第15卷第4期 数学研究与评论 Vol. 15 No. 4
1995年11月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Nov. 1995

# 关于同余式 $\sum_{j=1}^{n} a_j x_j^{d_j} \equiv b \pmod{p^l}$ 的解的个数*

孙 琦
(四川大学数学研究所，成都 610064)

**摘 要** 设 $N_{p^l}(b)$ 代表同余式 $\sum_{j=1}^{n} a_j x_j^{d_j} \equiv b \pmod{p^l}$ 的解的个数，这里 $p$ 是一个奇素数，$p \nmid b a_1 \cdots a_n$，$d_j \mid p-1$，$d_j > 1$，$j = 1, \cdots, n$. 本文给出 $N_{p^l}(b)$ 一个渐近公式.

**关键词** 同余式，对角型，非奇异解.
**分类号** AMS(1991) 11D79, 11T99/CCL O156.7

设 $f(x_1, \cdots, x_n)$ 是一个整系数的 $n$ 元多项式，$m > 1$，$m = p_1^{l_1} \cdots p_k^{l_k}$ 是 $m$ 的标准分解式. 熟知，同余式 $f(x_1, \cdots, x_n) \equiv 0 \pmod{m}$ 的可解问题等价于 $k$ 个同余式

$$f(x_1, \cdots, x_n) \equiv 0 \pmod{p_j^{l_j}}, \quad j = 1, \cdots, k$$

的可解问题. 因此，设 $p$ 是一个素数，有关同余式

$$f(x_1, \cdots, x_n) \equiv 0 \pmod{p^l} \quad l \geqslant 1. \tag{1}$$

的解的个数的研究，是一个重要问题. 关于同余式(1)的解的个数问题，以往的研究大多是定性的. 例如，一个著名的经典结果是说：如果 $f(x_1, \cdots, x_n)$ 是绝对不可约多项式，即 $f(x_1, \cdots, x_n)$ 在有理数域的任一扩域中均不可约，则除开有限个素数 $p$ 外，对任给的 $l \geqslant 1$，(1)均有解[1].

Mordell[2]曾经证明同余式 $y^2 \equiv x^3 + b \pmod{p^l}$，$l \geqslant 1$ 除开 $p = 7$，$b \equiv 6 \pmod 7$ 外，均有 $p \nmid y$ 的解，此处 $p$ 是一个奇素数.

本文对下面更一般的对角形同余式

$$a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} \equiv b \pmod{p^l}, \quad l \geqslant 1, \tag{2}$$

给出了解的个数的渐近公式，这里 $d_i \mid p-1$，$d_i > 1$，$p \nmid b a_1 \cdots a_n$.

我们有下面的定理.

**定理** 设 $N_{p^l}(b)$ 表同余式(2)的解的个数，则有

$$|N_{p^l}(b) - p^{l(n-1)}| < \left(\prod_{j=1}^{n}(d_j - 1) - \left(1 - \frac{1}{\sqrt{p}}\right) I(d_1, \cdots, d_n)\right) p^{\frac{n-1}{2} + (n-1)(l-1)},$$

其中 $I(d_1, \cdots, d_n)$ 表示同余式

$$\frac{y_1}{d_1} + \cdots + \frac{y_n}{d_n} \equiv 0 \pmod 1, \quad 1 \leqslant y_j \leqslant d_j - 1, \ j = 1, \cdots, n$$

* 1992年11月24日收到. 国家自然科学基金资助项目

的解 $y_1,\cdots,y_n$ 的个数.

显然有

**推论 1** $|N_{p^l}(b)-p^{l(n-1)}|<\left(\prod_{j=1}^{n}(d_j-1)\right)p^{\frac{n-1}{2}+(n-1)(l-1)}$

**推论 2** 当 $p^{n-1}>\prod_{j=1}^{n}(d_j-1)^2$ 时，$N_{p^l}(b)>0$.

证明定理之前，先证一个引理.

**引理** 设 $p$ 是一个素数，同余式

$$f(x_1,\cdots,x_n)\equiv 0(\mathrm{mod}\,p) \tag{3}$$

的所有非奇异解的个数为 $N$，设为 $(a_{j_1},\cdots,a_{j_n})$，$j=1,\cdots,N$，则由此 $N$ 个解，可构造出同余式(1)的 $p^{(n-1)(l-1)}N$ 个解，且可将这些解分成 $N$ 组，每组含 $p^{(n-1)(l-1)}$ 个解恰与某个 $(a_{j_1},\cdots,a_{j_n})$ 模 $p$ 同余.

**证明** 设 $(a_1,\cdots,a_n)$ 是(3)的 $N$ 个非奇异解中的一个，我们用归纳法来证明由此解可构造出 $p^{(n-1)(l-1)}$ 个(1)的解，且与 $(a_1,\cdots,a_n)$ 模 $p$ 同余. 设结论对模 $p^u(u\geqslant 1)$ 成立，即由 $(a_1,\cdots,a_n)$ 可构造出同余式

$$f(x_1,\cdots,x_n)\equiv 0(\mathrm{mod}\,p^u) \tag{4}$$

的 $p^{(n-1)(n-1)}$ 个解，且均与 $(a_1,\cdots,a_n)$ 模 $p$ 同余. 我们来证明，结论对同余式

$$f(x_1,\cdots,x_n)\equiv 0(\mathrm{mod}\,p^{u+1}) \tag{5}$$

也成立. 设 $(b_1,\cdots,b_n)$ 为(4)的上述 $p^{(n-1)(n-1)}$ 个解中的一个，则有 $f(b_1,\cdots,b_n)=p^u f$，$f$ 是一个整数. 考虑同余式

$$f(b_1+p^u s_1,\cdots,b_n+p^u s_n)\equiv 0(\mathrm{mod}\,p^{u+1}),\quad 0\leqslant s_j\leqslant p-1,\ j=1,\cdots,n. \tag{6}$$

由于 $2u\geqslant u+1$，

$$f(b_1+p^u s_1,\cdots,b_n+p^u s_n)\equiv f(b_1,\cdots,b_n)+p^u\sum_{j=1}^{n}\frac{\partial f}{\partial j}(b_1,\cdots,b_n)s_j(\mathrm{mod}\,p^{u+1}),$$

故(6)等价于同余式

$$f(b_1,\cdots,b_n)+p^u\sum_{j=1}^{n}\frac{\partial f}{\partial j}(b_1,\cdots,b_n)s_j\equiv 0(\mathrm{mod}\,p^{u+1}),$$

注意到 $f(b_1,\cdots,b_n)=p^u f$，即得

$$f+\sum_{j=1}^{n}\frac{\partial f}{\partial j}(b_1,\cdots,b_n)s_j\equiv 0(\mathrm{mod}\,p). \tag{7}$$

因为 $b_j\equiv a_j(\mathrm{mod}\,p)$，$(b_1,\cdots,b_n)$ 是(3)的一个非奇异解，故至少存在一个 $j$，$1\leqslant j\leqslant n$，使 $\frac{\partial f}{\partial j}(b_1,\cdots,b_n)\not\equiv 0(\mathrm{mod}\,p)$，故(7)有 $p^{n-1}$ 个解. 即(6)有 $p^{n-1}$ 个解. 由归纳假设，(4)有 $p^{(n-1)(n-1)}$ 个解(均与 $(a_1,\cdots,a_n)$ 模 $p$ 同余)，故可构造出(5)的 $p^{(n-1)(n-1)}p^{n-1}=p^{(n-1)n}$ 个解，显然其中每一个解均与 $(a_1,\cdots,a_n)$ 同余. 这样，我们也就证明了，同余式(3)的 $N$ 个非奇异解 $(a_{j_1},\cdots,a_{j_n})$，$j=1,\cdots,N$，可构造出同余式(1)的 $p^{(n-1)(l-1)}N$ 个解，且可将这些解分成 $N$ 个组，每组含 $p^{(n-1)(l-1)}$ 个解恰与某个 $(a_{j_1},\cdots,a_{j_n})$ 模 $p$ 同余. 证毕.

