Mathematica Slovaca

Stanislav Jakubec

Note on the number of solutions of the congruence $f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{p}$

Mathematica Slovaca, Vol. 44 (1994), No. 2, 163--169

Persistent URL: http://dml.cz/dmlcz/136607

Mathematica Slovaca
©1994
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **44** (1994), No. 2, 163–169

Dedicated to Academician Štefan Schwarz on the occasion of his 80th birthday

NOTE ON THE NUMBER OF SOLUTIONS OF THE CONGRUENCE $f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{p}$

STANISLAV JAKUBEC

(Communicated by Milan Paštéka)

ABSTRACT. In this paper, we find the number N_p modulo p of the solutions of the congruence $f(X_1, X_2, \ldots, X_n) \equiv 0 \pmod{p}$.

Let $f(X_1, X_2, \ldots, X_n)$ be a polynomial in the n-variables $X_1, X_2, \ldots, X_n$ with integral coefficients, say

$$f(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{m} d_i X_1^{a_{i1}} X_2^{a_{i2}} \ldots X_n^{a_{in}}, \qquad d_i \not\equiv 0 \pmod{p}.$$

Let p be a prime, $p \neq 2$, and denote by N_p the number of solutions of the congruence

$$f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{p}, \qquad x_1 x_2 \ldots x_n \not\equiv 0 \pmod{p}. \tag{1}$$

Put

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ a_{31} & \ldots\ldots\ldots\ldots & & \\ \ldots\ldots\ldots\ldots\ldots & & & \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

The aim of this paper is to prove the following theorem, which determines N_p modulo p.

AMS Subject Classification (1991): Primary 11D79.
Key words: Number of solutions of congruence.

THEOREM. *Let p be a prime, $p \neq 2$. The number N_p of solutions of congruence (1) satisfies the congruence*

$$N_p \equiv (-1)^{n+1} m + (-1)^n \left(1 + \sum_{\substack{u_1,u_2,\ldots,u_m \\ 0 \le u_j < p-1 \\ (u_1,u_2,\ldots,u_m)A \equiv \mathbf{0} \pmod{p-1} \\ u_1+u_2+\cdots+u_m = p-1}} \frac{d_1^{u_1} d_2^{u_2} \ldots d_m^{u_m}}{u_1! u_2! \ldots u_m!} \right) \pmod{p}.$$

P r o o f. Set

$$\alpha = \sum_{\substack{x_1,x_2,\ldots,x_n \\ x_1 x_2 \ldots x_n \not\equiv 0 \pmod{p}}} \zeta_p^{f(x_1,x_2,\ldots,x_n)},$$

where $\zeta_p = \cos\frac{2\pi}{p} + \mathrm{i}\sin\frac{2\pi}{p}$, and each of $x_1, x_2, \ldots, x_n$ runs through a complete residue system modulo p subject to $x_1 x_2 \ldots x_n \not\equiv 0 \pmod{p}$.

Clearly, $\alpha \in \boldsymbol{Q}(\zeta_p)$, and we have

$$\mathrm{Tr}_{\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}}(\alpha) = (p-1)N_p - \left((p-1)^n - N_p\right) = pN_p - (p-1)^n. \tag{2}$$

Let p be a prime with $p \equiv 1 \pmod{l}$, and let K be a subfield of the field $\boldsymbol{Q}(\zeta_p)$ of degree l over $\boldsymbol{Q}$. Let a be a primitive root modulo p. Let σ denote an automorphism of the field $\boldsymbol{Q}(\zeta_p)$ such that $\sigma(\zeta_p) = \zeta_p^a$. We also set

$$\beta_1 = \mathrm{Tr}_{\boldsymbol{Q}(\zeta_p)/K}(\zeta_p); \qquad \beta_i = \sigma^{i-1}(\beta_1) \quad \text{for} \quad i = 1, 2, \ldots l;$$
$$k = \frac{p-1}{l}; \qquad a^k \equiv g \pmod{p}.$$

The numbers $\beta_1, \beta_2, \ldots \beta_l$ are called the *Gaussian periods*, and it is known they form a normal integral basis for $K/\boldsymbol{Q}$.

The following lemma was proved in [1].

LEMMA. *There is a number $\pi \in K$, $\pi \mid p$, such that*

(i) $N_{K/\boldsymbol{Q}}(\pi) = (-1)^l p$,

(ii) $\sigma(\pi) \equiv g\pi \pmod{\pi^{l+1}}$,

(iii) $\beta_1 \equiv k \sum_{i=0}^{n} \frac{1}{(ki)!} \pi^i \pmod{\pi^{l+1}}$.

