Journal of Number Theory 187 (2018) 41–65

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

# Counting the solutions of $\lambda_1 x_1^{k_1} + \cdots + \lambda_t x_t^{k_t} \equiv c \bmod n$

Songsong Li, Yi Ouyang [*]

*Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, China*

ARTICLE INFO

*Article history:*
Received 27 June 2017
Received in revised form 1 October 2017
Accepted 26 October 2017
Available online 16 November 2017
Communicated by L. Smajlovic

*MSC:*
primary 11B13, 11L03, 11L05

*Keywords:*
Congruence equation
Decomposition and lifting of residue classes
Squares of units
Powers of units

ABSTRACT

Given a polynomial $Q(x_1, \cdots, x_t) = \lambda_1 x_1^{k_1} + \cdots + \lambda_t x_t^{k_t}$, for every $c \in \mathbb{Z}$ and $n \geq 2$, we study the number of solutions $N_J(Q; c, n)$ of the congruence equation $Q(x_1, \cdots, x_t) \equiv c \bmod n$ in $(\mathbb{Z}/n\mathbb{Z})^t$ such that $x_i \in (\mathbb{Z}/n\mathbb{Z})^\times$ for $i \in J \subseteq I = \{1, \cdots, t\}$. We deduce formulas and an algorithm to study $N_J(Q; c, p^a)$ for $p$ any prime number and $a \geq 1$ any integer. As consequences of our main results, we completely solve: the counting problem of $Q(x_i) = \sum\limits_{i \in I} \lambda_i x_i$ for any prime $p$ and any subset $J$ of $I$; the counting problem of $Q(x_i) = \sum\limits_{i \in I} \lambda_i x_i^2$ in the case $t = 2$ for any $p$ and $J$, and the case $t$ general for any $p$ and $J$ satisfying $\min\{v_p(\lambda_i) \mid i \in I\} = \min\{v_p(\lambda_i) \mid i \in J\}$; the counting problem of $Q(x_i) = \sum\limits_{i \in I} \lambda_i x_i^k$ in the case $t = 2$ for any $p \nmid k$ and any $J$, and in the case $t$ general for any $p \nmid k$ and $J$ satisfying $\min\{v_p(\lambda_i) \mid i \in I\} = \min\{v_p(\lambda_i) \mid i \in J\}$.

[*] Corresponding author.
*E-mail addresses:* songsli@mail.ustc.edu.cn (S. Li), yiouyang@ustc.edu.cn (Y. Ouyang).

https://doi.org/10.1016/j.jnt.2017.10.017
0022-314X/© 2017 Elsevier Inc. All rights reserved.

## 1. Introduction and main results

### 1.1. Introduction

Given a polynomial

$$Q(x_1, \cdots, x_t) = \lambda_1 x_1^{k_1} + \cdots + \lambda_t x_t^{k_t} \in \mathbb{Z}[x_1, \cdots, x_t].$$

Let $\boldsymbol{\lambda} = (\lambda_1, \cdots, \lambda_t) \in (\mathbb{Z} - \{0\})^t$ and $\mathbf{k} = (k_1, \cdots, k_t) \in \mathbb{Z}_{\geq 1}^t$. For any $c \in \mathbb{Z}$ and $n \geq 2$, and for a subset $J$ of $I = \{1, \cdots, t\}$, denote by $\Gamma_J(c, n) = \Gamma_J(Q; c, n) = \Gamma_J(\boldsymbol{\lambda}, \mathbf{k}; c, n)$ the set of solutions $(x_1, \cdots, x_t)$ of the congruence equation

$$Q(x_1, \cdots, x_t) \equiv c \bmod n$$

such that $x_j \in (\mathbb{Z}/n\mathbb{Z})^\times$ for $j \in J$, and by $N_J(Q; c, n)$ the cardinality of $\Gamma_J(Q; c, n)$. In particular, write $\Gamma$, $N$, $\Gamma^*$ and $N^*$ for $\Gamma_\emptyset$, $N_\emptyset$, $\Gamma_I$ and $N_I$ respectively. The problem to determine $N_J(Q; c, n)$ has been studied by many authors extensively in various special cases:

(i) The linear case $\mathbf{k} = (1, \cdots, 1)$. For $J = I$ and $\boldsymbol{\lambda} = (1, \cdots, 1)$, this is a problem proposed by H. Rademacher [7] in 1925 and answered by A. Brauer [2] in 1926, and recovered by many authors later from time to time. For $J = I$ and $\boldsymbol{\lambda} = (\lambda_i)$ where the $\lambda_i$'s are divisors of $n$, this is the work of Sun and Yang [9] in 2014.

(ii) The quadratic case $\mathbf{k} = (2, \cdots, 2)$. For $J = \emptyset$, this is studied in the work of Tóth [10] in 2014. For $t = 2$ and $\boldsymbol{\lambda} = (1, 1)$, this is the work of Yang and Tang [11] in 2015. For $t = 2$, $\boldsymbol{\lambda}$ arbitrary and $J = I$, this is the work of Sun and Cheng [8] in 2016. For general $t$, $\boldsymbol{\lambda} = (1, \cdots, 1)$ and $J = I$, this is the recent work of Mollahajiaghaei [6]. See also [3] for more development.

(iii) The case $t = 2$, $\boldsymbol{\lambda} = (1, 1)$ and $\mathbf{k} = (k, k)$. Partial results were obtained by Deaconescu and Du [4].

### 1.2. Notations

We first fix the following notations in this paper.

$p$ is always a prime number and $v_p$ is the $p$-adic valuation, $a$ is always a positive integer and $I$ is the set $\{1, \cdots, t\}$.

For a set $X$, $\#X$ or $|X|$ means the cardinality of $X$. For two subsets $X$ and $Y$ of the set $U$, the difference set $X - Y$ is the set $\{x \in U \mid x \in X,\ x \notin Y\}$.

For the congruence equation

$$Q(x_1, \cdots, x_t) = \lambda_1 x_1^{k_1} + \cdots + \lambda_t x_t^{k_t} \equiv c \bmod n, \quad (c \in \mathbb{Z},\ n \in \mathbb{Z}_{\geq 2})$$

we call $t$, $\mathbf{k}$ and $n$ its *dimension*, *degree* and *level* respectively.

For $J$ a nonempty subset of $I$, the *depth* $d_{p,J} = d_{p,J}(Q) = d_{p,J}(\boldsymbol{\lambda}, \mathbf{k})$ of $Q$ at prime $p$ associated to $J$ is defined by

$$d_{p,J} = \begin{cases} \min\limits_{i\in J}\{v_p(\lambda_i k_i) + 1\}, & \text{if } p \text{ odd;} \\ \min\limits_{i\in J}\{v_2(\lambda_i k_i) + 2 \text{ if } 2 \mid k_i,\ v_2(\lambda_i k_i) + 1 \text{ if } 2 \nmid k_i\}, & \text{if } p = 2. \end{cases}$$

Write $d_p$ for $d_{p,I}$ and call it the depth of $Q$ at $p$.

For $J$ a nonempty subset of $I$, let $\boldsymbol{\lambda}_J = (\lambda_i)_{i\in J}$, $\mathbf{k}_J = (k_i)_{i\in J}$ and $Q_J = \sum\limits_{j\in J} \lambda_j x^{k_j} \in \mathbb{Z}[x_j :\ j \in J]$. Set $Q_\emptyset = 0$ and

$$N_\emptyset(0; c, p^a) = N^*(0; c, p^a) = \begin{cases} 1, & \text{if } p^a \mid c; \\ 0, & \text{if } p^a \nmid c. \end{cases}$$

If $Q$ and $(\boldsymbol{\lambda}, \mathbf{k})$ are clear from the context, we may drop them in our notations.

### *1.3. Main results*

Suppose $n$ has the prime decomposition

$$n = \prod_{p\mid n} p^{n_p}.$$

By Chinese Remainder Theorem, the set of solutions of $Q(x_1, \cdots, x_t) \equiv c \bmod n$ is in one-to-one correspondence with the product set of solutions of the equations $Q(x_1, \cdots, x_t) \equiv c \bmod p^{n_p}$ for primes $p \mid n$. Moreover, $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $x \in (\mathbb{Z}/p^{n_p})^\times$ for all $p \mid n$. Thus for any $J \subseteq I$, we have the product formula

$$N_J(Q; c, n) = \prod_{p\mid n} N_J(Q; c, p^{n_p}). \tag{1}$$

So to compute $N_J(Q; c, n)$, it suffices to study the prime power case $N_J(Q; c, p^a)$. By simple argument (as seen in Proposition 2.1(2)), we may reduce $Q$ to the case $p \nmid \lambda_i$ for some $i \in I$, which we call $Q$ is *reduced at* $p$.

Our first main result, which we call the *decomposition formula*, is the following theorem:

**Theorem A.** *Given the polynomial $Q$. For subsets $J_1 \subsetneq J_2 \subseteq I$, let*

$$B_i(J_1, J_2; a) = \begin{cases} \{0\}, & \text{if } i \notin J_2 - J_1; \\ \{0, \cdots, a\}, & \text{if } i \in J_2 - J_1, \end{cases} \qquad B(J_1, J_2; a) = \prod_{i=1}^{t} B_i(J_1, J_2; a).$$

*For $\mathbf{b} \in B(\emptyset, I; a)$, but $\mathbf{b} \neq (a, \cdots, a)$, let*

$$J_{\mathbf{b}} = \{i \in I \mid b_i < a\}, \quad Q_{\mathbf{b}} = \sum_{j \in J_{\mathbf{b}}} \lambda_j p^{k_j b_j} x_j^{k_j}, \quad s(\mathbf{b}) = \sum_{j \in J_{\mathbf{b}}} b_j.$$

*If* $\mathbf{b} = (a, \cdots, a)$*, let* $J_{\mathbf{b}} = \emptyset$*,* $Q_{\mathbf{b}} = 0$ *and* $s(\mathbf{b}) = 0$*. Then we have the* decomposition formula

$$N_{J_1}(Q; c, p^a) = \sum_{\mathbf{b} \in B(J_1, J_2; a)} p^{-s(\mathbf{b})} N_{J_2 \cap J_{\mathbf{b}}}(Q_{\mathbf{b}}; c, p^a). \tag{2}$$

Our next two results are consequences of the following *lifting formula*

$$N_J(Q; c, p^{a+1}) = p^{t-1} N_J(Q; c, p^a) \tag{3}$$

for $a$ sufficiently large under various assumptions. We shall establish this formula by simple $p$-adic analysis, not by the more complicated exponential sum argument employed by other authors. More precisely, we have

