

CONGRUENCES MODULO A POWER OF A PRIME NUMBER

S. A. Stepanov

1969

SovietRxiv

View the original and related papers at <https://sovietrxiv.org/items/ru-196901.85885>

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.

Abstract

Full Text

UDC 511.26

MATHEMATICS

S. A. STEPANOV

CONGRUENCES MODULO A POWER OF A PRIME NUMBER

(Presented by Academician I. M. Vinogradov on 1 X 1968)

1. Let

$$F(x, y) = y^n + P_1(x)y^{n-1} + \dots + P_{n-1}(x)y + P_n(x)$$

be an absolutely irreducible polynomial with integer rational coefficients, and let p be a prime number. In the present paper we study the number of solutions of the congruence

$$F(x, y) \equiv 0 \pmod{p^m}, \quad (1)$$

where x and y run through an incomplete system of residues.

In the special case, namely for the congruence $x^2 + y^2 \equiv 1 \pmod{p^m}$, such an investigation was carried out by L. P. Postnikova ⁽¹⁾. This investigation was based essentially on the fact that the congruence has the form $y^n \equiv f(x) \pmod{p^m}$. The congruence $ax^3 + y^3 \equiv 1 \pmod{p^m}$, considered by P. D. Varbanets ⁽²⁾, has the same form. We shall show in what way an investigation of the general case (1) can be carried out.

In what follows, by $D(x)$ we shall denote the discriminant of the polynomial $F(x, y)$, and by $c_1, c_2, \dots$ positive constants depending only on the polynomial $F(x, y)$. Denote by $N(F, p)$ the number of solutions of the congruence $F(x, y) \equiv 0 \pmod{p}$. A well-known result of A. Weil ⁽³⁾ asserts that for the quantity $N(F, p)$ the estimate

$$|N(F, p) - p| < c_1 \sqrt{p}.$$

Theorem. Let $m > c_2$ be a natural number,

$$p^{(m-1)/\{c_3(m-1)-n\}-1} \leq T_1 \leq p^m, \quad 1 \leq T_2 \leq p^m.$$

Denote by $A(T_1, T_2)$ the number of solutions of the congruence (1) such that $D(x) \not\equiv 0 \pmod{p}$, for which $0 \leq x \leq T_1 - 1$, $0 \leq y \leq T_2$. Then for the quantity $A(T_1, T_2)$ we have the expression

$$A(T_1, T_2) = \frac{T_1 T_2}{p^m} \frac{N(F, p) + O(1)}{p} + O\left(e^{7m \ln^2 m} T_1^{-1/12m^3 \ln 12m^3}\right),$$

where the constants entering the symbol O depend only on the polynomial F .

2. Suppose that (x_0, y_0) is a solution of the congruence $F(x, y) \equiv 0 \pmod{p}$ such that

$$D(x_0) \not\equiv 0 \pmod{p}. \quad (2)$$

Lemma 1. Let condition (2) be fulfilled. Then for any rational integer t , $0 \leq t \leq p^{m-1} - 1$, there exists a unique solution of the congruence

$$F(x_0 + pt, y) \equiv 0 \pmod{p^m}$$

such that $y \equiv y_0 \pmod{p}$.

This lemma is a variant of the well-known Hensel lemma (see ⁽⁴⁾, p. 365).

Lemma 2. Let θ be a primitive integer of the field of algebraic numbers K , let $f(y)$ be its minimal polynomial, and let p be a prime number not dividing the discriminant of the polynomial f . Suppose that modulo p there is the factorization

$$f(y) \equiv f_1(y) \cdots f_s(y) \pmod{p},$$

where $f_1, \dots, f_s$ are irreducible integral polynomials of degrees $n_1, \dots, n_s$, respectively, pairwise distinct modulo p . Then the decomposition of the number p into a product of prime divisors of the field K has the form

$$p = \mathfrak{p}_1 \cdots \mathfrak{p}_s,$$

where the distinct prime divisors $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ have degrees $n_1, \dots, n_s$, respectively, and moreover $f_i(\theta) \equiv 0 \pmod{\mathfrak{p}_i}$ for each $i = 1, 2, \dots, s$.

For the proof see [4], p. 271, Theorem 8.

Lemma 3. There exists a polynomial of degree not exceeding $m - 1$

$$y(t) = \sum_{\nu=0}^{m-1} e_\nu(x_0, y_0) p^{\lambda_\nu} t^\nu,$$

for which $e_\nu(x_0, y_0)$, $\nu = 0, 1, \dots, m - 1$, are integral rational numbers relatively prime to p , and λ_ν are nonnegative integral rational numbers satisfying the inequalities $\lambda_\nu \geq \nu$, $\nu = 0, 1, \dots, m - 1$, such that

$$F(x_0 + pt, y(t)) \equiv 0 \pmod{p^m}$$

and $y(t) \equiv y_0 \pmod{p}$.

