Mathematical Subject Classification: 11N25, 11S40
UDC 511.33

L. Balyas
I. I. Mechnikov Odessa National University

THE DISTRIBUTION OF THE SOLUTIONS OF THE CONGRUENCES OF SPECIAL FORM MODULO p^n

Баляс Л. Розподілення розв'язків конгруенцій спеціального типу за модулем p^n. Ми отримуємо нетривіальну асимптотичну формулу для числа розв'язків конгруенції $ax^3 + by^4 \equiv c \pmod{p^n}$.
Ключові слова: тригонометрична сума, асимптотична формула, розв'язок порівняння.

Баляс Л. Распределение решений сравнений специального вида по модулю p^n. Мы получаем нетривиальную асимптотическую формулу для числа решений сравнения $ax^3 + by^4 \equiv c \pmod{p^n}$.
Ключевые слова: тригонометрическая сумма, асимптотическая формула, решение сравнения.

Balyas L. The distribution of the solutions of the congruences of special form modulo p^n. We obtain nontrivial asymptotic formula for the number of the solutions of the congruence $ax^3 + by^4 \equiv c \pmod{p^n}$
Key words: exponential sum, asymptotic formula, solution of the congruence.

Introduction. In 1918 I. M. Vinogradov and G. Polya nearly at the same time got the non-trivial estimate for the number of quadratic residue classes prime modulo in the interval $[1, x]$, where $x < p$. It was the first problem on the distribution of solutions of the congruence $f(x, y) \equiv 0 \pmod{p^n}$, where $f(x, y)$ is a polynomial with coefficients from the field $\mathbb{Z}_p$. Nowadays the problem on the incomplete residue system is defined in the following manner.

Let $f(x_1, \cdots, x_n)$ be a polynomial with integer coefficients and let $\mathbb{Z}_q$ be a residue class ring modulo q, where $q \in \mathbb{N}\setminus\{1\}$; let $A_q(a_1, b_1, \cdots, a_n, b_n)$ be the number of solutions of the congruence

$$f(x_1, \cdots, x_n) \equiv 0 \pmod{q}, \; (x_1, \cdots, x_n) \in R, \tag{1.1}$$

where

$$R := \left\{ \begin{array}{l} a_i \leq x_i < a_i + b_i, \; i = \overline{1, n}, \\ 0 \leq a_i < a_i + b_i < q, \\ a_i, b_i \in \mathbb{N} \bigcup \{0\}, \; i = \overline{1, n} \end{array} \right\}. \tag{1.2}$$

The purpose of our work is the derivation of the asymptotic formula for the congruence of special form with the use of the solutions of proper congruences modulo p^n, where p is prime and $n \in \mathbb{N}\setminus\{1\}$.

Notation. Latin letter p (with an index or without one) is always the notation of a prime number.

$\mathbb{Z}_p$ – residue class field prime modulo p.
$\mathbb{Z}_q$ – residue class ring modulo q.
"$\ll$", "O" – Landau and Vinogradov symbols respectively.
$(a_1, \ldots, a_k)$ – greatest common divisor of $a_1, \ldots, a_k \in \mathbb{Z}$.
$\nu_p(a)$ – index of power, with which a prime number p is included in canonical decomposition of $a \in \mathbb{Z}$. If $(a,p)=1$, then $\nu_p(a)=0$.

Auxiliary arguments. The purpose of our work is the derivation of the asymptotic formula for congruence analogously to Postnikova work [2].

$$ax^3 + by^4 \equiv c \pmod{p^n}, \tag{2.1}$$

where $p \geq 5$, $(a,b,c,p)=1$.

The congruence (2.1) is equivalent to the congruence

$$y^4 \equiv c - ax^3 \pmod{p^n}. \tag{2.2}$$

Let (x_0, y_0) be an arbitrary solution of the congruence

$$y^4 \equiv c - ax^3 \pmod{p}. \tag{2.3}$$

If there is no such solution, our initial congruence has no solutions at all.

Firstly one can concede that $x_0 \not\equiv 0 \pmod{p}$. For every t, $t = \overline{0, p^{n-1}}$ we set $A(t) \equiv c - a(x_0 + pt)^3 \pmod{p^n}$.