From the lemma, in case $l = p-1$, $K = \boldsymbol{Q}(\zeta_p)$, we have:

$$\zeta_p \equiv 1 + p + \frac{1}{1!}\pi + \frac{1}{2!}\pi^2 + \cdots + \frac{1}{(p-2)!}\pi^{p-2} \pmod{\pi^p}.$$

If c is an integer not divisible by p, we denote by σ_c the automorphism such that $\sigma_c(\zeta_p) = \zeta_p^c$. Hence

$$\alpha = \sum_{\substack{x_1,x_2,\ldots,x_n \\ x_1x_2\ldots x_n \not\equiv 0 \pmod p}} \zeta_p^{f(x_1,x_2,\ldots,x_n)} = \sum_{\substack{x_1,x_2,\ldots,x_n \\ x_1x_2\ldots x_n \not\equiv 0 \pmod p}} \prod_{i=1}^{m} \sigma_{d_i}\sigma_{x_1}^{a_{i1}}\sigma_{x_2}^{a_{i2}}\ldots\sigma_{x_n}^{a_{in}}(\zeta_p)$$

$$\equiv \sum_{\substack{x_1,x_2,\ldots,x_n \\ x_1x_2\ldots x_n \not\equiv 0 \pmod p}} \prod_{i=1}^{m} \sigma_{d_i}\sigma_{x_1}^{a_{i1}}\sigma_{x_2}^{a_{i2}}\ldots\sigma_{x_n}^{a_{in}}\left(1 + \sum_{j=1}^{p-2}\frac{\pi^j}{j!}\right) \pmod{\pi^p}.$$

Therefore

$$\alpha \equiv (1+p)^m \sum_{\substack{x_1,x_2,\ldots,x_n \\ x_1x_2\ldots x_n \not\equiv 0 \pmod p}} \prod_{i=1}^{m}\left(1 + \sum_{j=1}^{p-2}\frac{(d_i x_1^{a_{i1}}x_2^{a_{i2}}\ldots x_n^{a_{in}})^j\pi^j}{j!}\right) \pmod{\pi^p}.$$

Multiplying out the product we obtain

$$\alpha \equiv (1+p)^m \sum_{\substack{x_1,x_2,\ldots,x_n \\ x_1x_2\ldots x_n \not\equiv 0 \pmod p}} \big(1 + F_1(x_1,x_2,\ldots,x_n)\pi + F_2(x_1,x_2,\ldots,x_n)\pi^2 + \ldots$$
$$\cdots + F_{p-1}(x_1,x_2,\ldots,x_n)\pi^{p-1}\big) \pmod{\pi^p}.$$

By Lemma, we have

$$\mathrm{Tr}_{\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}}(\pi^k) = \pi^k + g^k\pi^k + g^{2k}\pi^k + \cdots + g^{k(p-2)}\pi^k \pmod{\pi^p};$$

hence, if $k < p-1$, then

$$\mathrm{Tr}_{\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}}(\pi^k) \equiv 0 \pmod{\pi^p}.$$

This implies

$$\mathrm{Tr}_{\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}}(\alpha)$$
$$\equiv (1+p)^m \,\mathrm{Tr}_{\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}}\left(\sum_{\substack{x_1,x_2,\ldots,x_n \\ x_1x_2\ldots x_n \not\equiv 0 \pmod p}} \big(1 + F_{p-1}(x_1,x_2,\ldots,x_n)\pi^{p-1}\big)\right) \pmod{\pi^p}.$$

The polynomial $F_{p-1}(x_1, x_2, \dots, x_n)$ has the form

$$F_{p-1}(x_1, x_2, \dots, x_n) = K x_1^{A_1} x_2^{A_2} \dots x_n^{A_n},$$

where K is a constant independent of $x_1, x_2, \dots, x_n$.

Clearly,

$$\sum_{\substack{x_1, x_2, \dots, x_n \\ x_1 x_2 \dots x_n \not\equiv 0 \pmod p}} K x_1^{A_1} x_2^{A_2} \dots x_n^{A_n} \equiv 0 \pmod p$$

if some A_i is not divisible by $p-1$, and

$$\sum_{\substack{x_1, x_2, \dots, x_n \\ x_1 x_2 \dots x_n \not\equiv 0 \pmod p}} K x_1^{A_1} x_2^{A_2} \dots x_n^{A_n} \equiv K(p-1)^n \pmod p$$

if

$$A_1 \equiv A_2 \equiv \dots \equiv A_n \equiv 0 \pmod{p-1}.$$

The Lemma gives

$$N_{\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}}(\pi) \equiv (-1)^{p-1} p \equiv \pi g \pi g^2 \pi \dots g^{p-2} \pi \pmod{\pi^p},$$

which implies

$$\pi^{p-1} \equiv -p \pmod{\pi^p}.$$

Therefore we obtain

$$\begin{aligned} &\operatorname{Tr}_{\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}}(\alpha) \\ &\equiv (1+p)^m (p-1)^{n+1} \left(1 - p \sum_{\substack{u_1, u_2, \dots, u_m \\ 0 \le u_j < p-1 \\ (u_1, u_2, \dots, u_m) A \equiv \mathbf{0} \pmod{p-1} \\ u_1 + u_2 + \dots + u_m = p-1}} \frac{d_1^{u_1} d_2^{u_2} \dots d_m^{u_m}}{u_1! u_2! \dots u_m!} \right) \pmod{\pi^p}, \end{aligned}$$