**Theorem B.** *Given the polynomial* $Q$*, and assume it is reduced at prime* $p$*. Then*

(1) *For* $a \geq d_{p,J}$ *and* $c \in \mathbb{Z}$*,*

$$N_J(Q; c, p^a) = p^{(t-1)(a-d_{p,J})} N_J(Q; c, p^{d_{p,J}}). \tag{4}$$

(2) *For* $a \leq d_p = d_{p,I}$*, the map*

$$\varphi_a : (\mathbb{F}_p)^t \to \mathbb{Z}/p^a\mathbb{Z}, \ (a_1, \cdots, a_t) \mapsto Q(\alpha_1, \cdots, \alpha_t) \bmod p^a,$$

*where* $\alpha_i \in \mathbb{Z}$ *is any lifting of* $a_i \in \mathbb{F}_p$*, is well defined. Let* $\varphi_{a,J}$ *be the restriction of* $\varphi_a$ *on* $\prod_{i \in I-J} \mathbb{F}_p \times \prod_{i \in J} \mathbb{F}_p^\times$*, then*

$$N_J(Q; c, p^a) = p^{(a-1)t} \# \varphi_{a,J}^{-1}(c \bmod p^a). \tag{5}$$

*In particular, if* $p = 2$ *and* $a \leq d_2$*,*

$$\# \varphi_{a,J}^{-1}(c \bmod 2^a) = \#\{T \subseteq \{1, \cdots, t\} \mid T \supseteq J, \ v_2(\sum_{i \in T} \lambda_i - c) \geq a\}. \tag{6}$$

**Theorem C.** *Given polynomial* $Q$ *and prime* $p$*. Let* $f_p = \max\{v_p(k_i) + 1\}$ *(or* 3 *if* $p = 2$ *and* $\max\{v_2(k_i)\} = 1$*). For integer* $c \neq 0$*, let* $c_p$ *be the* $p$*-adic valuation of* $c$*. Then for any* $a \geq 1$*, any* $J \subseteq I$ *(empty or not),* $f \geq f_p$ *and any* $x \in \mathbb{Z}/p^a\mathbb{Z}$*,*

$$N_J(Q; c(1 + p^f x), p^a) = N_J(Q; c, p^a). \tag{7}$$

*In particular, for* $a \geq c_p + f_p$*,*

$$N_J(Q;c,p^a)=p^{(t-1)(a-c_p-f_p)}N_J(Q;c,p^{c_p+f_p}). \tag{8}$$

*Thus $N_J(Q;c,p^a)$ as $a$ varies is completely determined by $N_J(c,p^a)$ for $a\le c_p+f_p$.*

**Remark.** For $J=\emptyset$, even if $p\nmid\prod_{i=1}^{t}k_i$, the formula for $N(Q;0,p^a)$ is much more complicated. In general we don't always have $N(0,p^a)=p^{t-1}N(0,p^{a-1})$ for $a$ sufficiently large. For example, consider $Q(x_1,x_2)=x_1^3+px_2^3$. Then $N(0,p^{3a})=p^{4a}$, $N(0,p^{3a+1})=p^{4a+1}$ and $N(0,p^{3a+2})=p^{4a+2}$.

As a consequence of Theorems A, B and C, we will give a (theoretical) algorithm to effectively compute $N_J(Q;c,p^a)$ for all possible $J$, $c$ and $a$ if the prime number $p\nmid\prod_{i=1}^{t}k_i$. Moreover, except the case $J=\emptyset$ and $c=0$, the number of steps to compute $N_J(Q;c,p^a)$ is bounded by a constant independent of $a$.

Using the main theorems and the algorithm, we shall work on the example $Q(x_1,\cdots,x_t)=\lambda_1x_1^k+\cdots+\lambda_tx_t^k$. We obtain the following results:

(1) In the linear case ($k=1$), we solve the counting problem in full generality (cf. [9]). Namely, for any prime $p$, we completely determine the value of $N_J(Q;c,p^a)$ for arbitrary $J\subseteq I$, $c\in\mathbb{Z}$ and $a\ge1$. Our result is stated in Theorem 4.1.
(2) In the quadratic case ($k=2$), for any prime $p$, we completely determine the value of $N_J(Q;c,p^a)$ for any $J\subseteq I$ satisfying $\min\{v_p(\lambda_i)\mid i\in I\}=\min\{v_p(\lambda_i)\mid i\in J\}$, and arbitrary $c\in\mathbb{Z}$ and integer $a\ge1$. In particular, we get the exact formula for $N^*(Q;c,p^a)$ for any $c\in\mathbb{Z}$ and $a\ge1$. Our result is stated in Theorem 4.4. This is a vast generalization of Yang–Tang [11], Sun–Cheng [8] and Mollahajiaghaei [6].
(3) In the general case, for prime $p\nmid k$, we give a more detailed version of our algorithm in Theorem 4.2. We obtain formulas so that $N_J(Q;c,p^a)$ can be computed in finite steps independent of $a$ except the case $c=0$ and $J=\emptyset$.
(4) We study the case $p\nmid k$ and the dimension $t=2$ in full generality. When $k=2$, $N_J(c,2^a)$ is also studied in full generality.

Finally we shall work on the example $Q(x_1,x_2,x_3)=9x_1+3x_2^3+x_3^9$ for $p=3$, which is not covered by our algorithm, but the main theorems are still applicable.

As a final remark, let us make a comparison of our method with those methods by previous work. The majority of previous study was concentrated on the quadratic case. The exponential sum especially the quadratic Gauss sum was used in [3,9,8,10,11], which was the main tool to study this type of counting problem. In [6], a new combinatorial approach via spectral graph theory was used. In our paper, for the decomposition formula, we decompose the residue ring $\mathbb{Z}/p^a\mathbb{Z}$ into pieces of the form $p^b\mathbb{Z}/p^a\mathbb{Z}-p^{b+1}\mathbb{Z}/p^a\mathbb{Z}$, and then use a simple counting argument to deduce the formula. The lifting formula is a consequence of a simple fact from elementary number theory about $p^k$-th power modulo $p^a$. These two formulas and the Inclusion–Exclusion Principle reduce the general counting problem (in most cases) to the counting problem of solutions of polynomials over finite fields with no restriction on variables, where the exponential sum is needed but much has been done in this subject (see for example [1,5]). All these results then are used in the application to count the solutions of $Q(x_1, \cdots, x_t) = \lambda_1 x_1^k + \cdots + \lambda_t x_t^k$.

## 2. Preliminaries

### 2.1. *Reduce Q to the reduced case*

The following fact is obvious:

**Proposition 2.1.** *Consider the number $N_J(Q; c, p^a)$ for $p$ a prime number and $J \subseteq I$.*

(1) *(Lowering dimension.) If there exists $j \in I$ such that $v_p(\lambda_j) \geq a$, then*

$$N_J(Q; c, p^a) = \begin{cases} p^a N_J(Q_{I-\{j\}}; c, p^a) & \text{if } j \notin J; \\ p^{a-1}(p-1) N_{J-\{j\}}(Q_{I-\{j\}}; c, p^a) & \text{if } j \in J. \end{cases} \tag{9}$$

(2) *(Lowering level.) Let $e = \min\{v_p(\lambda_i) \mid i \in I\}$ and $v_p(c) = c_p$. Then*

$$N_J(Q; c, p^a) = \begin{cases} p^{te} N_J(Q/p^e; c/p^e, p^{a-e}) & \text{if } e \leq \min\{a, c_p\}, \\ p^{(at-|J|)}(p-1)^{|J|} & \text{if } a \leq \min\{e, c_p\}, \\ 0 & \text{if } c_p < \min\{e, a\}. \end{cases} \tag{10}$$

(3) *(Lowering degree.) If one has $v_p(k_i) \geq a$, replace $k_i$ by $k_i/p^{v_p(k_i)-a+1}$. Then the new $k_i$ has $p$-adic valuation $a$ and $N_J(Q; c, p^a)$ is unchanged.*

**Proof.** The only thing needs to prove is (3), which follows from Euler's Theorem that for $x \in (\mathbb{Z}/p^a\mathbb{Z})^\times$, $x^{p^s} = x^{p^{a-1}}$ for all $s \geq a-1$, and for $x \in p\mathbb{Z}/p^a\mathbb{Z}$, $x^{p^s} = 0$ for all $s \geq a-1$ since $p^{a-1} \geq a$ for any prime $p$ and integer $a \geq 1$. □

Based on Proposition 2.1, to compute $N_J(Q; c, p^a)$, it suffices to consider the case that $\min\{v_p(\lambda_i)\} = 0$, $\max\{v_p(\lambda_i),\ v_p(k_i) \mid i = 1, \cdots, t\} < a$ and the depth $d_p \leq a$. In particular, we can always assume $p \nmid \lambda_i$ for some $i \in I$.

### 2.2. *Formulas for $N(Q; c, p)$*

We recall the classical formulas for $N(Q; c, p)$. First recall for complex characters $\chi_1, \cdots, \chi_t$ of the prime field $\mathbb{F}_p$, the *Jacobi sum* $J(\chi_1, \cdots, \chi_t)$ is defined by the formula

$$J(\chi_1, \cdots, \chi_t) = \sum_{u_1 + \cdots + u_t = 1} \chi_1(u_1) \cdots \chi_t(u_t)$$

and the *Jacobi sum* $J_0(\chi_1, \cdots, \chi_t)$ is defined by the formula

$$J_0(\chi_1, \cdots, \chi_t) = \sum_{u_1+\cdots+u_t=0} \chi_1(u_1)\cdots\chi_t(u_t).$$

Then the following theorem is well known:

**Theorem 2.2.**

(1) *Suppose $p$ is odd and $\lambda_1 \cdots \lambda_t \neq 0 \in \mathbb{F}_p$. Then $N(c, p)$, the number of solutions of*

$$Q(x_1, \cdots, x_t) = \lambda_1 x^{k_1} + \cdots \lambda_t x^{k_t} = c$$

*over the prime field $\mathbb{F}_p$, is given by*

$$N(0, p) = p^{t-1} + \sum_{\substack{\chi_i^{k_i}=1,\ \chi_i\neq 1 \\ \chi_1\cdots\chi_t=1}} \chi_1(\lambda_1^{-1})\cdots\chi_t(\lambda_t^{-1}) J_0(\chi_1, \cdots, \chi_t), \tag{11}$$

*and*

$$N(c, p) = p^{t-1} + \sum_{\substack{\chi_i^{k_i}=1 \\ \chi_i\neq 1}} \chi_1\cdots\chi_t(c)\chi_1(\lambda_1^{-1})\cdots\chi_t(\lambda_t^{-1}) J(\chi_1, \chi_2, \cdots, \chi_t) \tag{12}$$

*for $c \neq 0$.*

(2) *If $2 \nmid \lambda_i$ for some $i \in I$, then $N(0, 2) = N(1, 2) = 2^{t-1}$.*

**Proof.** Part (1) follows from Theorem 5 in § 8.7 in [5]. Part (2) is clear, since $x^k = x$ in $\mathbb{F}_2$. □

## 3. Proof of the main theorems and the algorithm

### *3.1. The decomposition formula and its special cases*

We now prove Theorem A.