Let the congruence

$$y^4 \equiv c - ax_0^3 \pmod{p}, \tag{2.4}$$

have κ, $\kappa \geq 1$ solutions. From elementary theory of numbers we have that the congruence

$$y^4 \equiv A(t) \pmod{p^n}, \tag{2.5}$$

also has κ, $\kappa \geq 1$ solutions for every t.

Let us denote $y_1(t), \ldots, y_\kappa(t)$ as all the solutions of the congruence (2.5). Furthermore, we have κ solutions $y_1(0), \ldots, y_\kappa(0)$ in the case, when $t=0$. Let $y(0)$ be one of these solutions.

Lemma 1. *2.1 Let* $s = \left[\frac{p-1}{p-2}\left(n + \nu_p(a)\right)\right]$. *Then there exists the polynomial* $f(t)$, $\deg f(t) = s$

$$f(t) = \Phi_0(x_0) + p^{\lambda_1}\Phi_1(x_0)t + \cdots + p^{\lambda_s}\Phi_s(x_0)t^s,$$

such that

$$y_i(t) \equiv y_i(0) f(t) \pmod{p^n}, \ i = 1, \ldots, \kappa.$$

Moreover, all the coefficients $\Phi_j(x_0) \in \mathbb{Z}$, $\lambda_j \in \mathbb{N} \cup \{0\}$, $j = \overline{0,s}$, $\lambda_0 = 0$, $\lambda_j \geq j\frac{p-2}{p-1}$, $j = \overline{1,s}$.

Proof. From $(y_0, p) = 1$ we obtain that the congruence $(c - ax_0^3)x \equiv 1 \pmod{p^n}$ has the unique solution. Let us denote it as x_0'.

We shall suppose, that $0 \leq x_0 \leq p-1$, $1 \leq x_0' \leq p^{n-1}$. We consider the expansion in series of the function

$$U(w) = \left(1 - 3awx_0^2x_0' - 3ax_0x_0'w^2 - ax_0'w^3\right)^{\frac{1}{4}}$$

in powers of w:

$$U(w) = \sum_{j=0}^{\infty} X_j w^j.$$

We equate the two expressions for the derivative of the function (using the written above equations) and easily get:

$$\sum_{j=1}^{\infty} jX_j w^{j-1}(1 - 3awx_0^2 x_0^{'} - 3ax_0 x_0^{'} w^2 - ax_0^{'} w^3) =$$
$$= -\frac{1}{4}\sum_{j=0}^{\infty} X_j w^j (3ax_0^2 x_0^{'} + 6ax_0 x_0^{'} w + 3ax_0^{'} w^2).$$

After this we equate the coefficients at equal powers of w and get the recurrence relation:

$$(j+1)X_{j+1} = \frac{9j}{4} ax_0^2 x_0^{'} X_j + \frac{3(j-1)}{2} ax_0 x_0^{'} X_{j-1} + \frac{j-2}{4} ax_0^{'} X_{j-2}. \tag{2.6}$$

We should notice that X_0, X_1, X_2 can be directly defined:

$$X_0 = 1,\ X_1 = -\frac{3ax_0^2 x_0^{'}}{4},\ X_2 = -\frac{3ax_0 x_0^{'}}{4} - \frac{3}{32} a^2 x_0^4 x_0^{'2}.$$

Let us consider the following polynomial

$$U_s(w) = \sum_{j=0}^{s} X_j w^j,$$

in which a value of s will be defined later. Now in view of this formula we shall consider the following equations:

$$U_s^4(w) - B(w)^4 = (U_s(w) - B(w))\,(U_s(w) + B(w))\left(U_s^2(w) - B(w)^2\right) \tag{2.7}$$

where $B(w) = \left(1 - 3awx_0^2 x_0^{'} - 3ax_0 x_0^{'} w^2 - ax_0^{'} w^3\right)^{\frac{1}{4}}$.

From the expansion in series of $B(w)$ we obtain that the coefficients at powers of w in the expansion in series at the left of (2.7) go to zero, when $j = \overline{0, s}$. Since the coefficients $X_j \in \mathbb{Q}$, the coefficients of $U_s(pt)$ are rational numbers too.

But we have

$$U_s(pt) = \sum_{j=0}^{s} X_j p^j t^j.$$

Let us denote

$$X_j p^j = p^{\lambda_j} \frac{c_j}{d_j},\ (c_j, p) = (d_j, p) = 1. \tag{2.8}$$

From formula (2.6) we can see that the denominators at $j = 2, 3, \ldots$ in formula

$$X_{j+1} = \frac{9j}{4(j+1)} ax_0^2 x_0^{'} X_j + \frac{3(j-1)}{2(j+1)} ax_0 x_0^{'} X_{j-1} + \frac{j-2}{4(j+1)} ax_0^{'} X_{j-2}$$

are the divisors of $2^{2j}j!$.

From the formula for an index of power, with which a prime number p is included in canonical decomposition into factors, we have

$$\nu_p\left(X_j p^j\right) \geq j - \frac{j}{p-1} + \nu_p(a) = j\frac{p-2}{p-1} + \nu_p(a) \tag{2.9}$$

Let us consider the series $U(w)$ over the field of p-adic numbers $\mathbb{Q}_p$. Then from the result that has been received before we get, that for every $w \in \mathbb{Q}_p$, $\|w\|_p < 1$ the series converges and, furthermore, for $w = pt$, $t \in \mathbb{Z}$ we have:

$$U(pt) = U_s(pt) \pmod{p^n}, \; if\ s = \left[\frac{p-1}{p-2}\left(n + \nu_p(a)\right)\right].$$

We shall define e_j from the congruence $e_j d_j \equiv c_j \pmod{p^n}$ and put

$$f(t) = \sum_{j=0}^{s} e_j p^{\lambda_j} t^j.$$

We know that X_j depend on x_0. That is why we shall write that

$$e_j = \Phi_j(x_0), \; j = \overline{0, s}.$$

Thus, we established the assertion of lemma. □

Lemma 2. *2.2 Let $p \geq 5$ be a prime number. With the notations of Lemma 2.1 for $j = 3, 4, \ldots, s$ we have:*

$$\min\left(\lambda_j, \lambda_{j-1}, \lambda_{j-2}\right) \leq j + 7 + \frac{5j-7}{p-1}.$$

Proof. Let us consider for every $j = \overline{1, s}$ the following values X_j, Y_j, Z_j, which are defined by the relations:

$$\begin{aligned}
&X_0 = 1, \; X_1 = -\frac{3ax_0^2 x_0^{'}}{4}, \; X_2 = -\frac{3ax_0 x_0^{'}}{4} - \frac{3}{32}a^2 x_0^4 x_0^{'2}, \\
&Y_0 = 0, \; Y_1 = 1, \; Y_2 = -\frac{3ax_0^2 x_0^{'}}{4}, \\
&Z_0 = 0, \; Z_1 = 0, \; Z_2 = 1,
\end{aligned}$$

and for $j = 3, 4, \ldots, s$, X_j, Y_j and Z_j satisfy the recurrence relation (2.6).

We shall consider the determinants

$$\Delta_j = \begin{vmatrix} X_{j-2} & X_{j-1} & X_j \\ Y_{j-2} & Y_{j-1} & Y_j \\ Z_{j-2} & Z_{j-1} & Z_j \end{vmatrix}, \; j = 3, 4, \ldots, s.$$

In particular,$\Delta_3 = -\frac{3ax_0^2 x_0^{'}}{4}$.

From now on we consider appearing fractions modulo p^n.

We know that $\left(x_0^{'}, p\right) = 1$. But then $\nu_p(\Delta_3) = \nu_p(a)$. Furthermore, for $j \geq 4$ we easily get

$$\Delta_j = \frac{j-3}{4j} a x_0^{'} \Delta_{j-1} = (a x_0^{'})^{j-3} \frac{1}{j(j-1)(j-2)} \Delta_3. \tag{2.10}$$

Let us denote

$$\nu_p\left(X_j p^j\right) = \nu_p(\lambda_j),\ \nu_p\left(Y_j p^j\right) = \nu_p(\mu_j),\ \nu_p\left(Z_j p^j\right) = \nu_p(\tau_j).$$

It is clear that $\mu_j = \lambda_{j-1}$, $\tau_j = \lambda_{j-2}$. And from formula (2.10) we obtain

$$j(j-1)(j-2) \begin{vmatrix} X_{j-2}p^{j-2} & X_{j-1}p^{j-1} & X_j p^j \\ Y_{j-2}p^{j-2} & Y_{j-1}p^{j-1} & Y_j p^j \\ Z_{j-2}p^{j-2} & Z_{j-1}p^{j-1} & Z_j p^j \end{vmatrix} = \left(a x_0^{'}\right)^{j-3} \Delta_3 p^{3j-3}.$$

We factor out from the rows of the determinant

$$p^{\min(\lambda_j, \lambda_{j-1}, \lambda_{j-2})},\ p^{\min(\mu_j, \mu_{j-1}, \mu_{j-2})},\ p^{\min(\tau_j, \tau_{j-1}, \tau_{j-2})}$$

and come to conclusion:

$$\min(\lambda_j, \lambda_{j-1}, \lambda_{j-2}) + \min(\mu_j, \mu_{j-1}, \mu_{j-2}) + \min(\tau_j, \tau_{j-1}, \tau_{j-2}) \leq 3j - 3.$$

But we already know that

$$\mu_j, \mu_{j-1}, \mu_{j-2} \geq (j-3)\frac{p-2}{p-1} + \nu_p(a),$$

$$\tau_j, \tau_{j-1}, \tau_{j-2} \geq (j-4)\frac{p-2}{p-1} + \nu_p(a).$$

That is why we obtain:

$$\min(\lambda_j, \lambda_{j-1}, \lambda_{j-2}) \leq 3j + (2j-7)\,\frac{p-2}{p-1} + (j-6)\nu_p(a).$$

When $\nu_p(a) = 0$, the result takes the form:

$$\min(\lambda_j, \lambda_{j-1}, \lambda_{j-2}) \leq j + 7 + \frac{5j-7}{p-1}.$$

□

Now we consider the case, when $x_0 \equiv 0 \pmod{p}$. If the congruence $y^4 \equiv c \pmod{p}$ has no solutions, the congruence (2.5) has no solutions (x, y) under the condition $x \equiv 0 \pmod{p}$.

That is why we suggest that our congruence has a solution. Let $y_1, \ldots, y_k$ be all its solutions. A solution of the congruence (2.5) we search in the form $x = pt$, $y_j = y_j(t)$, $j = \overline{1, k}$, where

$$y_j(t) \equiv y_j(0)\left(1 + p^3 a_1 t^3 + p^{\lambda_2} a_2 t^6 + \cdots + a_r p^{\lambda_r} t^{3r}\right),\ t = \overline{0, p^{n-1}}.$$

Moreover, $r \leq \left[\frac{n-1}{3}\right]$ and

$$\lambda_j \geq 4,\ j = 2, \ldots, r,\ (a_i, p) = 1,\ i = 1, \ldots, r.$$

Main Results. Let $A(T_1, T_2)$ be the number of solutions of the congruence (2.2), which belong to the rectangle $R = \{0 \leq x \leq T_1,\ 0 \leq y \leq T_2\}$. Then let $A(T_1, T_2)$ be the number of pairs of fractional portions $\left\{\frac{x}{p^n}, \frac{y}{p^n}\right\}$, that have got into the rectangle $\left\{0 \leq u \leq \frac{T_1}{p^n},\ 0 \leq v \leq \frac{T_2}{p^n}\right\}$, when a pair (x, y) range over the set of the solutions of the congruence (2.2).

Let $\chi(v)$ be the characteristic function of the interval $\left[0, \frac{T_2}{p^n}\right]$. Using the description of the solutions of the congruence (2.2), we can write

$$A(T_1, T_2) = \sum_{i=1}^{\kappa} \sum_{x_0}^{*} \sum_{0 \leq t < \frac{T_1}{p}} X\left(\frac{y_i(t)}{p^n}\right) + \sum_{i=1}^{\kappa} \sum_{0 \leq t < \frac{T_1}{p}} X\left(\frac{y_i(t)}{p^n}\right) = \sum\nolimits_1 + \sum\nolimits_2,$$

where the sign "$*$" means the summation over such $x_0 \in \mathbb{Z}_p$, that $x_0 \neq 0$ and the congruence $y^4 \equiv c - ax_0^3 \pmod{p}$ has solutions (it has κ, $\kappa \geq 1$ solutions $y_0 \in \mathbb{Z}_p$).

Furthermore, $y_i(t)$ runs all the solutions of the congruence (2.5) in the first sum and the congruence $y^4 \equiv c - a(pt)^3 \pmod{p^n}$ $(2.5)'$ for the second sum respectively.

We shall extend the characteristic function $\chi_{\alpha,\beta}(u)$ of the interval $[\alpha, \beta]$, $0 < \beta + \alpha \leq 1$ periodically with period 1 to the whole real axis. We need the following assertion.

Lemma 3. *(Vinogradov's "glasses", see [1]) Let $0 < \Delta < \frac{1}{2}$, $\Delta \leq \beta - \alpha \leq 1 - \Delta$. Then for every natural r there exists the periodical function with period 1 $\varphi(u)$ such, that:*

$$\varphi(u) = 1, \qquad if \quad \alpha + \Delta \leq u \leq \beta - \Delta;$$

$$\varphi(u) = 0, \qquad if \quad 0 \leq u \leq \alpha + \Delta \ or \ \beta + \Delta \leq u < 1;$$

$$0 \leq \varphi(u) \leq 1, \quad if \quad \alpha - \Delta \leq u \leq \alpha + \Delta \ or \ \beta - \Delta \leq u \leq \beta + \Delta,$$

and the function is monotone in each of these intervals.

Moreover, the function $\varphi(u)$, has the expansion in a Fourier series

$$\varphi(x) = \beta - \alpha + \sum_{\substack{m=-\infty \\ m \neq 0}}^{m=+\infty} a_m e^{2\pi i m u},$$

where $|a_m| \leq \min\left(\frac{1}{|m|}, \beta - \alpha, \frac{1}{|m|}\left(\frac{r}{\pi |m|}\right)^r\right)$.

Furthermore, we need the theorem of Vinogradov on the estimate of the exponential sum.

Theorem 1. *Let $f(x) = a_1 x + a_2 x^2 + \cdots + a_{n+1} x^{n+1}$ be a polynomial with real coefficients. Moreover, $a_r = \frac{a}{q} + \frac{\theta}{q^2}$, $(a, q) = 1$, $1 < q < r$ for some $r \in \{2, 3, \ldots, n+1\}$. Let us define τ from the condition:*

1. *$q = P^\tau$, $1 < q \leq P$;*
2. *$\tau = 1$, $P < q < P^{r-1}$;*

3. $q = P^{r-\tau}$, $P^{r-1} < q < P^r$.

Then

$$\left|\sum_{x=1}^{P} e^{2\pi i m f(x)}\right| < (8n)^{\frac{nl}{2}}\, m^{\frac{2\rho}{\tau}} P^{1-r},$$

where $m \in \mathbb{N}$, $l = \log\frac{12n(n+1)}{\tau}$, $\rho = \frac{\tau}{3n^2 l}$.

Theorem 2. *3.1 Let* $p \geq 5$ *be a prime number and* $1 < T_2 \leq p^n$, $p^{\frac{5n+43}{9}} \leq T_1 \leq p^n$, $n \geq 13$. *Then for the number of the solutions* $A(T_1, T_2)$ *of the congruence (2.2) (with the condition* $(a,p) = 1$*), for which the following asymptotic formula is true:*

$$a\left(T_1, T_2\right) = \frac{T_1 T_2}{p^n} \cdot \frac{N(a,c;p)}{p} + O\left(T_1^{1-\frac{1}{28n^3 \log 27n^3}} e^{7n(\log n)^2}\right), \tag{3.1}$$

where $N(a,c;p)$ *is the number of the solutions of the congruence* $y^4 \equiv c - ax^3 \pmod p$.

Proof. From the equation (3.1) it follows, that it is sufficient to us to calculate the inner sums in the sums $\sum_1$ and $\sum_2$. Let us calculate the inner sum in the first sum. From the description of $y(t)$ (see Lemma 2.1) we obtain:

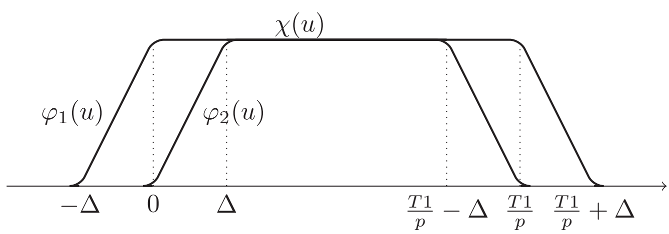
$$\sum_{t_1 < \frac{T_1}{p}} \chi\left(\frac{y(t)}{p^n}\right) = \sum_{t_1 < \frac{T_1}{p}} \chi\left(\frac{\Phi_0(x_0) + p^{\lambda_1}\Phi_1(x_0)t + \cdots + p^{\lambda_s}\Phi_s(x_0)t^s}{p^n}\right),$$

where $s = \left[\frac{p-1}{p-2}\left(n + \nu_p(a)\right)\right]$.

We shall consider the most important case, when $\nu_p(a) = 0$, because the general case may be resolved to the case $\nu_p(a) = 0$. We choose $0 < \Delta \leq \frac{T_1}{2p}$ (we shall define its value more precisely later). Let $\varphi_1(u)$ be the function from the Vinogradov lemma about "glasses" for $\alpha = -\Delta$, $\beta = \frac{T_2}{p^n} + \Delta$ and let $\varphi_2(u)$ be the function for $\alpha = \Delta$, $\beta = \frac{T_2}{p^n} - \Delta$. We can see from Picture 1, that for every $u \in \mathbb{R}$ the inequality $\varphi_1(u) \leq \chi(u) \leq \varphi_2(u)$ takes place and that is why

$$\sum_{u \in [0,1)} \chi(u) = \sum_{u \in [0,1)} \varphi_1(u) + O\left(\Delta\right) = \sum_{u \in [0,1)} \varphi_2(u) + O\left(\Delta\right). \tag{3.2}$$

From the lemma about "glasses" we have



$$\sum_{t_1<\frac{T_1}{p}} \chi\left(\frac{\Phi_0(x_0)+p^{\lambda_1}\Phi_1(x_0)t+\cdots+p^{\lambda_s}\Phi_s(x_0)t^s}{p^n}\right)=$$
$$=\sum_{t_1<\frac{T_1}{p}} \varphi_1\left(\frac{\Phi_0(x_0)+p^{\lambda_1}\Phi_1(x_0)t+\cdots+p^{\lambda_s}\Phi_s(x_0)t^s}{p^n}\right)+O(\Delta)= \tag{3.3}$$
$$=\frac{T_1T_2}{p^{n+1}}+O\left(\frac{T_1\Delta}{p}\right)+\sum_{m=1}^{\infty}|a_m|\cdot\sum_{t_1<\frac{T_1}{p}} e^{2\pi i\frac{y_i(0)\left(p^{\lambda_1}\Phi_1(x_0)t+\cdots\right)}{p^n}}+O(\Delta).$$

Let us define the largest value of j, for which by Lemma 2 the following condition takes place:

$$\min(\lambda_j,\lambda_{j-1},\lambda_{j-2})\le j+7+\frac{5j-7}{p-1}\le j+7+\frac{5j-7}{4}\le(n-1). \tag{3.4}$$

Thus, we get that $j=\left[\frac{4n-25}{9}\right]$.

Now with the help of Vinogradov theorem we shall get the estimate for the inner sum with respect to t in the formula (3.3) on such index of $\left[\frac{4n-25}{9}\right]$ or $\left[\frac{4n-25}{9}\right]-1$, for which $\lambda_j\le n-1$. Thus, we have $\frac{4n-34}{9}\le\lambda_j$. From $(y_i(0),p)=1$, $(\Phi_j(x_0),p)=1$ we get, that the coefficient at t^j has the form of the irreducible fraction $\frac{y_i(0)\Phi_j(x_0)}{p^{n-\lambda_j}}$ and $1\le n-\lambda_j\le\frac{5n+34}{9}$.

By our suggestion $p^{\frac{5n+34}{9}}\le T_1\le p^n$, and that is why we have, that $p^{n-1}\ge\frac{T_1}{p}\ge p^{\frac{5n+34}{9}}$. In terms of Vinogradov theorem $P=\frac{T_1}{p}$, and this means, that we have come to the first case of the theorem. Let us put $p^{n-\lambda_j}=P^\tau$. That is why $P^\tau\le P$, $\tau\le1$. On the other side we have $n-\lambda_j\le1$, $p\le P^\tau$, $p\le p^{(n-1)\tau}$. We have the estimate $\frac{1}{n-1}\le\tau\le1$.

Let us put $l=\log\frac{12(s-1)s}{\tau}$. By virtue of the fact, that $s\ge n$, $\tau<1$, $s\le\frac{3}{2}n$, we have that $\log 12(n-1)n\le l\le\log 27n^2(n-1)$.

Let us denote more

$$\rho=\frac{\tau}{3(s-1)^2l},\ \frac{1}{7n^3\log 27n^2}\le\rho\le\frac{1}{3(n-1)^2\log 12(n-1)n}.$$

And then Vinogradov theorem gives the following result:

$$\left|\sum_{t_1<\frac{T_1}{p}} e^{2\pi i m\frac{y_i(0)\left(p^{\lambda_1}\Phi_1(x_0)t+\cdots+p^{\lambda_s}\Phi_s(x_0)t^s\right)}{p^n}}\right|\le$$
$$\le(12n)^{\frac{3}{4}n\log 27n^2(n-1)}m^{\frac{1}{3(n-1)^2\log 12(n-1)n}}\left(\frac{T_1}{p}\right)^{1-\frac{1}{7n^3\log 27n^3}}.$$

We divide the sum over m into two parts: $m\le\frac{1}{\Delta}$ and $m>\frac{1}{\Delta}$. We use the estimate $|a_m|\le\frac{1}{|m|}$ for the first sum and the estimate $|a_m|\le\frac{1}{|m|}\left(\frac{2}{\pi|m|\Delta}\right)^2$ for the second sum.

And then, using Abel lemma on partial summation, choosing

$$\Delta = \left(\frac{T_1}{p}\right)^{-\frac{1}{7n^3\log 27n^3}}$$

and taking account of the condition $n \geq 13$, we obtain:

$$\sum\nolimits_1 = \sum_{i=1}^{\kappa}\sum_{x_0}{}^{*} \sum_{t<\frac{T_1}{p}} \chi\left(\frac{y_i(t)}{p^n}\right) =$$

$$= \sum_{i=1}^{\kappa}\sum_{x_0}\left(\frac{T_1T_2}{p^{n+1}} + O\left(\left(\frac{T_1}{p}\right)^{1-\frac{1}{14n^3\log 27n^3}} e^{7n\log^2 n}\right)\right).$$

We do the same things for the second sum and obtain the similar result. And after that we get the asymptotic formula (3.1). □

Remark 1. *One can consider the congruence* $x^m + y^3 \equiv 1 \pmod{p^n}$ *on the condition, that* $(m, p) = 1$, $p \geq 5$ *and get similar results.*

Conclusion. Nontrivial asymptotic formula for the number of the solutions of the congruence $ax^3 + by^4 \equiv c \pmod{p^n}$ was obtained.

1. **Vinogradov I.M.** Osnovy teorii chisel / Vinogradov I.M. – M.;L.: Gostehizdat, 1952. — 180 p. (in russian)

2. **Postnikova L. P.** Raspredelenie reshenij sravneniya $x^2 + y^2 \equiv 1 \pmod{p^n}$ / Postnikova L. P. // Matematicheskij sbornik. – 1964. – 65 (2). – P. 228-238 (in russian).