and so, from (2), we deduce

$$\begin{aligned} &pN_p - (p-1)^n \\ &\equiv (1+p)^m (p-1)^{n+1} \left(1 - p \sum_{\substack{u_1, u_2, \dots, u_m \\ 0 \le u_j < p-1 \\ (u_1, u_2, \dots, u_m) A \equiv \mathbf{0} \pmod{p-1} \\ u_1 + u_2 + \dots + u_m = p-1}} \frac{d_1^{u_1} d_2^{u_2} \dots d_m^{u_m}}{u_1! u_2! \dots u_m!} \right) \pmod{\pi^p}. \end{aligned}$$

and the assertion of Theorem follows. □

E x a m p l e 1. Using Theorem 1 we determine the number of solutions of the congruence

$$X^3 + aX + b \equiv 0 \pmod{p}, \qquad ab \not\equiv 0 \pmod{p}.$$

Clearly,

$$A = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix},$$

and so

$$N_p \equiv 3 - \left(1 + \sum_{\substack{u_1,u_2,u_3 \\ 0 \le u_j < p-1 \\ 3u_1+u_2 \equiv 0 \pmod{p-1} \\ u_1+u_2+u_3 = p-1}} \frac{a^{u_2} b^{u_3}}{u_1! u_2! u_3!} \right) \pmod{p}.$$

Let $p = 3$, $X^3 + aX + b \equiv 0 \pmod{3}$, $ab \not\equiv 0 \pmod{3}$.

All solutions of the system

$$\begin{gathered} 0 \le u_i < 2, \\ 3u_1 + u_2 \equiv 0 \pmod{2}, \\ u_1 + u_2 + u_3 = 2 \end{gathered}$$

are $(u_1, u_2, u_3) = (1, 1, 0)$, hence

$$N_3 \equiv 3 - \left(1 + \frac{ab^0}{1!1!0!} \right) \equiv 2 - a \pmod{3}.$$

Let $p = 11$, $X^3 + X + 1 \equiv 0 \pmod{11}$.

$$\begin{gathered} 0 \le u_i < 10, \\ 3u_1 + u_2 \equiv 0 \pmod{10}, \\ u_1 + u_2 + u_3 = 10. \end{gathered}$$

All solutions of this system are $(u_1, u_2, u_3) = (1, 7, 2); (2, 4, 4); (3, 1, 6); (5, 5, 0); (6, 2, 2)$.

Hence

$$N_{11} \equiv 3 - \left(1 + \frac{1}{1!7!2!} + \frac{1}{2!4!4!} + \frac{1}{3!1!6!} + \frac{1}{5!5!0!} + \frac{1}{6!2!2!}\right) \equiv 1 \pmod{11}.$$

E x a m p l e 2. In this example, we determine the number N_p of solutions of the congruence

$$X_1^3 + X_2^3 + 1 \equiv 0 \pmod{p}.$$

We have

$$A = \begin{pmatrix} 3,0 \\ 0,3 \\ 0,0 \end{pmatrix},$$

hence

$$\begin{aligned} 0 \le u_i < p-1, \\ 3u_1 \equiv 0 \pmod{p-1}, \\ 3u_2 \equiv 0 \pmod{p-1}, \\ u_1 + u_2 + u_3 = p-1. \end{aligned}$$

I. Let $p \equiv 2 \pmod 3$. Clearly, this system has no solution, hence

$$N_p \equiv 3(-1)^3 + (-1)^2 \equiv -2 \pmod{p}.$$

II. Let $p \equiv 1 \pmod 3$. Denote $k = \frac{p-1}{3}$. Therefore all the solutions are $(u_1, u_2, u_3) = (0, k, 2k); (0, 2k, k); (k, 0, 2k); (2k, 0, k); (2k, k, 0); (k, 2k, 0); (k, k, k)$.

Hence

$$N_p \equiv -3 + \left(1 + (-6) + \frac{1}{(k!)^3}\right) \equiv -8 + \frac{1}{(k!)^3} \pmod{p}.$$

Let $4p = a^2 + 27b^2$, $a \equiv 1 \pmod 3$. It can be proved (see [1]) that

$$\frac{1}{(k!)^3} \equiv a \pmod{p}.$$

Therefore

$$N_p \equiv a - 8 \pmod{p}.$$

REFERENCES

[1] JAKUBEC, J.: *The congruence for Gauss's period*, J. Number Theory (To appear).

Received January 11, 1994

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK-814 73 Bratislava
Slovakia
E-mail: jakubec@savba.sk