AN ELEMENTARY METHOD IN ALGEBRAIC NUMBER THEORY

S. A. Stepanov

The following is the author's abstract of his dissertation for the doctoral degree in the physical and mathematical sciences. The dissertation was defended Jan. 6, 1977, at a meeting of the special council D 002.38.02 of the V. A. Steklov Mathematics Institute of the Academy of Sciences of the USSR. The official examiners were: corresponding member of the Academy of Sciences of the USSR and doctor of physical and mathematical sciences D. K. Faddeev, corresponding member of the Academy of Sciences of the Belorussian SSR and doctor of physical and mathematical sciences V. G. Spirindzhuk, and professor and doctor of physical and mathematical sciences A. F. Lavrik.

The solution of arithmetic problems in number theory is characterized by the use of methods which are only indirectly related to the statement of the problems. It therefore naturally becomes of interest to seek direct methods which rest essentially on the arithmetic nature of the problem studied.

In problems in the theory of equations over finite fields, the most effective methods up to the present time have been those of abstract algebraic geometry. Starting in 1968, the author developed a constructive method in the theory of equations over finite fields, with the aid of which all the results deduced previously by algebrogeometric methods have recently been proved, as well as a number of new results.

Congruences modulo a prime p lie at the foundation of the theory of equations over finite fields. Isolated results concerning the number N_p of solutions of the congruences

$$f(x, y) \equiv 0 \pmod{p},$$

where f is a polynomial in x, y, with integral coefficients, were obtained long ago. Thus, Lagrange [1] in his solution of Fermat's problem on the expressibility of every natural number as a sum of four squares established that the congruence

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

is solvable. A far-reaching study of quadratic congruences was undertaken by Gauss [2]. He also obtained exact formulas for the number N_p of solutions of certain cubic and biquadratic congruences with two unknowns.

In 1924, Artin [3] conjectured that the number N_p of solutions of the hyperelliptic congruence

$$y^2 \equiv f(x) \pmod{p},$$

where f(x) is a polynomial of degree $n \geq 3$, which is square free modulo p, satisfies the estimate

$$|N_p - p| \leqslant \begin{cases} (n-1)\sqrt{p}, & n\text{—odd}, \\ (n-2)\sqrt{p}, & n\text{—even}. \end{cases}$$

This conjecture was proved by Hasse [4, 5] for n = 3, 4 using the theory developed by him of algebraic functions with a finite field of constants. Subsequently, Manin [6] undertook an elementary proof of Hasse's theorem.

Weil [7] extended the Hasse method to the general case of absolutely irreducible polynomials f(x, y), and he obtained for the number of solutions N_q of equations

$$f(x, y) = 0 \tag{1}$$

the estimate

$$|N_q - q| \leqslant 2g\sqrt{q}, \tag{2}$$

V. A. Steklov Mathematics Institute, Academy of Sciences of the USSR. Translated from Matematicheskie Zametki, Vol. 24, No. 3, pp. 425-431, September, 1978. Original article submitted February 21, 1978.

 0001-4346/78/2434-0728$07.50

in Galois fields K_q consisting of $q = p^r$ elements. Here g is the genus of the curve (1). This estimate is equivalent to an analog of the Riemann hypotheses for the zeta functions of fields generated by the curve (1). As a corollary of this result, the estimate

$$\left|\sum_{\substack{x\in K_q \\ f(x)\neq\infty}} e^{2\pi i S_p f(x)/p}\right| \leqslant c\,(f)\sqrt{q}$$

was obtained by a number of authors [8-12] for a trigonometric sum with a rational function f(x), and in particular, for the Weyl and Kloosterman sums.

However, Weil's proof of estimate (2) requires the use of methods of modern algebraic geometry and is very complicated.

In Chap. I of this dissertation we propose an elementary method for deriving estimate (2) for the case of a hyperelliptic curve

$$y^2 = f(x). \tag{3}$$

Namely, we prove the following theorem.

THEOREM 1. Let $n \geqslant 3$ be an odd number, r any natural number, p a prime, $p^r > 9n^2$, and let $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ be a polynomial with integral coefficients, $a_0 \not\equiv 0 \pmod p$. Then if N_q is the number of solutions of Eq. (3) in the field K_q consisting of $q = p^r$ elements, we have the estimate

$$|N_q - q| \leqslant \sqrt{3n}\, n \sqrt{q}.$$

An analogous estimate, which however, covers only the case of the congruences

$$y^m \equiv f(x) \pmod p$$

modulo a prime p, was obtained in the dissertation of the author submitted for the candidate's degree in the physical and mathematical sciences, and in the papers [23, 24]. The method of proof of Theorem 1 is a further development of the method proposed by the author in these papers and serves primarily as an illustration of the technical tools employed in Chap. II of the dissertation.

Using the theory of zeta-functions of curves, the result of Theorem 1 can easily be strengthened.