**Proof of Theorem A.** Note that $\mathbb{Z}/p^a\mathbb{Z}$ has a disjoint decomposition (assuming $p^{a+1}\mathbb{Z}/p^a\mathbb{Z}$ is the empty set)

$$\mathbb{Z}/p^a\mathbb{Z} = \bigsqcup_{b=0}^{a} (p^b\mathbb{Z}/p^a\mathbb{Z} - p^{b+1}\mathbb{Z}/p^a\mathbb{Z}).$$

Suppose $\mathbf{x} = (x_1, \cdots, x_t) \in \Gamma_{J_1}(Q; c, p^a)$, and if $J_1 = \emptyset$ and $J_2 = I$, suppose $\mathbf{x} \neq \mathbf{0}$. Then for $j \in J_2 - J_1$, $x_j \in p^{b_j}\mathbb{Z}/p^a\mathbb{Z} - p^{b_j+1}\mathbb{Z}/p^a\mathbb{Z}$ for some $0 \leq b_j \leq a$. Set $b_j = 0$ for $j \notin J_2 - J_1$. Let $\mathbf{b} = \mathbf{b}(\mathbf{x}) = (b_j)_{j=1,\cdots,t} \in B(J_2, J_1; a)$ and $J_{\mathbf{b}} \neq \emptyset$.

For $j \in J_2 \cap J_{\mathbf{b}}$, the element $\tilde{x}_j = x_j/p^{b_j}$ is a well defined element in $(\mathbb{Z}/p^{a-b_j}\mathbb{Z})^\times$. Let $C_j = \{x \in (\mathbb{Z}/p^a\mathbb{Z})^\times \mid x \equiv \tilde{x}_j \bmod p^{a-b_j}\}$. For $j \in J_{\mathbf{b}} - J_2$, let $C_j = \{x_j\}$. Then

$$C_{\mathbf{x}} = \prod_{j \in J_{\mathbf{b}}} C_j \subseteq \Gamma_{J_2 \cap J_{\mathbf{b}}}(Q_{\mathbf{b}}; c, p^a).$$

On the other hand, if $Q_{\mathbf{b}} \neq 0$, then $J_{\mathbf{b}}$ as the set of $j$'s such that $x_j$ appears in $Q_{\mathbf{b}}$ is not empty. For $(y_j)_{j \in J_{\mathbf{b}}} \in \Gamma_{J_2 \cap J_{\mathbf{b}}}(Q_{\mathbf{b}}; c, p^a)$, let $\tilde{x}_j \equiv y_j \bmod p^{a-b_j}$, then $x_j = p^{b_j}\tilde{x}_j$ is a well defined element in $p^{b_j}\mathbb{Z}/p^a\mathbb{Z} - p^{b_j+1}\mathbb{Z}/p^a\mathbb{Z}$. Let $x_j = 0$ for $j \notin J_{\mathbf{b}}$. Then $\mathbf{x} = (x_j) \in \Gamma_{J_1}(Q; c, p^a)$. In this way, one element $\mathbf{x}$ corresponds exactly to $p^{\sum_{j: b_j < a} b_j} = p^{s(\mathbf{b})}$ elements in $\Gamma_{J_2 \cap J_{\mathbf{b}}}(Q_{\mathbf{b}}; c, p^a)$.

If $J_1 = \emptyset$ and $J_2 = I$, then $\mathbf{0} \in \Gamma_{J_1}(Q; c, p^a)$ if and only if $p^a \mid c$, which is corresponding to the case $\mathbf{b} = (a, \cdots, a)$ and $Q_{\mathbf{b}} = 0$.

In conclusion, (2) is proved. □

**Special cases of the decomposition formula.** We shall use the following special cases in this paper:

(1) The case $J = J_1 \subsetneq I = J_2$. Then

$$N_J(Q; c, p^a) = \sum_{\mathbf{b} \in B(J, I; a)} p^{-s(\mathbf{b})} N^*(Q_{\mathbf{b}}; c, p^a). \tag{13}$$

This means that if we can determine $N^*(Q_{\mathbf{b}}; c, p^a)$ for all $\mathbf{b} \in B(J, I; a)$, then we get $N_J(Q; c, p^a)$.

(2) The case $a = 1$. Then

$$N_{J_1}(Q; c, p) = \sum_{T \subseteq J_2 - J_1} N_{J_2 - T}(Q_{I-T}; c, p). \tag{14}$$

By the Inclusion–Exclusion Principle, (14) has the following inverse formula

$$N_{J_2}(Q; c, p) = \sum_{T \subseteq J_2 - J_1} (-1)^{|T|} N_{J_1}(Q_{I-T}; c, p). \tag{15}$$

Take $J_1 = \emptyset$ and $J_2 = J$ in (15), then we have

$$N_J(Q; c, p) = \sum_{T \subseteq J} (-1)^{|T|} N(Q_{I-T}; c, p). \tag{16}$$

This means that $N_J(Q; c, p)$ is determined by $N(Q_{I-T}; c, p)$ for all $T \subseteq J$.

**Remark.** Another interesting question is to count the number $N_{J_1,J_2}(Q; c, n)$ of solutions of $Q(x_1, \cdots, x_t) \equiv c \bmod n$ such that $x_i \in (\mathbb{Z}/n\mathbb{Z})^\times$ for $i \in J_1$ and $x_i \notin (\mathbb{Z}/n\mathbb{Z})^\times$ for

$i \in J_2$. First one must keep in mind that no product formula exists in general for $N_{J_1,J_2}(Q;c,n)$ if $J_2 \neq \emptyset$. However, by the Inclusion–Exclusion Principle, we have

$$N_{J_1,J_2}(Q;c,n) = \sum_{T \subseteq J_2} (-1)^{|T|} N_{J_1 \cup T}(Q;c,n). \tag{17}$$

As a consequence, the values $N_J(Q;c,n)$ for all $J$ determine $N_{J_1,J_2}(Q;c,n)$ for all disjoint pairs $(J_1, J_2)$.

### *3.2. The lifting formula*

We need the following lemma whose proof is an easy exercise of Newton's Binomial Theorem and $p$-adic analysis:

**Lemma 3.1.**

(1) *Let $p$ be an odd prime. For integers $x$, $y$, $k \geq 1$, and $m \geq 1$, we have*

$$(x + p^m y)^k - x^k \equiv kx^{k-1} y p^m \bmod p^{m+v_p(k)+1}.$$

(2) *For integers $x$ and integer $y$, $k \geq 1$, and $m \geq 1$, then*

$$(x + 2^m y)^k - x^k \equiv \begin{cases} 0 \bmod 2^{v_2(k)+2}, & \textit{if } k \textit{ even and } m = 1, \\ kx^{k-1} y \cdot 2^m \bmod 2^{v_2(k)+m+1}, & \textit{otherwise.} \end{cases}$$

*For odd integer $x$,*

$$v_2(x^k - 1) \geq \begin{cases} 1, & \textit{if } k \textit{ odd,} \\ 2 + v_2(k), & \textit{if } k \textit{ even.} \end{cases}$$

(3) *Let $U_{p,a}^{(i)} = \{1 + p^i x \mid x \in \mathbb{Z}/p^a\mathbb{Z}\} \subseteq (\mathbb{Z}/p^a\mathbb{Z})^\times$. Then for $f > 0$, $(U_{p,a}^{(i)})^{p^f} = U_{p,a}^{(f+i)}$ if $(p, i) \neq (2, 1)$ and $(U_{2,a}^{(1)})^{p^f} = U_{2,a}^{(f+2)}$.*

We are now ready to prove Theorem B and Theorem C.

**Proof of Theorem B.** Write $d = d_p$. Let $\psi_{a,b}$ be the natural reduction map from $\Gamma_J(c, p^a)$ to $\Gamma_J(c, p^b)$.

(1) First assume $p$ is odd. Suppose that $j$ satisfies $v_p(\lambda_j k_j) = e_j + f_j = d_j < a$. By Lemma 3.1(1), if $(x_1, \cdots, x_j, \cdots, x_t) \in \Gamma_J(c, p^a)$, then $(x_1, \cdots, x_j + p^{a-d_j} y_j, \cdots, x_t) \in \Gamma_J(c, p^a)$ for any $y_i \in \mathbb{Z}/p^a\mathbb{Z}$.

If $a > d_{p,J}$, then $a > d_j + 1$ for some $j \in J$. Let $(a_1, \cdots, a_t) \in \Gamma_J(c, p^{a-1})$. Let $u \in \{0, \cdots, p-1\}$. Let $x_i \in \mathbb{Z}/p^a\mathbb{Z}$ be any lifting of $a_i$. Then

$$Q(x_1,\cdots,x_j+up^{a-d_j-1},\cdots,x_t)\equiv Q(x_1,\cdots,x_t)+\frac{\lambda_j k_j}{p^{d_j}}x_j^{k_j-1}up^{a-1} \bmod p^a.$$

Thus there exists exactly one $u\in\{0,\cdots,p-1\}$ such that $(x_1,\cdots,x_j+up^{a-d_j-1},\cdots,x_t)\in\Gamma_J(c,p^a)$, and $\psi_{a,a-1}$ is a $p^{t-1}$-to-1 map. Thus we have the lifting formula

$$N_J(c,p^a)=p^{t-1}N_J(c,p^{a-1}) \tag{18}$$

for all $a>d_{p,J}$.

Now assume $p=2$. Assume $a>d_{2,J}$. Then the assumption means that $a>d_j+2$ for some $j\in J$ with $k_j$ even or $a>d_j+1$ for some $j\in J$ with $k_j$ odd. Let $(a_1,\cdots,a_t)\in\Gamma_J(c,2^{a-1})$. Let $x_i\in\mathbb{Z}/2^a\mathbb{Z}$ be any lift of $a_i$. Then

$$Q(x_1,\cdots,x_j+2^{a-d_j-1},\cdots,x_t)\equiv Q(x_1,\cdots,x_t)+2^{a-1} \bmod 2^a.$$

Thus one of $(x_1,\cdots,x_t)$ and $(x_1,\cdots,x_j+2^{a-d_j-1},\cdots,x_t)$ is a solution of $Q(x_1,\cdots,x_t)\equiv c \bmod 2^a$, and $\psi_{a,a-1}$ is a $2^{t-1}$-to-1 map. Again we have the lifting formula.

(2) Assume $a\le d=d_{p,I}$. Suppose $(a_1,\cdots,a_t)\in\mathbb{F}_p^t$, let $\alpha_i\in\mathbb{Z}$ be any lifting of $a_i$. Then

$$\lambda_i\alpha_i^{k_i}\equiv\lambda_i(\alpha_i+py_i)^{k_i} \bmod p^a$$

for any $y_i\in\mathbb{Z}$, and $Q(\alpha_1,\cdots,\alpha_t) \bmod p^a$ is a fixed element in $\mathbb{Z}/p^a\mathbb{Z}$ independent of the lifting, so the map $\varphi_a$ is well-defined. Thus for $(a_1,\cdots,a_t)\in\Gamma_J(c,p)\subseteq\mathbb{F}_p^t$,

$$\#\psi_{a,1}^{-1}(a_1,\cdots,a_t)=\begin{cases}p^{(a-1)t}, & \text{if } \varphi_a(a_1,\cdots a_t)=c \bmod p^a;\\ 0, & \text{if otherwise.}\end{cases}$$

Assume furthermore that $p=2$. For $T\subseteq I$, let $e_T=(e_{T,i})_{i\in I}$ be the element in $\mathbb{F}_2^t$ that $e_{T,i}=1$ for $i\in T$ and $e_{T,i}=0$ for $i\notin T$. Then $\Gamma_J(c,2)$ consists of elements $e_T$ satisfying $T\supseteq J$ and $v_2(\sum_{i\in T}\lambda_T-c)\ge 1$. Let 0 and 1 in $\mathbb{Z}$ be the liftings of 0 and 1 in $\mathbb{F}_2$ respectively. Then $\varphi_a(e_T)=\sum\limits_{i\in T}\lambda_i \bmod 2^a$. This finishes the proof of Theorem B(2). □

**Corollary 3.2.** *Given the polynomial $Q(x_1,\cdots,x_t)$. If at prime $p$ one has $d_p\ge t$. Then there exists $c\in\mathbb{Z}$ such that $N^*(Q;c,p^{d_p})=0$.*

**Proof.** This is because there are $p^{d_p}$ conjugacy classes modulo $p^{d_p}$ but there are only $(p-1)^t$ points in $\mathbb{F}_p^{\times\, t}$. □

**Proof of Theorem C.** Write $k_i=p^{f_i}k_i'$ such that $(p,k_i')=1$. By Lemma 3.1, if $f\ge f_p$, then for any $i\in I$, $1+p^fx=(1+py_i)^{p^{f_i}}$ for some $y_i\in\mathbb{Z}/p^a\mathbb{Z}$. If $a\le c_p+f$, the formula is certainly true. For $a>c_p+f$, let $u_i,v_i\in\mathbb{Z}$ such that $u_ik_i'+p^{a-f_i}v_i=1$, then $1+p^fx=(1+py_i)^{u_ik_i}=\beta_i^{k_i}$ for some $\beta_i\in(\mathbb{Z}/p^a\mathbb{Z})^\times$. Thus we have a one-to-one correspondence

$$\Gamma_J(c,p^a) \to \Gamma_J(c(1+p^f x),p^a), \qquad (x_i) \mapsto (x_i\beta_i)$$

and hence $N_J(c,p^a) = N_J(c(1+p^f x),p^a)$.

Now consider the natural map $\psi_{a+1,a} : (\mathbb{Z}/p^{a+1}\mathbb{Z})^t \to (\mathbb{Z}/p^a\mathbb{Z})^t$. For $a > c_p + f_p$, $\psi^{-1}_{a+1,a}(\Gamma_J(c,p^a))$ is the disjoint union of $\Gamma_J(c + up^a, p^{a+1})$ for $u \in \{0, \cdots, p-1\}$, but all $\Gamma_J(c+up^a,p^{a+1})$ are of the same cardinality $N_J(c,p^{a+1})$, hence the lifting formula $N_J(c,p^{a+1}) = p^{t-1}N_J(c,p^a)$ holds. This finishes the proof of Theorem C. □

### 3.3. An algorithm to compute $N_J(Q;c,p^a)$ if $p \nmid \prod\limits_{i\in I} k_i$

By Theorems A, B and C, we then have the following algorithm to effectively compute $N_J(Q;c,p^a)$.

(1) Reduce $Q$ to the reduced form at $p$ (i.e., $d_p(Q) = 1$) by Proposition 2.1. We suppose $Q$ is reduced hereafter.

(2) Compute $N(Q;c,p)$ for all $Q$ by using formulas in Theorem 2.2.

(3) For $J$ nonempty, compute $N_J(Q;c,p)$ by the inverse formula (16) of the decomposition formula. If $d_{p,J} = 1$, use the relation $N_J(Q;c,p^a) = p^{(a-1)(t-1)}N_J(Q;c,p)$ by Theorem B to get $N_J(Q;c,p^a)$, in particular, get $N^*(Q;c,p^a)$.

(4) For $J$ nonempty and $d_{p,J} = b+1 > 1$, use the decomposition formula (13) to compute $N_J(Q;c,p^a)$ for all $1 < a \le b+1$, then $N_J(Q;c,p^a) = p^{(a-b-1)(t-1)}N_J(Q;c,p^{b+1})$ for $a \ge b+1$ by Theorem B. (Note: the assumption $p \nmid \prod k_i$ means the reduced form of $Q_{\mathbf{b}}$ for any $\mathbf{b}$ in the right hand side of (13) is of depth 1, hence $N^*(Q_{\mathbf{b}};c,p^a)$ can be computed as in the previous step.)

(5) If $c \ne 0$, let $c_p = v_p(c)$. Compute $N(Q;c,p^a) = N(Q;0,p^a)$ for $a \le c_p$ and $N(Q;c,p^{c_p+1})$ by the decomposition formula (13). Then for $a > c_p+1$, $N(Q;c,p^a) = p^{(a-c_p-1)(t-1)}N(Q;c,p^{c_p+1})$ from Theorem C.

(6) Use the decomposition formula (13) to compute $N(Q;0,p^a)$ for any given $a$.

**Remark.** We see that except the last step to compute the case $J = \emptyset$ and $c = 0$, the number of steps to compute $N_J(Q;c,p^a)$ is bounded by a constant independent of $a$.

In the case $J$ is nonempty, let $|J| = s$. If $c_p = v_p(c) < b$, by Theorem C, one can furthermore get

$$N_J(Q;c,p^{b+1}) = p^{b-c_p+c_p s}(p-1)^s N(Q_{I-J};c,p^{c_p+1}).$$

In particular, if $p \nmid c$, i.e., $c_p = 0$, then we just need formulas for $N(Q_{I-J};c,p)$ in Theorem 2.2 to get $N_J(Q;c,p^a)$.

## 4. Applications of the main theorems

In this section, we shall apply the general formulas obtained in the previous section to compute $N_J(Q;c,p^a)$ in many special cases. Without loss of generality, we assume $Q$ is reduced, i.e., $p \nmid \lambda_i$ for some $i$ because of (10).

### *4.1. The linear case* $Q(x_1, \cdots, x_t) = \sum_{i=1}^{t} \lambda_i x_i$

Consider the linear congruence equation

$$\lambda_1 x_1 + \cdots + \lambda_t x_t \equiv c \mod p^a.$$

**Theorem 4.1.** *Suppose $p \nmid \lambda_i$ for some $i \in I$. For any subset $J$ of $I$ and prime $p$, let $s = \#J$ and $s_p = \#J_p$ where $J_p = \{j \in J \mid p \nmid \lambda_j\}$. Then*

(1) *The lifting formula holds for all $a \geq 1$:*

$$N_J(Q; c, p^a) = p^{(a-1)(t-1)} N_J(Q; c, p). \tag{19}$$

(2) *If there exists $i \notin J$, $p \nmid \lambda_i$, then*

$$N_J(Q; c, p) = (p-1)^s \ p^{(t-s-1)}; \tag{20}$$

*if for all $i \notin J$, $p \mid \lambda_i$, then*

$$N_J(Q; c, p) = (p-1)^s \ p^{(t-s-1)} + (-1)^{s_p} (p-1)^{s-s_p} \ p^{(t-s-1)} (p\delta_c - 1) \tag{21}$$

*where $\delta_c = 1$ if $p \mid c$ and $= 0$ if $p \nmid c$.*

**Proof.** If there exists $i \notin J$, $p \nmid \lambda_i$, then one can choose all possible $x_j$ for $j \neq i$, and then $x_i$ is decided by the $x_j$'s, so $N_J(Q; c, p^a) = p^{a(t-s-1)} \cdot \varphi(p^a)^s$. Thus (20) holds, so does (19) in this situation.

If for all $i \notin J$, $p \mid \lambda_i$, then there exists $i \in J$ such that $p \nmid \lambda_i$, so $d_{p,J} = 1$ and (19) holds in this situation by Theorem B. Now one easily has $N_J(Q; c, p) = p^{t-s}(p-1)^{s-s_p} N^*(Q_{J_p}; c, p)$, and by (15),

$$\begin{aligned} N^*(Q_{J_p}; c, p) &= \sum_{i=0}^{s_p-1} (-1)^i \binom{s_p}{i} p^{s_p-i-1} + (-1)^{s_p} \delta_c \\ &= \frac{1}{p}(p-1)^{s_p} + (-1)^{s_p}(\delta_c - \frac{1}{p}). \end{aligned}$$

The theorem is proved. □

### *4.2. The case* $Q(x_1, \cdots, x_t) = \sum_{i=1}^{t} \lambda_i x_i^k$

In this subsection, we consider the congruence equation

$$\lambda_1 x_1^k + \cdots + \lambda_t x_t^k \equiv c \mod p^a.$$

### 4.2.1. A general result

The following Theorem is a more detailed version of our algorithm:

**Theorem 4.2.** *Suppose prime $p \nmid k$ and $Q$ is reduced at $p$. For $c \neq 0$, let $c_p$ be the $p$-adic valuation of $c$. Let $I_p = \{i \in I \mid p \nmid \lambda_i\}$ and $t_p = \#I_p$. For $J$ a nonempty subset of $I$, let $J_p = \{i \in J \mid p \nmid \lambda_i\}$, $s = \#J$ and $s_p = \#J_p$. Then*

(1) *For $c \neq 0$, $N(Q; c, p^a)$ for all $a \geq 1$ is completely determined by $N(Q; 0, p^a)$ for $1 \leq a \leq c_p$ and $N(Q; c, p^{c_p+1})$ through the formula*

$$N(Q; c, p^a) = p^{(a-c_p-1)(t-1)} N(Q; c, p^{c_p+1}), \quad \text{if } a \geq c_p + 1. \tag{22}$$

*In particular, if $p \nmid c$, then for $a \geq 1$,*

$$N(Q; c, p^a) = p^{(a-1)(t-1)} N(Q; c, p) = p^{at-a-t_p+1} N(Q_{I_p}; c, p) \tag{23}$$

