common multiple of given numbers are discussed. The highest power of p, a prime, contained in $m!$ is next found, and the result is applied in a purely arithmetical proof that the following expressions are integers:

$$\frac{m!}{r!\,s!\ldots t!}, \qquad (m = r + s + \ldots + t,)$$

† $$\frac{2a!\,2b!}{a!\,b!(a+b)!}.$$

The section closes with the evaluation of the expression $\phi(n)$ by a method different from that ordinarily used.

SECTION II. *Congruences.* — In establishing the *preliminary* theorems concerning congruences stress is laid upon the fact that we have really to do, not with the numbers themselves, but simply with the classes to which they belong (mod m). The fact that the classes which are characterized by residues prime to the modulus have a definite law of multi-

* *Liouville's Journal*, vol. 10.
† Catalan, *Nouv. Ann.* 1874.

plication which is associative and "invertible,"* together with the fact that their number finite assumes that they form a finite *group*. The notion of a group is accordingly introduced, and some of the elementary properties of groups are set forth. The results are applied in achieving the solution of linear congruences. Of Fermat's theorem and its generalization three different proofs are given and analyzed. Kronecker's theorem† concerning the generation of groups whose elements are commutative with each other follows with somewhat more detail than in its original presentation. This amplification of this important theorem is welcome, though no amplification can remove the inherent abstractness of the subject. It would perhaps have been of advantage to bring forward explicitly the idea of a quotient-group recently introduced by Hölder,‡ which is fundamental for the whole proof. The theorem is at once applied in the proof of the existence of primitive roots for a prime modulus, and later in the consideration of the same question for a modulus which is a power of a prime. The existence of primitive roots for any modulus is discussed, and the properties and applications of indices are briefly presented.

SECTION III. *Quadratic Residues.*—Quadratic residues are defined, Euler's criterion for the possibility of the congruence $x^2 \equiv n \pmod{p}$ is set up, Legendre's symbol is introduced, the congruence $x^2 \equiv n \pmod{m}$ is considered for composite moduli of various forms, and then the problem is attacked: "To determine of what moduli a given number n is residue (or non-residue)" Restricting consideration first to prime moduli, we ask successively, "Of what odd primes is the numbers, $-1, 2,$ any other prime q, residue (or non-residue)?" For the first two cases the question is satisfactorily and readily answered, while the third leads to Legendre's *law of reciprocity* of quadratic residues. The consideration of this important theorem is begun by proving the "Gaussian lemma," that $\left(\frac{n}{p}\right) = (-1)^{\mu}$, where μ is the number of negative numbers in the series of absolutely least residues (mod p) of

$$n,\ 2n,\ 3n,\ \ldots\ \frac{p-1}{2}\,.\,n.$$

* I have ventured so to express "einpaarig," the latter a term introduced by our author. It is meant that from $ab = ac$, as well as from $ba = ca$, we infer that $b = c$. This means that the *inverse* of multiplication (which we may call division) is an unambiguous process for "divisors" prime to the modulus, those not prime to the modulus corresponding more or less closely to zero in ordinary numerical division.

† *Berl. Monatsber.* 1870.

‡ *Math. Annalen*, vol. 34.

Before proceeding to a proof of the law of reciprocity, the author classifies the proofs which have been given into four categories:

First Category.—The first proof of Gauss, simplified by Dirichlet, constitutes a category by itself. Of all the proofs ever given, it attacks the problem most directly, and by induction achieves the result through simple conclusions from the idea of a quadratic residue.

Second Category.—The proofs of this category are based upon the theory of quadratic forms. To this category belong the second proof of Gauss, those of Kummer, and that of Legendre (incomplete).

Third Category.—Proofs directly connected with the division of the circle. They are exemplified by the fourth and the sixth proof of Gauss.

Fourth Category.—Proofs based on the Gaussian lemma. Examples, the third and the fifth proof of Gauss.

As the first category is treated in full in Dedekind-Dirichlet's text-book, and as the second and the third category are not elementary, they are (with one exception in the second category to be noticed later) excluded from detailed consideration.

Of the fourth category, the proof of the pastor Zeller is given.* This proof, though simple and elegant, has not before, as far as the reviewer knows, been presented in a text-book on the theory of numbers.† There follow Jacobi's generalization of Legendre's symbol and the generalized law of reciprocity, Eisenstein's algorithm for the determination by means of the law of reciprocity of the value of $\left(\frac{m}{n}\right)$, m and n being any two relatively prime integers of which at least one is positive, while with Schering's and Kronecker's generalization of the Gaussian lemma and, based on it, Schering's proof of the generalized law of reciprocity, and Kronecker's representation of the symbol $\left(\frac{Q}{P}\right)$ (Q and P being any two positive, odd, relatively prime integers) as the sign of certain

---

* *Berl. Montasber.* 1872.

† It may be of interest to give in this connection a list of the proofs presented in various text-books:

Tschebyscheff, Gauss III.

Dedekind-Dirichlet, Gauss I, III, IV.

Serret (*Alg. Sup.*), Gauss III.

Bachmann (*Kreistheilung*), { Gauss VI, Eisenstein (*Crelle* 27). Liouville, Eisenstein (*Crelle* 29). Gauss IV (sketch).

Wertheim, Gauss V, Eisenstein (*Crelle* 28).

Mathews, Gauss I, III, Eisenstein (*Crelle* 27, in part).

products and the consequent simplification of Gauss' third proof, and as an application of Kronecker's representation another proof by Kronecker of the law of reciprocity, bring us into the field of the most recent researches in this subject.

