TẠP CHÍ KHOA HỌC
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP HỒ CHÍ MINH
Tập 21, Số 3 (2024): 468-475
Website: https://journal.hcmue.edu.vn
ISSN: 2734-9918

HO CHI MINH CITY UNIVERSITY OF EDUCATION
JOURNAL OF SCIENCE
Vol. 21, No. 3 (2024): 468-475
https://doi.org/10.54607/hcmue.js.21.3.4123(2024)

Research Article

THE NUMBER OF SOLUTIONS OF CONGRUENCE OF HOMOGENEOUS QUADRATIC POLYNOMIALS WITH PRIME MODULUS

Le Van Manh

Ho Chi Minh City University of Education, Ho Chi Minh City, Vietnam

Corresponding author: Le Van Manh – Email: 4601101084@student.hcmue.edu.vn

Received: February 01, 2024; Revised: March 04, 2024; Accepted: March 06, 2024

ABSTRACT

This research focuses on the proofs of the formula to calculate the number of solutions of the congruence $f(x_1,...,x_n) \equiv a \pmod{p}$, *where* $f(x_1,...,x_n)$ *is a homogeneous quadratic polynomial with integer coefficients and* p *is a prime (referred to as congruence of a homogeneous quadratic polynomial with prime modulus). The study studies the problem naturally through relatively elementary results, including those from number theory and quadratic forms, to construct the formula to calculate the number of solutions of the aforementioned congruence. Unlike other proofs using advanced knowledge, the research results not only provide the formula to calculate the number of solutions but also demonstrate that all solutions of a congruence of a homogeneous quadratic polynomial with prime modulus are entirely determined by applying algebraic transformations to quadratic forms.*

Keywords: congruences; quadratic forms; prime modulus

1. Introduction

Congruences is a major research direction of modern number theory. According to the fundamental theorem of number theory, every number greater than 1 is the product of some prime numbers. Therefore, studying the congruences to a modulus m can be reduced to studying the congruences to a prime modulus. The existence of a solution and the formula to calculate the number of solutions of congruence of a homogeneous quadratic polynomial with prime modulus can be derived by combining well-known results from number theory such as Chevalley's Theorem, Warning's theorem, Gauss's sum (Borevich & Shafarevich, 1966). In this paper, we present a new method for the proof. This method only relies on elementary knowledge at the undergraduate level including knowledge of quadratic forms (Bowers, 2000) and number theory (Davenport, 2008).

Cite this article as: Le Van Manh (2024). The number of solutions of congruence of homogeneous quadratic polynomials with prime modulus. *Ho Chi Minh City University of Education Journal of Science, 21*(3), 468-475.

2. Quadratic forms

This section introduces some results on quadratic forms necessary for the subsequent proofs. From now on, p is an odd prime.

Definition 2.1. *A homogeneous quadratic polynomial* over the ring $\mathbb{Z}$ is a polynomial in some variables with coefficients in $\mathbb{Z}$ and each term is of degree 2.

For a homogeneous quadratic polynomial $f(x_1,...,x_n)$ over $\mathbb{Z}$, if we consider its coefficients as elements of the field $\mathbb{Z}_p$, we get a quadratic form over the field $\mathbb{Z}_p$ and we also denote it by $f(x_1,...,x_n)$. In this case, the number of solutions to the congruence $f(x_1,...,x_n) \equiv a \pmod p$ is equal to the number of solutions of the equation $f(x_1,...,x_n) = a$ over the field $\mathbb{Z}_p$.

Note that a quadratic form in n variables over the field $\mathbb{Z}_p$ can be written as the form

$$f(x_1,...,x_n) = \sum_{\substack{1\le i\le n\\ 1\le j\le n}} a_{ij}x_i x_j \quad (1),$$

where $a_{ij} \in \mathbb{Z}_p$, $a_{ij} = a_{ji} \forall i, j$. The matrix $A = \left[a_{ij} \right]$ is the matrix of the quadratic form f. The form f in (1) can also be written as the form $f = X^T AX$ where X is the column vector of n variables and X^T denoted the transpose matrix of X. The determinant of A is called the determinant of the form f. From now on, we only consider quadratic forms over $\mathbb{Z}_p$ with nonzero determinants (these quadratic forms are called nonsingular).

Definition 2.2. (*Equivalent quadratic forms*). