NUMBERS OF SOLUTIONS OF EQUATIONS IN FINITE FIELDS

ANDRÉ WEIL

The equations to be considered here are those of the type

$$a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = b. \tag{1}$$

Such equations have an interesting history. In art. 358 of the *Disquisitiones* [1 a],[1] Gauss determines the Gaussian sums (the so-called cyclotomic "periods") of order 3, for a prime of the form $p=3n+1$, and at the same time obtains the numbers of solutions for all congruences $ax^3-by^3\equiv 1 \pmod{p}$. He draws attention himself to the elegance of his method, as well as to its wide scope; it is only much later, however, viz. in his first memoir on biquadratic residues [1b], that he gave in print another application of the same method; there he treats the next higher case, finds the number of solutions of any congruence $ax^4-by^4\equiv 1 \pmod{p}$, for a prime of the form $p=4n+1$, and derives from this the biquadratic character of 2 mod p, this being the ostensible purpose of the whole highly ingenious and intricate investigation. As an incidental consequence ("*coronidis loco*," p. 89), he also gives in substance the number of solutions of any congruence $y^2\equiv ax^4-b \pmod{p}$; this result includes as a special case the theorem stated as a conjecture ("*observatio per inductionem facta gravissima*") in the last entry of his *Tagebuch* [1c];[2] and it implies the truth of what has lately become known as the Riemann hypothesis, for the function-field defined by that equation over the prime field of p elements.

Gauss' procedure is wholly elementary, and makes no use of the Gaussian sums, since it is rather his purpose to apply it to the determination of such sums. If one tries to apply it to more general cases, however, calculations soon become unwieldy, and one realizes the necessity of inverting it by taking Gaussian sums as a starting point. The means for doing so were supplied, as early as 1827, by Jacobi, in a letter to Gauss [2a] (cf. [2b]). But Lebesgue, who in 1837 devoted two papers [3a, b] to the case $n_0= \cdots =n_r$ of equation (1), did not

Received by the editors October 2, 1948; published with the invited addresses for reasons of space and editorial convenience.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

[2] It is surprising that this should have been overlooked by Dedekind and other authors who have discussed that conjecture (cf. M. Deuring, Abh. Math. Sem. Hamburgischen Univ. vol. 14 (1941) pp. 197–198).