SECTION IV. *Quadratic Forms.*—Varying the usual order, the author takes up first the representation of numbers by means of quadratic forms, and from this passes to transformation and equivalence of forms. Connection is made with quadratic residues by noticing that the question whether or not the *congruence* $x^2 \equiv n \pmod{m}$ can be satisfied is equivalent to the question whether or not the *form* $x^2 - n$ can represent at least one number which is a multiple of m. After defining forms, primitive and derived, properly and improperly primitive, the subsequent considerations are confined to *properly* primitive forms, i.e., forms

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

in which a, $2b$, c have no common divisor other than unity. The various cases of the value of the determinant $D = b^2 - ac$ are discussed, and, omitting less important theorems, the following fundamental results are reached:

I. *That the number m be properly representable by (a, b, c) of determinant D, it is necessary, though not sufficient, that D be quadratic residue of m.*

II. *Every proper representation of m by (a, b, c) belongs to a definite root of the congruence*

$$1) \quad \ldots\ldots x^2 \equiv D \pmod{m}.$$

This affords basis for the classification* of all possible representations of m by the form (a, b, c).

III. *All representations belonging to the same root of the above congruence are deduced from any one of them by means of the solutions of*

$$t^2 - Du^2 = 1.$$

This is the well-known Pellian equation, and its solutions are next found. In the only difficult case, viz., $D > 0$, it is shown, according to Dirichlet, how to derive all solutions from the fundamental solution ; i.e., that in which u has its smallest value.

* The author says "into groups." This is not happy, because the technical meaning of the term group has been used, and it is not shown that the classes of representations are, technically, a group, no multiplication law being defined.

In Nos. 12 and 14 of this section the method is indicated of finding all the representations of m by (a, b, c), $D > 0$, and then we pass to the "equivalence of quadratic forms," defined as follows:

Two quadratic forms of the same determinant are equivalent if every number which can be represented by the one can be represented also by the other by a representation belonging to the same root of the congruence 1) *as the first representation.*

With this definition as a basis, various particular theorems are established and illustrated, and finally the general result is reached:

Two forms of the same determinant are equivalent as soon as there exists at least one number m which can be represented by each form by a representation belonging in both cases to the same root of the congruence 1).

The subject of equivalence is concluded by translating the above *arithmetical* condition of equivalence into the ordinary *algebraic* condition, viz.:

The necessary and sufficient condition for the equivalence of two forms is that one can be transformed into the other by the substitution $x = \alpha x_1 + \beta y_1$, $y = \gamma x_1 + \delta y_1$, *where* $\alpha\delta - \beta\gamma = 1$.

The idea of equivalence affords a basis for the division of the infinity of properly primitive forms of the same determinant into *classes;* the forms of each class being equivalent with one another and with no others. The proof is next given that for every determinant D, *the number of classes is finite.* The next main problem considered is the determination of the representations of m by a *system of forms* consisting of one and only one form from each class of determinant D. The method is illustrated at length in an example. The decomposition of numbers into the sum of two squares is next discussed, improper representations being also considered in this case. After ambiguous forms and classes have been defined and illustrated, the problem of *composition of forms* is taken up. The method of composition having been defined, it is shown that the *class* of the resulting form is dependent only on the *classes* of the forms composed, that the process of composition is associative, commutative, and invertible. On account of these properties it is preferred to call the process *multiplication* rather than (with Gauss) *addition* of forms. From these results it follows that *the totality of equivalent properly primitive forms of given determinant constitutes a group,* and indeed a group whose elements are all commutative with one another. We see then immediately from Kronecker's theorem on commutative groups that certain classes can be selected such that all the others can be derived by composition of the selected classes with themselves. In a

paper on the composition of forms,* Schering showed how "to set up a complete system of fundamental classes which by composition give rise to each of the classes under consideration in a single definite manner." Though Schering's proof contained not a word about groups, yet it is not essentially connected with form classes, and translated into group language. Schering's results are nothing else than those published by Kronecker.

The author next gives his reasons for excluding the consideration of the division of classes into genera, and also of Gauss's second proof of the law of reciprocity, as well as that of Legendre and the first of Kummer, from a work confined to the *elements* of the theory of numbers, while Kummer's second proof, based only on the solution of the Pellian equation and the composition of forms, closes the section. These proofs all belong to the second category, mentioned before.

An excellent table of contents facilitates reference, and the presswork done by the house of publication is so well known that nothing need be said on this head. Spaced type has been introduced occasionally to make important theorems prominent, but more might have been done to assist the reader through the eye by means of the typography.

Though dealing with the elements of the subject, the book is not well adapted to serve as a first introduction because of the unhesitating use, wherever preferable from a theoretic point of view, of more abstract methods than would really be necessary. But precisely this commends it to one with some previous acquaintance with the subject. The work is a pleasing and welcome addition to the literature of the theory of numbers, on account of its contents and their manner of presentation, but still more as the forerunner of other volumes written in the same style and with the same aims, and dealing with the less elementary portions of the subject. There exists now quite a number of text-books covering the elementary field, but a clear, well-digested presentation in coördinated and unified form, brought down to the present time, of the principal results in the field beyond, is a real want. Our author proposes a continuation of his work : that it will deserve the characterization just written, the present volume gives reason to believe. It is to be hoped that he will be able speedily to bring this difficult task to a satisfactory conclusion.

J. W. A. YOUNG.

THE UNIVERSITY OF CHICAGO, *May* 1, 1894.

* *Gött. Abh.*, 1868.