*where $N(Q_{I_p}; c, p)$ can be computed by the formulas in Theorem 2.2.*

(2) *If $J_p \neq \emptyset$, i.e., $s_p \neq 0$ and $d_{p,J} = 1$, then for any $a \geq 1$, for any $c \in \mathbb{Z}$,*

$$N_J(Q; c, p^a) = p^{(a-1)(t-1)} N_J(Q; c, p), \tag{24}$$

$$N_J(Q; c, p) = (p-1)^{s-s_p} p^{t-s+s_p-t_p} \cdot N_{J_p}(Q_{I_p}; c, p), \tag{25}$$

*and*

$$N_{J_p}(Q_{I_p}; c, p) = \sum_{I_p - J_p \subseteq T \subseteq I_p} (-1)^{t_p - |T|} N(Q_T; c, p) \tag{26}$$

*where $N(Q_T; c, p)$ can be computed by the formula in Theorem 2.2.*

*In particular, $N^*(Q; c, p^a)$ can be computed by the formulas above, in this case $J = I$ and $J_p = I_p$.*

(3) *If $d_{p,J} = b + 1 > 1$, i.e., $s_p = 0$, then for $c \in \mathbb{Z}$,*

$$N_J(Q; c, p^a) = p^{(a-b-1)(t-1)} N_J(Q; c, p^{b+1}). \tag{27}$$

*If moreover, $c_p < b$, then*

$$N_J(Q; c, p^a) = \begin{cases} (p-1)^s p^{as-s} N(Q_{I-J}; c, p^a), & \text{if } a < c_p + 1; \\ (p-1)^s p^{(a-c_p-1)(t-1)+c_p s} N(Q_{I-J}; c, p^{c_p+1}), & \text{if } a \geq c_p + 1. \end{cases} \tag{28}$$

*Here $N_J(Q; c, p^a)$ for $a \leq b + 1$ and $N(Q_{I-J}; c, p^a)$ for $a \leq c_p + 1$ can be computed by the decomposition formula (13).*

*In particular, if $p \nmid c$, then for $a \geq 1$,*

$$N_J(Q;c,p^a) = (p-1)^s p^{at-a-s-t_p+1} N(Q_{I_p};c,p) \tag{29}$$

*where $N(Q_{I_p};c,p)$ can be computed by Theorem 2.2.*

### *4.2.2. The quadratic case*

In this case, we recall the following well-known result:

**Proposition 4.3.** *Suppose $Q(x_1,\cdots,x_t) = \lambda_1 x_1^2 + \cdots + \lambda_t x_t^2$. For odd prime $p$, let $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol. If $p \nmid \prod\limits_{i=1}^{t} \lambda_i$, then*

$$N(Q;c,p) = \begin{cases} p^{t-1} + \left(\frac{c\lambda_1\cdots\lambda_t}{p}\right)\left(\frac{-1}{p}\right)^{\frac{t-1}{2}} p^{\frac{t-1}{2}}, & \text{if } t \text{ odd;} \\ p^{t-1} - \frac{1}{p}\left(\frac{\lambda_1\cdots\lambda_t}{p}\right)\left(\frac{-1}{p}\right)^{\frac{t}{2}} p^{\frac{t}{2}}, & \text{if } t \text{ even and } p \nmid c; \\ p^{t-1} + \frac{p-1}{p}\left(\frac{\lambda_1\cdots\lambda_t}{p}\right)\left(\frac{-1}{p}\right)^{\frac{t}{2}} p^{\frac{t}{2}}. & \text{if } t \text{ even and } p \mid c. \end{cases} \tag{30}$$

**Proof.** This follows from §8.6 in [5], and can also be found in [1]. □

**Remark.** The above formula holds for $I = \emptyset$. In this case $t = 0$ and $N(0;c,p) = 1$ if $p \mid c$ and 0 if not.

**Theorem 4.4.** *Suppose $Q(x_1,\cdots,x_t) = \lambda_1 x_1^2 + \cdots + \lambda_t x_t^2$ and $p \nmid \lambda_i$ for some $i \in I$.*

(1) *For $p$ odd, suppose $p \nmid \lambda_i$ for some $i \in I$. Let $I_p = \{i \in I \mid p \nmid \lambda_i\}$, let $t_p = \#I_p$ and $r_p = \#\{i \in I \mid \lambda_i$ is a quadratic non-residue modulo $p\}$. Write $p^* = p \cdot \left(\frac{-1}{p}\right)$, and for $i \geq j \geq 0$, write*

$$A_p(i,j) = \frac{(\sqrt{p^*}+1)^{i-j}(\sqrt{p^*}-1)^j + (\sqrt{p^*}-1)^{i-j}(\sqrt{p^*}+1)^j}{2},$$
$$B_p(i,j) = \frac{(\sqrt{p^*}+1)^{i-j}(\sqrt{p^*}-1)^j - (\sqrt{p^*}-1)^{i-j}(\sqrt{p^*}+1)^j}{2}.$$

*Then for $a \geq 1$, we have*

$$N^*(Q;c,p^a) = p^{(t-1)(a-1)}(p-1)^{t-t_p} N^*(Q_{I_p};c,p), \tag{31}$$

*where $N^*(Q_{I_p};c,p)$ is given by*

$$\frac{1}{p}(p-1)^{t_p} + \begin{cases} (-1)^{r_P}\left(\frac{A_p(t_p,r_p)}{\sqrt{p^*}}\left(\frac{c}{p}\right) + \frac{B_p(t_p,r_p)}{p}\right), & \text{if } 2 \nmid t_p \text{ and } p \nmid c; \\ (-1)^{r_p-1}\left(\frac{A_p(t_p,r_p)}{p} + \frac{B_p(t_p,r_p)}{\sqrt{p^*}}\left(\frac{c}{p}\right)\right), & \text{if } 2 \mid t_p \text{ and } p \nmid c; \\ (-1)^{r_p-1}\frac{(p-1)B_p(t_p,r_p)}{p}, & \text{if } 2 \nmid t_p \text{ and } p \mid c; \\ (-1)^{r_p}\frac{(p-1)A_p(t_p,r_p)}{p}, & \text{if } 2 \mid t_p \text{ and } p \mid c. \end{cases} \tag{32}$$

(2) *Moreover, for $J \subseteq I$ such that $d_{p,J} = 1$, i.e., if there exists $i \in J$ such that $p \nmid \lambda_j$. Let $J_p = \{i \in J \mid p \nmid \lambda_i\}$, let $s = \#J$, $s_p = \#J_p$ and $r_{p,J} = \#\{i \in J \mid \lambda_i$ is a quadratic non-residue modulo $p\}$. Then for $a \geq 1$, we have*

$$N_J(Q; c, p^a) = p^{(t-1)(a-1)} p^{t-t_p-s+s_p} (p-1)^{s-s_p} N_{J_p}(Q_{I_p}; c, p), \tag{33}$$

*where*

$$\begin{aligned} N_{J_p}(Q_{I_p}; c, p) =& (p-1)^{s_p} p^{t_p-s_p-1} + (-1)^{r_p} (\sqrt{p^*})^{t_p-s_p} \\ & \times \begin{cases} \left( \dfrac{A_p(s_p, r_{p,J})}{\sqrt{p^*}} \left(\dfrac{c}{p}\right) + \dfrac{B_p(s_p, r_{p,J})}{p} \right), & \text{if } 2 \nmid t_p \text{ and } p \nmid c; \\ \left( -\dfrac{A_p(s_p, r_{p,J})}{p} - \dfrac{B_p(s_p, r_{p,J})}{\sqrt{p^*}} \left(\dfrac{c}{p}\right) \right), & \text{if } 2 \mid t_p \text{ and } p \nmid c; \\ \dfrac{(1-p) B_p(s_p, r_{p,J})}{p}, & \text{if } 2 \nmid t_p \text{ and } p \mid c; \\ \dfrac{(p-1) A_p(s_p, r_{p,J})}{p}, & \text{if } 2 \mid t_p \text{ and } p \mid c. \end{cases} \end{aligned} \tag{34}$$

(3) *For $p = 2$, for $J \subseteq I$ such that $d_{2,J} = 3$, i.e. if there exists $j \in J$ such that $2 \nmid \lambda_j$, then for $a \geq 3$,*

$$N_J(Q; c, 2^a) = 2^{(t-1)(a-3)} N_J(Q; 2, 8); \tag{35}$$

*and for $1 \leq a \leq 3$,*

$$N_J(Q; c, 2^a) = 2^{(a-1)t} \cdot \#\{J \subseteq T \subseteq I \mid v_2(\sum_{i \in T} \lambda_i - c) \geq a\}. \tag{36}$$

*In particular, for $J = I$, let $c_2' = v_2(\sum_{i \in I} \lambda_i - c)$. Then*

$$N^*(Q; c, 2^a) = \begin{cases} 2^{at-a-t+3}, & \text{if } a \geq 3 \text{ and } c_2' \geq 3; \\ 2^{(a-1)t}, & \text{if } a \leq 3 \text{ and } c_2' \geq a; \\ 0, & \text{in other cases.} \end{cases} \tag{37}$$

**Remark.** For general $Q$ (reduced or not), if we replace the assumption $p \nmid \lambda_i$ for some $i \in J$ by the assumption $\min\{v_p(\lambda_i) \mid i \in I\} = \min\{v_p(\lambda_i) \mid i \in J\}$, along with Proposition 2.1(2), we get the formula for $N_J(Q; c, p^a)$ for all $c \in \mathbb{Z}$ and $a \geq 1$.

**Proof.** Part (3) follows from Theorem B(2), Part (1) is a special case of (2), and (33) follows from Theorem B(1), we just need to prove (34) in Part (2).