COROLLARY 1. In the notation of Theorem 1 we have

$$|N_q - q| \leqslant (n-1)\sqrt{q}. \tag{4}$$

We remark that for the case of a prime field K_p, some improvements of the method of the author [23] permitted Stark [16] and others [17, 18] to obtain a stronger estimate than (4). They thereby obtained results stronger than those equivalent to the Riemann hypothesis for the zeta functions of the corresponding curves.

Chapter II of the dissertation is devoted to an elementary proof of the Weil–Bombieri estimate for rational trigonometric sums with prime denominator.

Let p be a prime number, $P(x) = x^m + a_1x^{m-1} + \ldots + a_m$, $Q(x) = x^n + b_1x^{n-1} + \ldots + b_n$ mutually prime polynomials with coefficients in the residue field mod p, and put f(x) = P(x)/Q(x). We put

$$S_\nu^{(r)}(f) = \sum_{\substack{x\in K_q \\ Q(x)\neq 0}} e^{2\pi i\nu S p f(x)/p},$$

where $q = p^r$ and $s_p f(x) = f(x) + f(x)^p + \ldots + f(x)^{p^{r-1}}$.

THEOREM 2. Let $m \neq n$, $d = \max(m, n) \geqslant 2$, $p > d$, and $r > 12$. If N_q is the number of solutions of the equation

$$y^p - y = f(x) \tag{5}$$

in fields K_q consisting of $q = p^r$ elements, we have the estimate

$$|N_q - q| \leqslant 15d^2p^{s/2}p^{r/2}.$$

COROLLARY 1. Let $m \neq n$ and $r > 1$. Then if N_q is the number of solutions of Eq. (5) in the fields K_q consisting of $q = p^r$ elements, we have the estimate

$$|N_q - q| \leqslant 2g\sqrt{q},$$

where g is the genus of (5).

COROLLARY 2. If $m \neq n$ and $v \not\equiv 0 \pmod{p}$ we have

$$|S_v^{(r)}| \leqslant (l - 2 + \sum_{i=1}^{l} d_i) p^{r/2}, \quad r = 1, 2, \ldots, \tag{6}$$

where l is the number of distinct poles of f(x) counting the point at infinity, and d_i is the multiplicity of a pole.

We note two interesting special cases of inequality (6) leading to estimates for the classical sums of Weyl and Kloosterman.

COROLLARY 3. Let m be a natural number, p > m a prime, and let f(x) be a polynomial of degree m with integer coefficients. Then

$$\left|\sum_{x=1}^{p-1} e^{2\pi i f(x)/p}\right| \leqslant (m-1)\sqrt{p}. \tag{7}$$

COROLLARY 4. Let $v \not\equiv 0 \pmod{p}$. Then for p > 2

$$\left|\sum_{x=1}^{p-1} e^{2\pi i (vx + a/x)/p}\right| < 2\sqrt{p}. \tag{8}$$

Estimates (4), (7), (8) are of fundamental importance in many questions in number theory such as the distribution of power residues and nonresidues, estimates of rational trigonometric sums, the representation of natural numbers by means of quadratic forms, etc.

Chapter III of the dissertation is devoted to the study of congruences

$$f(x, y) \equiv 0 \pmod{p} \tag{9}$$

with a polynomial f(x, y) of general type.

Let $m, n \geqslant 2$ be mutually prime numbers; $p > 196m^3n(n-1)^2$ a prime number; K_p the residue field mod p; f(x, y) a polynomial in x, y with coefficients in K_p. The following theorem is proved.

THEOREM 3. Let $f(x, y) = y^n + a_1(x)y^{n-1} + \ldots + a_n(x)$ be irreducible over the field K_p and assume the degrees of the polynomials $a_i(x)$ satisfy the conditions

$$\deg a_n(x) = m; \quad n \deg a_i(x) < im, \quad i = 1, 2, \ldots, n-1. \tag{10}$$

Then if N_p is the number of solutions of (9), we have the estimate

$$|N_p - p| \leqslant 14\sqrt{mn}\, m(n-1)\sqrt{p}.$$

Like the proofs of Theorems 1 and 2, the proof of Theorem 3 is based on the construction of a polynomial R(x) of degree which is not too high and having as roots of sufficiently high multiplicity those values of the variable x (with the exception of $O(1)$ many values) which are solutions of congruence (9). Comparison of the number of roots of the polynomial R(x) taken with multiplicity with the degree of R(x) gives an upper bound for the number N_p. A lower bound for N_p is obtained analogously.

The principal factor in all these constructions is the existence of Fermat's little theorem stating that

$$x^q = x.$$

We emphasize that we do not require in Theorem 3 the condition that the polynomial f(x, y) be absolutely irreducible, which is hard to verify, but instead require only that it be irreducible in the field K_p and that the simple conditions (10) hold. We remark that these conditions can be regarded as a new criterion for the absolute irreducibility of the polynomial f(x, y).

The method of the author has been extended by Schmidt [19] to the general case of arbitrary finite fields. In Bombieri [21], this method was significantly simplified by not insisting on explicit constructions. It should, however, be remarked that explicit constructions have the advantage that they can be used to obtain stronger results than those following from general theories.

Finally, the above method permitted Schmidt [20] to strengthen somewhat the previously known [22] estimate for the number N_q of solutions over a field K_q of equations in several unknowns.