**定理的证明** 设 $f(x_1,\cdots,x_n)=ax_1^{d_1}+\cdots+a_nx_n^{d_n}-b$，熟知[3]，

$$f(x_1,\cdots,x_n)\equiv 0(\mathrm{mod}\,p) \tag{8}$$

的解的个数 $N_p(b)$ 满足

$$|N_p(b) - p^{n-1}| < (\prod_{j=1}^{n}(d_j - 1) - (1 - \frac{1}{\sqrt{p}})I(d_1,\cdots,d_n))p^{\frac{n-1}{2}}. \tag{9}$$

由于 $\frac{\partial}{\partial x_j}f(x_1,\cdots,x_n) = a_j d_j x_j^{d_j-1}$, $j=1,\cdots,n$, $p \nmid a_1\cdots a_n d_1\cdots d_n$, 且 $(0,\cdots,0)$ 不是(8)的解, 故(8)的 $N_p(b)$ 个解都是非奇异的. 由引理知, 此 $N_p(b)$ 个解可构造出(2)的 $p^{(n-1)(l-1)}N_p(b)$ 个解. 由于(2)的任一解 $(c_1,\cdots,c_n)$ 也是(8)的解, 同时也是同余式

$$a_1x_1^{d_1} + \cdots + a_nx_n^{d_n} - b \equiv 0 (\mathrm{mod}\, p^{l-1}) \tag{10}$$

的解, 故可设 $c_j \equiv a_j (\mathrm{mod}\, p)$, $c_j \equiv b_j (\mathrm{mod}\, p^{l-1})$, $j=1,\cdots,n$, 这里 $(a_1,\cdots,a_n)$ 和 $(b_1,\cdots,b_n)$ 分别是(8)和(10)的某一解. 可设 $c_j = b_j + p^{l-1}s_j$, $0 \leqslant s_j \leqslant p-1$, 如引理的证明过程所表明, $(c_1,\cdots,c_n)$ 可通过 $(a_1,\cdots,a_n)$ 构造出来, 这就证明了 $N_{p^l}(b) = p^{(n-1)(l-1)}N_p(b)$. 再由(9)的两端乘以 $p^{(n-1)(l-1)}$, 即得定理. □

由于 $I(d_1,\cdots,d_n) \leqslant \prod_{j=1}^{n}(d_j - 1)$, 由定理, 推论 1 即可得出.

由推论 1 可得

$$N_{p^l}(b) > p^{l(n-1)} - \prod_{j=1}^{n}(d_j - 1)p^{\frac{n-1}{2}+(n-1)(l-1)} = p^{\frac{n-1}{2}+(n-1)(l-1)}(p^{\frac{n-1}{2}} - \prod_{j=1}^{n}(d_j - 1)).$$

立得推论 2.

## 参 考 文 献


[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[2] J. L. Mordell, *The Diophantine Equations*, Academic Press, 1969.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclo. Math. and Appls. V. 20, Addison-Wesley, Reading, 1983.


# On Number of Solutions of Congruence $\sum_{j=1}^{n} a_j x_j^{d_j} \equiv b \pmod{p^l}$


*Sun Qi*

(Dept. of Math., Sichuan Univ., Chengdu 610064)



### Abstract

Let $N_{p^l}(b)$ be the number of solutions of congruence $\sum_{j=1}^{n} a_j x_j^{d_j} \equiv b \pmod{p^l}$, where $p$ is an odd prime, $p \nmid ba_1,\cdots,a_n, d_j | p-1. d_j > 1, j = 1,\cdots,n$. In this note, we give an estimate for $N_{p^l}(b)$.



**Keywords** congruences, diagonal form, nonsingular solutions.