By the Inclusion–Exclusion Principle, we know

$$N_{J_p}(Q_{I_p}; c, p) = \sum_{T \subseteq J_p} (-1)^{|T|} N(Q_{I_p - T}; c, p).$$

We use (30) and the above formula to compute $N_{J_p}(Q_{I_p}; c, p)$. We compute the main term and the error term separately. The main term is

$$\sum_{T \subseteq J_p} (-1)^{|T|} p^{t_p - |T| - 1} = (p-1)^{s_p} p^{t_p - s_p - 1}.$$

For the error term, we need the following identities

$$\sum_{i \text{ even}} \binom{n}{i} x^i = \frac{(1+x)^n + (1-x)^n}{2},$$
$$\sum_{i \text{ odd}} \binom{n}{i} x^i = \frac{(1+x)^n - (1-x)^n}{2}.$$

In the case $t_p$ is odd and $p \nmid c$, for the subset $T$ of even order, suppose there are $i$ quadratic residues in $\{\lambda_m \mid m \in T\}$ and $j$ quadratic non-residues, the contribution of the error term in $N(Q_{I_p - T}; c, p)$ is

$$(-1)^{r_p} \left(\frac{c}{p}\right) (\sqrt{p^*})^{t_p - 1} \times (-1)^j (\sqrt{p^*})^{-i-j}.$$

So the contribution for all $T$ of even order is $(-1)^{r_p} \left(\frac{c}{p}\right) (\sqrt{p^*})^{t_p-1} \times$

$$\begin{aligned} &\sum_{i+j \text{ even}} \binom{s_p - r_{p,J}}{i} \binom{r_{p,J}}{j} (-1)^j (\sqrt{p^*})^{-i-j} \\ =&\sum_{i \text{ even}} \binom{s_p - r_{p,J}}{i} (\sqrt{p^*})^{-i} \sum_{j \text{ even}} \binom{r_{p,J}}{j} (\sqrt{p^*})^{-j} \\ &+ \sum_{i \text{ odd}} \binom{s_p - r_{p,J}}{i} (\sqrt{p^*})^{-i} \sum_{j \text{ odd}} \binom{r_{p,J}}{j} (\sqrt{p^*})^{-j}, \end{aligned}$$

which is

$$(-1)^{r_p} (\sqrt{p^*})^{t_p - s_p - 1} \left(\frac{c}{p}\right) A_p(s_p, r_{p,J}).$$

Similarly for all $T$ of odd order, the error term contribution is

$$\begin{aligned} &\frac{(-1)^{r_p}}{p} (\sqrt{p^*})^{t_p} \sum_{i+j \text{ odd}} \binom{s_p - r_{p,J}}{i} \binom{r_{p,J}}{j} (-1)^j (\sqrt{p^*})^{-i-j} \\ =&(-1)^{r_p} (\sqrt{p^*})^{t_p - s_p} \frac{B_p(s_p, r_{p,J})}{p}. \end{aligned}$$

The other three cases in (34) are obtained by the same method. □

*4.2.3. The case $t = 2$ and $p \nmid k$*

For this case, note that if $p \nmid \lambda_1$, let $\lambda_1^{-1}$ be the $p$-adic inverse of $\lambda_1$, then

$$N_J(\lambda_1 x_1^k + \lambda_2 x_2^k; c, p^a) = N_J(x_1^k + \lambda_1^{-1}\lambda_2 x_2^k; \lambda_1^{-1}c, p^a).$$

Thus we may assume

$$Q(x_1, x_2) = x_1^k + \lambda p^e x_2^k$$

such that $p \nmid \lambda$ and $e \geq 0$. We want to compute $N_J(c, p^a)$ for $J = \emptyset$, $\{1\}, \{2\}$ and $I = \{1, 2\}$, $c \in \mathbb{Z}$ and $a \geq 1$.

If $p \nmid c$ and $e = 0$, by Theorem 2.2 and note that $J_0(\chi, \chi^{-1}) = (p-1)\chi(-1)$ if $\chi \neq 1$, $= p$ if $\chi = 1$, then

$$N(c, p) = p + \sum_{\substack{\chi_1, \chi_2 \\ \chi_i^k = 1, \chi_i \neq 1}} \chi_1\chi_2(c)\chi_2(\lambda^{-1})J(\chi_1, \chi_2), \tag{38}$$

$$N(0, p) = 1 + (p-1)\sum_{\chi\colon \chi^k = 1} \chi(-\lambda). \tag{39}$$

For $J = \{1\}$ or $I$, then $d_{p,J} = 1$. By Theorem B, we have $N_J(c, p^a) = p^{a-1}N_J(c, p)$. Then by (16), we have

**Proposition 4.5.** *Let $Q(x_1, x_2) = x_1^k + \lambda p^e x_2^k$ such that $p \nmid \lambda k$ and $e \geq 0$. Then*

$$N_{\{1\}}(c, p^a) = \begin{cases} p^{a-1}(N(c,p) - \sum_{\chi\colon \chi^k=1} \chi(\lambda^{-1}c)), & \textit{if } e = 0 \textit{ and } p \nmid c; \\ p^a \cdot \sum_{\chi\colon \chi^k=1} \chi(c), & \textit{if } e \geq 1 \textit{ and } p \nmid c; \\ p^{a-1}(N(0,p) - 1), & \textit{if } e = 0 \textit{ and } p \mid c; \\ 0, & \textit{if } e \geq 1 \textit{ and } p \mid c. \end{cases} \tag{40}$$

$$N^*(c, p^a) = \begin{cases} p^{a-1}(N(c,p) - \sum_{\chi\colon \chi^k=1} (\chi(c) + \chi(\lambda^{-1}c))), & \textit{if } e = 0 \textit{ and } p \nmid c; \\ p^{a-1}(p-1) \sum_{\chi\colon \chi^k=1} \chi(c), & \textit{if } e \geq 1 \textit{ and } p \nmid c; \\ p^{a-1}(N(0,p) - 1), & \textit{if } e = 0 \textit{ and } p \mid c; \\ 0, & \textit{if } e \geq 1 \textit{ and } p \mid c. \end{cases} \tag{41}$$

*Here $N(c, p)$ and $N(0, p)$ are given by (38) and (39) respectively.*

**Remark.** In the quadratic case, Theorem 4.4 gives more precise formulas for the cases $J = \{1\}$ or $I$, or $J = \{2\}$ and $e = 0$.

For $J = \emptyset$ and $\{2\}$, the situation for $N_J(c, p^a)$ is much more complicated. We first have

**Proposition 4.6.** *Let $Q(x_1, x_2) = x_1^k + \lambda p^e x_2^k$ such that $p \nmid \lambda k$ and $e \geq 0$. For $c \neq 0$, let $c_p$ be the $p$-adic valuation of $c$ and $c' = c/p^{c_p}$. For $c = 0$, let $c_p = +\infty$. Let $J = \{2\}$ or $\emptyset$. Then*

(1) *$N_J(Q; c, p^a) = p^{a-c_p-1} N_J(Q; c, p^{c_p+1})$ for $c \neq 0$.*
(2) *If $e \geq a$, then $N_{\{2\}}(Q; c, p^a) = p^{a-1}(p-1)N(x_1^k; c, p^a)$ and $N(Q; c, p^a) = p^a N(x_1^k; c, p^a)$, and*

$$N(x_1^k; c, p^a) = \begin{cases} p^{a-\lceil \frac{a}{k} \rceil}, & \textit{if } c_p \geq a; \\ p^{c_p - \frac{c_p}{k}} \sum\limits_{\chi:\ \chi^k=1} \chi(c'), & \textit{if } k \mid c_p < a; \\ 0, & \textit{if } k \nmid c_p < a. \end{cases} \tag{42}$$

*Here $\lceil x \rceil$ meanings the smallest integer $\geq x$.*
(3) *If $e < a$, $N_{\{2\}}(Q; c, p^a) = p^{a-e-1} N_{\{2\}}(Q; c, p^{e+1})$.*

*Consequently, the study of $N_J(Q; c, p^a)$ for the set $J = \emptyset$ and $\{2\}$ is reduced to the study of $N(Q; up^a, p^{a+1})$ for $u \in \{0, \cdots, p-1\}$ and $e \leq a$, and $N_{\{2\}}(Q; up^e, p^{e+1})$ for $u \in \{0, \cdots, p-1\}$.*

**Proof.** Part (1) follows from Theorem C and Part (3) follows from Theorem B. The first half of (2) follows from Proposition 2.1(1). For the second half of (2), the solutions of $x_1^k \equiv 0 \pmod{p^a}$ are of the form $x_1 = p^{\lceil \frac{a}{k} \rceil} x_1'$ for $x_1'$ arbitrary. If $c_p < a$, then $x_1^k \equiv c \pmod{p^a}$ is solvable only if $k \mid c_p$, in this case

$$N(x_1^k; c, p^a) = p^{c_p - c_p/k} N^*(x^k; c', p^{a-c_p}) = p^{c_p - c_p/k} N^*(x^k; c', p),$$

but $N^*(x^k; c', p) = N(x^k; c', p) = \sum\limits_{\chi:\ \chi^k=1} \chi(c')$. □

For the quadratic case, we have

**Proposition 4.7.** *Let $Q(x_1, x_2) = x_1^2 + \lambda p^e x_2^2$ such that $p \nmid 2\lambda$. Then*

(1) *For $u \in \{1, \cdots, p-1\}$,*

$$N_{\{2\}}(up^e, p^{e+1}) = \begin{cases} p^{\frac{3e+1}{2}}(1 + (\frac{\lambda u}{p})), & \textit{if } 2 \nmid e; \\ p^{\frac{3e}{2}}(p - (\frac{-\lambda}{p}) - (\frac{u}{p}) - 1), & \textit{if } 2 \mid e. \end{cases} \tag{43}$$

*For $u = 0$,*

$$N_{\{2\}}(0,p^{e+1}) = \begin{cases} 0, & \text{if } 2 \nmid e; \\ p^{\frac{3e}{2}}(p-1)(1+(\frac{-\lambda}{p})), & \text{if } 2 \mid e. \end{cases} \tag{44}$$

(2) *For $u \in \{1, \cdots, p-1\}$ and $a \geq e$,*

$$N(up^a, p^{a+1}) = p^{\frac{2a+e}{2}} \cdot \begin{cases} \sqrt{p}(1+(\frac{u}{p})), & \text{if } 2 \nmid e \text{ and } 2 \mid a; \\ \sqrt{p}(1+(\frac{\lambda u}{p})), & \text{if } 2 \nmid e \text{ and } 2 \nmid a; \\ (\frac{(a-e)(p-1)}{2}(1+(\frac{-\lambda}{p}))+(p-(\frac{-\lambda}{p}))), & \text{if } 2 \mid e \text{ and } 2 \mid a; \\ \dfrac{(a-e+1)(p-1)}{2}(1+(\frac{-\lambda}{p})), & \text{if } 2 \mid e \text{ and } 2 \nmid a. \end{cases} \tag{45}$$

*For $e < a$,*

$$N(0,p^a) = \begin{cases} p^{\frac{2a+e-1}{2}}, & \text{if } 2 \nmid e; \\ p^{\frac{2a+e}{2}}(\frac{(a-e)(p-1)}{2p}(1+(\frac{-\lambda}{p}))+1), & \text{if } 2 \mid e \text{ and } 2 \mid a; \\ p^{\frac{2a+e}{2}}(\frac{(a-e+1)(p-1)}{2p}(1+(\frac{-\lambda}{p}))+1), & \text{if } 2 \mid e \text{ and } 2 \nmid a. \end{cases} \tag{46}$$

**Proof.** We use the decomposition formula in Theorem A to count the number.

(1) Take $J_1 = \{2\}$ and $J_2 = I$ in Theorem A, then the decomposition formula for $N_{\{2\}}(Q; up^e, p^{e+1})$ is

$$N_{\{2\}}(Q; up^e, p^{e+1}) = \sum_{j=0}^{e} p^{-j} N^*(p^{2j}x_1^2 + \lambda p^e x_2^2; up^e, p^{e+1}) + N^*(\lambda p^e x_2^2; up^e, p^{e+1}).$$

If $j < e/2$, $N^*(p^{2j}x_1^2 + \lambda p^e x_2^2; up^e, p^{e+1}) = 0$. If $j > e/2$,

$$\begin{aligned} N^*(p^{2j}x_1^2 + \lambda p^e x_2^2; up^e, p^{e+1}) =& p^e(p-1)N^*(\lambda p^e x_2^2; up^e, p^{e+1}) \\ =& p^{2e}(p-1)(1+(\frac{\lambda u}{p})). \end{aligned}$$

If $j = e/2$, then

$$N^*(p^{2j}x_1^2 + \lambda p^e x_2^2; up^e, p^{e+1}) = p^{2e}(p-2-(\frac{-\lambda}{p})-(\frac{u}{p})-(\frac{\lambda u}{p})).$$

Combine the results we get the formula for $N_{\{2\}}(Q; up^e, p^{e+1})$.