Proof. We have

$$F(x_0 + pt, y) = y^n + P_1(x_0 + pt)y^{n-1} + \dots + P_{n-1}(x_0 + pt)y + P_n(x_0 + pt).$$

Put $z = pt$ and consider $F(x_0 + z, y)$ as a polynomial in z, y . Denote by $f(y)$ an irreducible divisor of the polynomial $F(x_0, y)$ for which y_0 is a root of the congruence $f(y) \equiv 0 \pmod{p}$. Let θ be a root of the polynomial $f(y)$ in the finite extension $K = R(\theta)$ of the field of rational numbers R . Denote by a_0 a root of the congruence $f(y) \equiv 0 \pmod{p^m}$. By Lemma 2, in view of condition (2), we obtain that

$$\theta \equiv a_0 \pmod{\mathfrak{p}^m}, \quad (3)$$

where $\mathfrak{p}$ is a prime divisor of the field K of degree one occurring in p .

Consider the equation $F(x_0 + z, y) = 0$ over the ring of integral rational numbers. Let $y = v(z)$ be a solution of this equation in a neighborhood of $z = 0$, and let $v(0) = \theta$. By condition (2), the point $z = 0$ will be regular, and $v(z)$ in some neighborhood of this point expands into a power series

$$v(z) = \theta + \sum_{\nu=1}^{\infty} \theta_{\nu} z^{\nu}.$$

It is easy to show that all $\theta_{\nu} \in K$. Further, from the Eisenstein theorem ([5], p. 155), again using condition (2), it is easy to obtain that the coefficients θ_{ν} of the expansion of $v(z)$ into a power series will be $\mathfrak{p}$ -integral. Hence, in view of (3), we obtain that $v(pt) \equiv \sum_{\nu=0}^{m-1} a_{\nu} t^{\nu} \pmod{\mathfrak{p}^m}$, where a_{ν} are integral rational numbers, and that $F(x_0 + pt, v(pt)) \equiv 0 \pmod{p^m}$. Representing now a_{ν} , $\nu = 0, 1, \dots, m-1$, in the form $a_{\nu} = e_{\nu}(x_0, y_0)p^{\lambda_{\nu}}$ and denoting $v(pt) = y(t)$, we obtain the assertion of the lemma.

The following lemma belongs to Dudzi.

Lemma 4. Let the function

$$a(z) = \sum_{\nu=0}^{\infty} a_{\nu} z^{\nu}$$

be regular in the unit disk $|z| < 1$, and let all singularities of this function for $|z| = 1$ be algebraic. Let n be the number of these singularities.

Then, for $\nu \geq \nu_0$,

$$0 < Ar^{\nu} \leq |a_{\nu}| + |a_{\nu+1}| + \dots + |a_{\nu+n-1}| \leq Br^{\nu},$$

where r is a rational number distinct from a negative integer, and A and B are certain constants independent of ν .

From this lemma it follows directly that if the series

$$v(z) = \theta + \sum_{\nu=1}^{\infty} \theta_{\nu} z^{\nu}$$

has radius of convergence $\lambda > 0$, then for $\nu \geq \nu_0$ the estimate $|\theta_{\nu}| \leq c_4 \nu^{c_5} \lambda^{-\nu}$ holds, and among n consecutive coefficients θ_{ν} at least one is nonzero. The same is also true for all conjugate numbers θ_{ν} in the field K . Then it is easy to obtain that, for $m > c_6(\nu_0 + n + 2) + 1 = c_2$, $\nu_0 \leq \nu \leq m/c_6$, for $a_{\nu} \neq 0$ the estimate $v_p(a_{\nu}) \leq c_7 \nu$ holds, where $v_p(\alpha)$ is the p -adic exponent of the number α . Thus we have proved:

Lemma 5. *Let the polynomial*

$$y(t) = \sum_{\nu=0}^{m-1} e_{\nu}(x_0, y_0) p^{\lambda_{\nu}} t^{\nu}$$

be defined by Lemma 3, and let $m > c_2$. Then for $\nu_0 \leq \nu < m/c_6 - n$, and for any x_0, y_0 that are solutions of the congruence $F(x, y) \equiv 0 \pmod{p}$ and satisfy condition (2), the estimate

$$\min(\lambda_{\nu}, \lambda_{\nu+1}, \dots, \lambda_{\nu+n-1}) \leq c_6(\nu + n) \quad (c_6 \geq c_7)$$

holds.