The results of the dissertation were reported at the All-Union Conference on Number Theory in Tbilisi (1970), at the International Conference on Number Theory dedicated to the 80-th anniversary of academician I. M. Vinogradov in Moscow (1971), at the All-Union School of Number Theory in Minsk (1972), at the All-Union Conference on Number Theory in Samarkand (1972), and at the International Congress of Mathematicians in Vancouver (Canada, 1974), and they have been published in [25-30].

LITERATURE CITED

1. J. L. Lagrange, Oevres, T. 3, Gauthier-Villars, Paris (1896), pp. 189-201.
2. C. F. Gauss, Werke, Bd. 2, Göttingen (1863).
3. E. Artin, "Quadratische Körper im Gebiete der höheren Kongruenzen. II," Math. Z., 19, 207-246 (1924).
4. H. Hasse, "Abstrakte Begründung der komplexen Multiplication und Riemannsche Vermutung in Funktionenkörper," Abhand. Math. Sem. Univ. Hamburg, 10, 325-348 (1934).
5. H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper. I-III," J. Reine Ang. Math., 175, 55-62, 69-88, 193-208 (1936).
6. Yu. I. Manin, "On congruences of the third degree with respect to a prime modulus," Izv. Akad. Nauk SSSR, Ser. Mat., 20, 673-678 (1956).
7. A. Weil, "Sur les courbes algébriques et les variétés que s'en déduisent," Act. Sci. Ind., 1041, Hermann, Paris (1948).
8. A. Weil, "On some exponential sums," Proc. Nat. Acad. Sci., 34, No. 5, 204-207 (1948).
9. L. Carlitz and S. Uchiyama, "A bound for exponential sums," Duke Math. J., 24, No. 1, 37-41 (1957).
10. L. Carlitz, "Kloosterman sums and finite field extensions," Acta. Arithm., 16, No. 2, 179-193 (1969).
11. E. Bombieri, "On exponential sums in finite fields," Am. J. Math., 88, No. 1, 71-105 (1966).
12. G. I. Perel'muter, "On some character sums," Usp. Mat. Nauk, 18, No. 2, 145-149 (1963).
13. M. Eichler, Einführung in die Theorie der algebraischen Zahlen und Funktionen, Basel-Stuttgart (1963).
14. S. Lang, Abelian Varieties, Wiley-Interscience, New York (1959).
15. A. G. Postnikov, "Ergodic problems in the theory of congruence and theory of Diophantine approximations," Tr. Mat. Inst. Akad. Nauk SSSR, 82 (1966).
16. H. M. Stark, "On the Riemann hypothesis in hyperelliptic function fields," Proc. Symp. Pure Math., 24, 285-302 (1973).
17. N. M. Korobov, "An estimate for a sum of Legendre symbols," Dokl. Akad. Nauk SSSR, 196, No. 4, 764-767 (1971).
18. D. A. Mit'kin, "An estimate for a sum of Legendre symbols of polynomials of even degree," Mat. Zametki, 14, No. 1, 73-81 (1973).
19. W. M. Schmidt, "Zur Methode von Stepanov," Acta. Arithm., 24, No. 4, 347-368 (1973).
20. W. M. Schmidt, "A lower bound for the number of solutions of equations over finite fields," J. Number Theory, 6, 448-480 (1974).
21. E. Bombieri, "Counting points on curves over finite fields (after S. A. Stepanov)," Sém. Bourbaki, Vol. 25, No. 430 (1972-73), pp. 234-241.
22. S. Lang and A. Weil, "Number of points of varieties in finite fields," Amer. J. Math., 76, No. 4, 819-827 (1954).
23. S. A. Stepanov, "On the number of points of a hyperelliptic curve over a finite prime field," Izv. Akad. Nauk SSSR, Ser. Mat., 33, No. 5, 1171-1181 (1969).
24. S. A. Stepanov, "Elementary method in the theory of congruences for a prime modulus," Acta. Arithm., 17, No. 3, 231-247 (1970).
25. S. A. Stepanov, "An elementary proof of the Hasse-Weil theorem for hyperelliptic curves," J. Number Theory, 4, No. 2, 118-143 (1972).
26. S. A. Stepanov, "On an estimate for rational trigonometric sums with prime denominator," Tr. Mat. Inst. Akad. Nauk SSSR, 112, 346-372 (1971).
27. S. A. Stepanov, "Congruences with two unknowns," Izv. Akad. Nauk SSSR, Ser. Mat., 36, 683-711 (1972).
28. S. A. Stepanov, "A constructive method in the theory of equations over finite fields," Tr. Mat. Inst. Akad. Nauk SSSR, 122, 237-246 (1973).
29. S. A. Stepanov, "Rational points of algebraic curves over finite fields," in: Current Problems in Analytic Number Theory [in Russian], Minsk (1974), pp. 223-243.
30. S. A. Stepanov, "An elementary method in the theory of equations over finite fields," in: Proc. Int. Cong. Mathematicians, Vancouver (1974), pp. 383-391.