The decomposition formula for $N_{\{2\}}(Q; 0, p^{e+1})$ is

$$N_{\{2\}}(Q; 0, p^{e+1}) = \sum_{j=0}^{e} p^{-j} N^*(p^{2j}x_1^2 + \lambda p^e x_2^2; 0, p^{e+1}) + N^*(\lambda p^e x_2^2; 0, p^{e+1}).$$

If $j \neq e/2$, $N^*(p^{2j}x_1^2 + \lambda p^e x_2^2; 0, p^{e+1}) = 0$ and $N^*(\lambda p^e x_2^2; 0, p^{e+1}) = 0$; for $j = e/2$, $N^*(p^{2j}x_1^2 + \lambda p^e x_2^2; 0, p^{e+1}) = p^{2e}(p-1)(1+\left(\frac{-\lambda}{p}\right))$. So we get the formula for $N_{\{2\}}(Q; 0, p^{e+1})$.

(2) Take $J_1 = \emptyset$ and $J_2 = \{2\}$, then the decomposition formula for $N(Q; up^a, p^{a+1})$ is

$$N(Q; up^a, p^{a+1}) = \sum_{j=0}^{a} p^{-j} N_{\{2\}}(x_1^2 + \lambda p^{e+2j} x_2^2; up^a, p^{a+1}) + N(x_1^2; up^a, p^{a+1}).$$

If $j \geq (a+1-e)/2$, then

$$N_{\{2\}}(x_1^2 + \lambda p^{e+2j}; up^a, p^{a+1}) = p^a(p-1)N(x_1^2; up^a, p^{a+1}),$$

and $N(x_1^2; up^a, p^{a+1}) = p^{a/2}(1+\left(\frac{u}{p}\right))$ if $2 \mid a$ and 0 if $2 \nmid a$, so

$$\begin{aligned}\sum_{j \geq (a+1-e)/2} & p^{-j} N_{\{2\}}(x_1^2 + \lambda p^{e+2jx_2^2}; up^a, p^{a+1}) + N(x_1^2; up^a, p^{a+1}) \\ &= \begin{cases} p^{\frac{3a}{2}+1-\lceil \frac{a+1-e}{2} \rceil}(1+\left(\frac{u}{p}\right)), & \text{if } 2 \mid a, \\ 0, & \text{if } 2 \nmid a. \end{cases}\end{aligned}$$

If $j < (a-e)/2$, then

$$N_{\{2\}}(x_1^2 + \lambda p^{e+2j} x_2^2; up^a, p^{a+1}) = p^{a-e-2j} N_{\{2\}}(x_1^2 + \lambda p^{e+2j} x_2^2; 0, p^{e+2j+1}).$$

If $j = (a-e)/2$, then

$$N_{\{2\}}(x_1^2 + \lambda p^{e+2j} x_2^2; up^a, p^{a+1}) = N_{\{2\}}(x_1^2 + \lambda p^a x_2^2; up^a, p^{a+1}).$$

We now can just use results in (1) to obtain the formula for $N(Q; up^a, p^{a+1})$.

The decomposition formula for $N(Q; 0, p^a)$ is

$$N(Q; 0, p^a) = \sum_{j=0}^{a-1} p^{-j} N_{\{2\}}(x_1^2 + \lambda p^{e+2j} x_2^2; 0, p^a) + N(x_1^2; 0, p^a).$$

If $j \geq (a-e)/2$, then

$$\begin{aligned} N_{\{2\}}(x_1^2 + \lambda p^{e+2j} x_2^2; 0, p^a) =& p^{a-1}(p-1)N(x_1^2; 0, p^a) \\ =& p^{2a-\lceil \frac{a}{2} \rceil - 1}(p-1). \end{aligned}$$

If $j < (a-e)/2$, then $e+2j < a$ and

$$N_{\{2\}}(x_1^2 + \lambda p^{e+2j} x_2^2; 0, p^a) = p^{a-e-2j-1} N_{\{2\}}(x_1^2 + \lambda p^{e+2j}; 0, p^{e+2j+1})$$

which is given by formulas in (1). Combine these results, we get the formula for $N(Q;0,p^a)$. □

**Remark.** For completeness, let us study $N_J(Q;c,2^a)$ for $Q(x_1,x_2) = x_1^2 + 2^e\lambda x_2^2$ and $2 \nmid \lambda$. The cases $J = \{1\}$ and $\{1,2\}$ are given in part (3) of Theorem 4.4. Here we give steps to compute $N_J(Q;c,2^a)$ for $J = \{2\}$ or $\emptyset$.

(1) We first compute $N(x_1^2;c,2^a)$. Assume that $c = 2^{c_2}u$ with $u$ odd for $c \neq 0$. Then
- if $c = 0$ or $c_2 \geq a$, $N(x_1^2;0,2^a) = 2^{a-\lceil \frac{a}{2} \rceil}$;
- if $a \geq c_2 + 3$, $N(x_1^2;c,2^a) = N(x_1^2;c,2^{c_2+3})$ (by Theorem C);
- if $c_2 + 1 \leq a \leq c_2 + 3$, $N(x_1^2;c,2^a) = 2^{a-\frac{c_2}{2}-1}$ if $2 \mid c_2$ and $u \equiv 1 \pmod{2^{a-c_2}}$ or 0 if otherwise.

(2) For $J = \{2\}$, if $a > e + 3$, by Theorem B, we have

$$N_{\{2\}}(Q;c,2^a) = 2^{a-e-3}N_{\{2\}}(Q;c,2^{e+3}).$$

If $a \leq e + 3$, since $2^e x_2^2 \equiv 2^e \pmod{2^a}$ for any $x_2 \in (\mathbb{Z}/2^a\mathbb{Z})^\times$,

$$N_{\{2\}}(Q;c,2^a) = 2^{a-1}N(x_1^2;c-2^e\lambda,2^a)$$

with $N(x_1^2;c-2^e\lambda,2^a)$ be given in part (1).

(3) For $J = \emptyset$, by the decomposition formula in Theorem A, we have

$$N(Q;c,2^a) = \sum_{j=0}^{a-1} 2^{-j}N_{\{2\}}(x_1^2 + \lambda 2^{e+2j}x_2^2;c,2^a) + N(x_1^2;c,2^a),$$

where $N_{\{2\}}(x_1^2 + \lambda p^{e+2j}x_2^2;c,2^a)$ is given in part (2) and $N(x_1^2;c,2^a)$ is given in part (1).

For the general case, we have

**Proposition 4.8.** *Let $Q(x_1,x_2) = x_1^k + \lambda p^e x_2^k$ such that $p \nmid \lambda k$ and $e \geq 0$. Let $C = N(x_1^k + \lambda x_2^k;u,p)$ and $C_0^* = N(x_1^k + \lambda x_2^k;0,p) - 1$ given by (38) and (39) respectively. Then*

(1) *For $u \in \{1,\cdots,p-1\}$,*

$$N_{\{2\}}(up^e,p^{e+1}) = \begin{cases} p^{2e-[\frac{e}{k}]}\sum\chi(u), & \text{if } k \nmid e; \\ p^{\frac{(2k-1)e}{k}}(C - \sum\chi(u)), & \text{if } k \mid e. \end{cases} \tag{47}$$

*For $u = 0$,*

$$N_{\{2\}}(0,p^{e+1}) = \begin{cases} 0, & \textit{if } k \nmid e; \\ p^{\frac{(2k-1)e}{k}} C_0^*, & \textit{if } k \mid e. \end{cases} \tag{48}$$

(2) *For* $u \in \{1, \cdots, p-1\}$ *and* $a \geq e$*,*

$$N(up^a, p^{a+1}) = \begin{cases} p^{\frac{2a(k-1)+e}{k}} C + \frac{p^{\frac{2a(k-1)+e}{k}} - p^{\frac{ak+e(k-1)}{k}}}{p^{k-2}-1} C_0^*, & \textit{if } k \mid e \textit{ and } k \mid a; \\ p^{\frac{ak+e(k-1)}{k}} \cdot \frac{p^{(k-2)\lceil \frac{a-e}{k} \rceil}-1}{p^{k-2}-1} C_0^*, & \textit{if } k \mid e \textit{ and } k \nmid a; \\ p^{\frac{(2k-1)a}{k} - [\frac{a-e}{k}]} \sum \chi(u), & \textit{if } k \nmid e \textit{ and } k \mid a; \\ p^{\frac{(2k-1)a+e}{k} - [\frac{a}{k}]} \sum \chi(u), & \textit{if } k \nmid e \textit{ and } k \mid a-e; \\ 0, & \textit{otherwise.} \end{cases} \tag{49}$$

*For* $e < a$*,*

$$N(0,p^a) = \begin{cases} p^{2a - \lceil \frac{a-e}{k} \rceil + \lceil \frac{a}{k} \rceil} + p^{a+e-1-\frac{e}{k}} \cdot \frac{p^{(k-2)\lceil \frac{a-e}{k} \rceil}-1}{p^{k-2}-1} C_0^*, & \textit{if } k \mid e; \\ p^{2a - \lceil \frac{a-e}{k} \rceil + \lceil \frac{a}{k} \rceil}, & \textit{if } k \nmid e. \end{cases} \tag{50}$$

*Here the sum* $\sum$ *is over all characters* $\chi$ *such that* $\chi^k = 1$*, and* $[n]$ *means the largest integer* $\leq n$*.*

**Proof.** The proof of part (1) is similar to the proof of Proposition 4.7. We just show how to get the formulas of part (2).