3. We proceed to the proof of the theorem. Suppose that $T_1 = pU - 1$. On the basis of Lemma 3 it is clear that $A(pU - 1, T_2)$ is equal to the number of fractional parts

$$\{[e_0(x_0, y_0) + e_1(x_0, y_0)p^{\lambda_1}t + \dots + e_{m-1}(x_0, y_0)p^{\lambda_{m-1}}t^{m-1}]/p^m\},$$

where x_0, y_0 run through all solutions of the congruence $F(x, y) \equiv 0 \pmod{p}$ such that $D(x_0) \not\equiv 0 \pmod{p}$, and $t = 0, 1, \dots, U - 1$, which fall in the interval $(0, T_2/p^m)$.

Denote by $\chi(t)$ the characteristic function of the interval $(0, T_2/p^m)$. Then

$$A(pU - 1, T_2) = \sum_{\substack{x_0, y_0 \\ D(x_0) \not\equiv 0 \pmod{p}}} \chi\left(\frac{e_0 + e_1 p^{\lambda_1} t + \dots + e_{m-1} p^{\lambda_{m-1}} t^{m-1}}{p^m}\right).$$

By a known method, the study of the number of fractional parts is reduced to estimating the modulus of the trigonometric sum

$$\sum_{t=0}^{U-1} \exp \left(2\pi i n \frac{e_0 + e_1 p^{\lambda_1} t + \dots + e_{m-1} p^{\lambda_{m-1}} t^{m-1}}{p^m} \right).$$

Put $\mu = [(m-1)/c_6 - n]$. From the condition $m > c_6(\nu_0 + n + 2) + 1$ it follows that $\mu \geq \nu_0 + 2$. Moreover, it is obvious that $\mu \leq (m-1)/c_6 - n$. Then by Lemma 5

$$\min(\lambda_\mu, \lambda_{\mu+1}, \dots, \lambda_{\mu+n-1}) \leq c_6(\mu + n) \leq m - 1.$$

Applying to the trigonometric sum (4) the estimate of I. M. Vinogradov (see (7), p. 389), which we shall carry out with respect to the coefficient of t^ν , where ν is equal to that one of the numbers $\mu, \mu+1, \dots, \mu+n-1$ for which $\lambda_\mu \leq m-1$, gives

$$\left| \sum_{t=0}^{U-1} \exp \left\{ 2\pi i n \frac{e_0 + e_1 p^{\lambda_1} t + \dots + e_{m-1} p^{\lambda_{m-1}} t^{m-1}}{p^m} \right\} \right| \leq \\ \leq e^{7m \ln^2 m} n^{27/32m^2 \ln 8m^2} U^{1-1/3m^3 \ln 12m^3}.$$

Then we obtain

$$A(pU - 1, T_2) = \frac{T_2 U}{p^m} \sum_{\substack{x_0, y_0 \\ D(x_0) \not\equiv 0 \pmod{p}}} + O\left(e^{7m \ln^2 m} p U^{1-1/6m^3 \ln 12m^3}\right).$$

Representing T_1 in the form $T_1 = pU - r$, where $1 \leq r \leq p-1$, it is then easy to show that

$$A(T_1, T_2) = \frac{T_1 T_2}{p^m} \frac{N(F, p)}{p} + O(1) + O\left(e^{7m \ln^2 m} T_1^{-1/12m^3 \ln 12m^3}\right).$$

The theorem is thereby proved.

Steklov Mathematical Institute
Academy of Sciences of the USSR

Received
1 X 1968

CITED LITERATURE

- ¹ L. P. Postnikova, *Matem. sborn.*, 65, no. 2, 228 (1964).
- ² P. D. Varbanets, *Analytic Theory of Congruences Modulo a Power of a Prime Number*, Abstract of Candidate's Dissertation, Saratov, 1967.
- ³ A. Weil, *Sur les courbes algébriques et les variétés qui s' en déduisent*, Act. Sci. Ind., 1041, Paris, 1948.
- ⁴ Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Moscow, 1964.
- ⁵ G. Pólya, G. Szegő, *Problems and Theorems in Analysis*, 2, Moscow, 1956.
- ⁶ M. Tsuji, *Japan. J. Math.*, 3, No. 1-2, Tokyo, 69 (1926).
- ⁷ I. M. Vinogradov, *Selected Works*, Publishing House of the Academy of Sciences of the USSR, 1952.

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.