BIBLIOGRAPHY.

Jacobi, *Fundamenta Nova.*

Cayley, *A memoir on the transformation of elliptic functions, Collected Math. Papers*, vol. 9, p. 113.

Clifford, *On the transformation of elliptic functions*, PROCEEDINGS OF THE LONDON MATH. SOC., vol. 7, 1875.

Darboux, *Sur une classe remarquable de courbes et de surfaces algébriques.*

Moutard, *Recherches analytiques sur les polygones simultanément inscrits et circonscrits à deux coniques.* Note added to Poncelet, *Applications d'analyse et de géométrie*, vol. 1.

UNIVERSITY OF CALIFORNIA,
BERKELEY, CALIFORNIA,
January 11, 1921.

BACHMANN ON FERMAT'S LAST THEOREM.

Das Fermatproblem in seiner bisherigen Entwickelung. By Paul Bachmann. Berlin and Leipzig, Walter de Gruyter, 1919. pp. viii + 160.

This volume reproduces to a considerable extent most of the important contributions which have so far been made toward a proof of Fermat's last theorem. It is far more complete than anything of the sort heretofore published. In particular, a reader of the book will find therein an account of the main results of Kummer, with proofs in most cases set forth in full. The writer wishes to call attention to the fact, however, that a number of references to articles bearing directly on some of the work given in the text have been omitted by Bachmann, a few of which will be noted, in detail, presently. If a better historical perspective is desired, it would be well for a reader to examine at the same time chapter 26, volume 2, of Dickson's *History of the Theory of Numbers.*

I shall now point out some parts of the text which give an account of results not given in detail elsewhere, aside from the original articles.* Consider

$$x^p + y^p + z^p = 0, \tag{1}$$

where x, y and z are rational integers, prime to each other, and p is an odd prime. The assumption that xyz is prime to p

* For an account of the more elementary results regarding the theorem, cf. Carmichael, *Diophantine Analysis*, chap. 5, or Bachmann, *Niedere Zahlentheorie*, vol. 2, chap. 9.

will be referred to as case I and the contrary assumption, $xyz \equiv 0 \pmod{p}$, as case II. In §§ 14–15 the researches of A. Fleck* are given. In §§ 23–24 the principles underlying Dickson's extensions of the method of Sophie Germain are set forth and the former's result is given that (1) is not satisfied in Case I for any $p < 7{,}000$ except perhaps 6,857.†

The proof of Dickson's theorem that there is at least one set of solutions in integers x, y and z, prime to each other and the prime q, of

$$x^p + y^p + z^p \equiv 0 \pmod{q},$$

if

$$q \geqq (p-1)^2(p-2)^2 + 6p - 2,$$

is reproduced in full (§§ 25–26) as well as the proof by Schur of an analogous result.

In § 32, Bachmann begins the treatment of (1) by the use of the cyclotomic field theory following the methods of Kummer. The class number h of the field defined by $e^{2i\pi/p}$ is referred to and the following statement (p. 104) is made:

"Die Kummersche Untersuchung ergibt ferner dass die Klassenzahl des Kreisteilungskörpers nur einmal durch eine Primzahl p teilbar ist, wenn diese nur in einer der gennanten Bernoullischen Zahlen aufgeht . . . ."

The class number h may have this property but Kummer's work does not prove it.‡

In §§ 36–37 is given substantially Hilbert's form of Kummer's proof that

$$\alpha^p + \beta^p + \gamma^p = 0$$

has no solution in integers α, β, γ, belonging to the cyclotomic field defined by $e^{2i\pi/p}$, provided p is a *regular* prime.

On page 111, the results given in Kummer's memoir§ of 1857 on Fermat's last theorem are mentioned, but no part of the argument is reproduced, except the derivation of the so-called Kummer criteria, namely that if (1) is satisfied in

* SITZUNGSBERICHTE MATH. GESELLSCHAFT BERLIN, vol. 8, p. 133, and vol. 9, p. 50.

† Dickson states that he has proved the result also for $p = 6857$, but he has not published the details. This would also follow from the relation $7 \times 6857 = 3 \times 2^7 \times 5^3 - 1$. See Vandiver, TRANS. AMER. MATH. SOC., vol. 15, p. 204.

‡ See the writer's criticism of a similar statement by Kummer, PROCEEDINGS NAT. ACAD. SCIENCES, vol. 6, p. 266 (May, 1920).

§ ABHANDLUNGEN, Berlin Academy, 1857, pp. 41–74.