Take $J_1 = \emptyset$ and $J_2 = \{2\}$, then the decomposition formula for $N(Q; up^a, p^{a+1})$ is

$$N(Q; up^a, p^{a+1}) = \sum_{j=0}^{a} p^{-j} N_{\{2\}}(x_1^k + \lambda p^{e+kj} x_2^k; up^a, p^{a+1}) + N(x_1^k; up^a, p^{a+1}).$$

If $e + kj > a$, i.e. $j \geq [\frac{a-e}{k}] + 1$, then

$$N_{\{2\}}(x_1^k + \lambda p^{e+kj}; up^a, p^{a+1}) = p^a(p-1) N(x_1^k; up^a, p^{a+1}),$$

and $N(x_1^k; up^a, p^{a+1}) = p^{a-\frac{a}{k}} \sum \chi(u)$ if $k \mid a$ and 0 if $k \nmid a$, so

$$\sum_{j=[\frac{a-e}{k}]+1}^{a} p^{-j} N_{\{2\}}(x_1^k + \lambda p^{e+kj} x_2^k; up^a, p^{a+1}) + N(x_1^k; up^a, p^{a+1})$$
$$= \begin{cases} p^{2a-\frac{a}{k}-[\frac{a-e}{k}]} \sum \chi(u), & \text{if } k \mid a, \\ 0, & \text{if } k \nmid a. \end{cases}$$

If $e + kj < a$, i.e. $j \leq \lceil \frac{a-e}{k} \rceil - 1$, then

$$N_{\{2\}}(x_1^k+\lambda p^{e+kj}x_2^k;up^a,p^{a+1})=p^{a-e-kj}N_{\{2\}}(x_1^k+\lambda p^{e+kj}x_2^k;0,p^{e+kj+1}).$$

By (48), we have

$$\begin{aligned}&\sum_{j=0}^{\lceil\frac{a-e}{k}\rceil-1} p^{-j}N_{\{2\}}(x_1^k+\lambda p^{e+kj}x_2^k;up^a,p^{a+1})\\ &\quad=\begin{cases}p^{a+e-\frac{e}{k}}\cdot\frac{p^{(k-2)\lceil\frac{a-e}{k}\rceil}-1}{p^{k-2}-1}C_0^*, & \text{if } k\mid e\\ 0, & \text{if } k\nmid e.\end{cases}\end{aligned}$$

If $e+kj=a$, i.e. $j=\frac{a-e}{k}$, then by (47) we have

$$\begin{aligned}&p^{-j}N_{\{2\}}(x_1^k+\lambda p^a x_2^k;up^a,p^{a+1})\\ &\quad=\begin{cases}p^{2a-\frac{a-e}{k}-\frac{a}{k}}(C-\sum\chi(u)), & \text{if } k\mid a \text{ and } k\mid a-e;\\ p^{2a-\frac{a-e}{k}-[\frac{a}{k}]}\sum\chi(u), & \text{if } k\nmid a \text{ and } k\mid a-e.\end{cases}\end{aligned}$$

Thus we get the formula for $N(Q;up^a,p^{a+1})$.

The decomposition formula for $N(Q;0,p^a)$ is

$$N(Q;0,p^a)=\sum_{j=0}^{a-1}p^{-j}N_{\{2\}}(x_1^k+\lambda p^{e+kj}x_2^k;0,p^a)+N(x_1^k;0,p^a).$$

If $e+kj\geq a$, i.e. $j\geq\lceil\frac{a-e}{k}\rceil$ then

$$\begin{aligned}N_{\{2\}}(x_1^k+\lambda p^{e+kj}x_2^k;0,p^a)=&p^{a-1}(p-1)N(x_1^k;0,p^a)\\ =&p^{2a-\lceil\frac{a}{k}\rceil-1}(p-1),\end{aligned}$$

so

$$\sum_{j=\lceil\frac{a-e}{k}\rceil}^{a-1}p^{-j}N_{\{2\}}(x_1^k+\lambda p^{e+kj}x_2^k;0,p^a)+N(x_1^k;0,p^a)=p^{2a-\lceil\frac{a}{k}\rceil-\lceil\frac{a-e}{k}\rceil}$$

If $e+kj<a$, i.e. $j\leq\lceil\frac{a-e}{k}\rceil-1$, then

$$N_{\{2\}}(x_1^k+\lambda p^{e+kj}x_2^k;0,p^a)=p^{a-e-kj-1}N_{\{2\}}(x_1^k+\lambda p^{e+kj}x_2^k;0,p^{e+kj+1})$$

and

**Table 1**
$N_J(c, 27)$ for $J$ nonempty.

| $c$ | 0 | 1, 26 | 3, 24 | 9, 18 | 2,4, 23,25 | 8,10, 17,19 | 6,12, 15,21 | else |
|---|---|---|---|---|---|---|---|---|
| $N^*(c,27)$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $3^6$ |
| $N_{\{1,2\}}(c,27)$ | 0 | 0 | 0 | 0 | 0 | 0 | $3^6$ | $3^6$ |
| $N_{\{1,3\}}(c,27)$ | 0 | 0 | 0 | 0 | 0 | $3^6$ | 0 | $3^6$ |
| $N_{\{2,3\}}(c,27)$ | 0 | 0 | 0 | 0 | $3^6$ | 0 | 0 | $3^6$ |
| $N_{\{1\}}(c,27)$ | 0 | 0 | 0 | $3^6$ | 0 | $3^6$ | $3^6$ | $3^6$ |
| $N_{\{2\}}(c,27)$ | 0 | 0 | $3^6$ | 0 | $3^6$ | 0 | $3^6$ | $3^6$ |
| $N_{\{3\}}(c,27)$ | 0 | $3^6$ | 0 | 0 | $3^6$ | $3^6$ | 0 | $3^6$ |

$$\sum_{j=0}^{\lceil \frac{a-e}{k}\rceil -1} p^{-j} N_{\{2\}}(x_1^k + \lambda p^{e+kj} x_2^k; 0, p^a)$$

$$= \begin{cases} p^{a+e-\frac{e}{k}-1} \cdot \frac{p^{(k-2)\lceil \frac{a-e}{k}\rceil}-1}{p^{k-2}-1} C_0^*, & \text{if } k \mid e; \\ 0, & \text{if } k \nmid e; \end{cases}$$

thus we get the formula for $N(Q; 0, p^a)$. □

**Remark.** The case $t \geq 3$ can also be computed, but the discussion is a little bit tedious.

### *4.3. The example $Q(x_1, x_2, x_3) = 9x_1 + 3x_2^3 + x_3^9$ for $p = 3$*

At last we consider the congruence equation

$$Q(x_1, x_2, x_3) = 9x_1 + 3x_2^3 + x_3^9 \equiv c \bmod 3^a, \ (a \geq 3),$$

which is not included in the algorithm.

Since for any $J \neq \emptyset$, $d_{3,J} = 3$, by Theorem B, we have

$$N_J(Q; c, 3^a) = 3^{2(a-3)} N_J(Q; c, 27).$$

After simple calculation, we then get $N_J(Q; c, 27)$ in Table 1.

For $J = \emptyset$, the map $\varphi_3 : (a_1, a_2, a_3) \mapsto Q(\alpha_1, \alpha_2, \alpha_3) \bmod 27$ from $(\mathbb{Z}/3\mathbb{Z})^3$ to $\mathbb{Z}/27\mathbb{Z}$ is found to be one-to-one. Note that any solution $(\beta_1, \beta_2, \beta_3) \in \Gamma(Q; c, 27)$ is a lifting of some $(a_1, a_2, a_3) \in \varphi_3^{-1}(c)$, but we always have

$$Q(\beta_1, \beta_2, \beta_3) = \varphi_3(a_1, a_2, a_3).$$

Thus for any $c \in \mathbb{Z}$, we have $N(Q; c, 27) = 3^6$. In fact, we have $N(Q; c, 3^a) = 3^{2a}$ for $a \leq 3$. For the case $a > 3$, we use the notation $N_{J_1,J_2}$ introduced in the remark of §3.1, then

$$N(c, 3^a) = N_{\emptyset,\{2,3\}}(c, 3^a) + N_{\{2\},\{3\}}(c, 3^a) + N_{\{3\},\{2\}}(c, 3^a) + N_{\{2,3\}}(c, 3^a).$$

We compute the right hand side term by term:

- if $c_3 = v_3(c) = 0$, then $N_{\emptyset,\{2,3\}} = N_{\{2\},\{3\}} = 0$, $N_{\{3\},\{2\}} = 3^{2a}$ for $c \equiv 1, 8, 10, 17, 19, 26 (\mathrm{mod} 27)$, and $N_{\{2,3\}} = 3^{2a}$ for $c \equiv 2, 4, 5, 7, 11, 13, 14, 16, 20, 22, 23, 25 (\mathrm{mod} 27)$ from Table 1;
- if $c_3 = 1$, then $N_{\emptyset,\{2,3\}} = N_{\{3\},\{2\}} = N_{\{2,3\}} = 0$, and $N_{\{2\},\{3\}} = 3^{2a}$;
- if $c_3 \geq 2$, $N_{\{2\},\{3\}} = N_{\{3\},\{2\}} = N_{\{2,3\}} = 0$, and $N_{\emptyset,\{2,3\}} = 3^{2a}$.

Thus we have

$$N(Q; c, 3^a) = 3^{2a}$$

for any $a > 0$.

## Acknowledgments

Research is partially supported by National Key Basic Research Program of China (Grant No. 2013CB834202) and National Natural Science Foundation of China (Grant No. 11571328).

We thank the anonymous referee for helpful comments.

## References

[1] T. Agoh, T. Shoji, Quadratic equations over finite fields and class numbers of real quadratic fields, Monatsh. Math. 125 (1998) 279–292.

[2] A. Brauer, Lösung der Aufgabe 30, Jahresber. Dtsch. Math.-Ver. 35 (1926) 92–94.

[3] C. Calderón, J.M. Grau, A.M. Oller-Marcén, L. Tóth, Counting invertible sums of squares modulo $n$ and a new generalization of Euler's totient function, Publ. Math. Debrecen 87 (1–2) (2015) 133–145.

[4] M. Deaconescu, H.K. Du, Counting similar automorphisms of finite cyclic groups, Math. Jpn. 46 (1997) 345–348.

[5] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second edition, Graduate Text in Mathematics, vol. 84, Springer Verlag, New York, 1990.

[6] M. Mollahajiaghaei, On the addition of squares of units modulo $n$, J. Number Theory 170 (2017) 35–45.

[7] H. Rademacher, Aufgabe 30, Jahresber. Dtsch. Math.-Ver. 34 (1925) 158.

[8] C.F. Sun, Z. Cheng, On the addition of two weighted squares of units mod $n$, Int. J. Number Theory 12 (7) (2016) 1783–1790.

[9] C.F. Sun, Q.H. Yang, On the sumset of atoms in cyclic groups, Int. J. Number Theory 10 (2014) 1355–1363.

[10] L. Tóth, Counting solutions of quadratic congruences in several variables revisited, J. Integer Seq. 17 (2014) 14.11.6.

[11] Q.H. Yang, M. Tang, On the addition of squares of units and nonunits modulo $n$, J. Number Theory 155 (2015) 1–12.