Case I, then the congruences

$$B_s \frac{d_0^{p-2s} \log (x + e^v y)}{dv^{p-2s}} \equiv 0 \pmod{p} \qquad (s = 1, 2, \cdots, (p-3)/2), \tag{2}$$

all hold, where the B's are the Bernoulli numbers, $B_1 = 1/6$, $B_2 = 1/30$, etc., and where the symbol d_0^{p-2s}/dv^{p-2s} means that zero is substituted for v after the differentiation is performed. Setting $x + e^v y = (x, y)$, then the same congruences hold with (y, x), (x, z), (z, x), (y, z) and (z, y) substituted for (x, y). The greater part of Kummer's proof of (2) is reproduced, but there are several points in the work which are not brought out by either Kummer or Bachmann, and which might puzzle a reader going over it for the first time. For example our author does not reproduce the argument employed by Kummer to establish the relation

$$\Pi_i (x + \alpha^{g^i} y) = \pm \alpha^m f(\alpha)^p, \tag{3}$$

where g is a primitive root of p, and where i ranges over the integers in the set $0, 1, 2, \cdots, p-2$, which have the property $g_{\mu-1} + g_{\mu-1+\text{ind } r} > p$, where $\mu = (p-1)/2$ and g_s is defined as the least positive residue of g^s, modulo p, $r = 1, 2, \cdots, p-2$, $g^{\text{ind } r} \equiv r \pmod{p}$ and $\alpha = e^{2i\pi/p}$. In this connection it may be noted that the writer has not been able to justify Kummer's method* of showing that $\pm \alpha^m$ is the particular type of unit which appears in this relation.†

More details in the derivation of some of the other results regarding (3) would have been distinctly helpful to the reader; for example, in the derivation of relation 159 on page 114, and of the relation at the bottom of page 115.

On page 123, Bachmann outlines the method of Mirimanoff for proving that

$$\varphi(t) = (1+t)^{p-i} P_i(1, t) \qquad (i = 2, 3, \cdots, p-1)$$
$$\equiv t - 2^{i-1}t^2 + 3^{i-1}t^3 - \cdots - (p-1)^{i-1}t^{p-1} \pmod{p}$$

where

$$\frac{d_0^i \log (x + e^v y)}{dv^i} = \frac{P_i(x, y)}{(x+y)^i}.$$

* Kummer, loc. cit., p. 62, and CRELLE, vol. 35, p. 364.

† Compare with the writer's treatment of a similar problem, ANNALS OF MATHEMATICS, vol. 21, No. 2, Dec., 1919, pp. 74–75.

No reference is made to the much simpler method due to Frobenius* for obtaining the same result.

In connection with the derivation of the Kummer criteria, Bachmann does not mention (except on page 126 as to a minor detail) the researches of Cauchy, who anticipated Kummer in obtaining some of the important results related to these criteria. Cauchy† gave without proof a relation equivalent to (3) of this review for $r = 1$, and also stated that if (1) is possible in case I, then

$$1^{p-4} + 2^{p-4} + \cdots + ((p-1)/2)^{p-4} \equiv 0 \pmod{p},$$

which is a transformation of the criterion $B_{\mu-1} \equiv 0 \pmod{p}$. A consideration of these results in connection with the fact that Cauchy gave‡ a theorem regarding functions having properties similar to those of $\varphi(t)$, indicates the probability that he had obtained relations equivalent to two or more of the criteria of Kummer.

In §§ 47–48 an account is given of Frobenius' derivation§ of Mirimanoff's transformation of (2) which led the latter to the criteria $2^{p-1} \equiv 3^{p-1} \equiv 1 \pmod{p^2}$, for the solution of (1) in case I. This work of Frobenius is based on the symbolic method of Blissard|| for treating formulas involving Bernoulli's numbers.

On page 150, Bachmann makes a statement which would lead a reader to suppose that this work of Frobenius should be regarded as an introduction to the latter's later paper on Fermat's last theorem, the contents of which are not given by Bachmann. This is misleading, as the method employed in the second paper for deriving the relation

$$(x^p - 1)G_m^{k}(x) - (x^m - 1)F_{m;k}(x) \equiv H_m^{(k)}(x) \pmod{p}$$

is based on an extension of the method used by the writer¶ and is quite different from the method of Frobenius' earlier paper.

The book will constitute a valuable aid to anyone attempting a serious study of Fermat's last theorem.

H. S. VANDIVER.

* SITZUNGSBERICHTE MATH. GESELLSCHAFT BERLIN, July, 1910, p. 843.
† *Oeuvres*, (1), vol. 10, p. 362, Th. 3, and p. 364, Cor. 2.
‡ Loc. cit., p. 356, Th. 5.
§ SITZUNGSBERICHTE MATH. GESELLSCHAFT BERLIN, 1910, p. 200.
|| QUARTERLY JOURNAL, vol. 4, 1861, p. 279. Erroneously attributed to Lucas by numerous writers.
¶ CRELLE, vol. 144, p. 314.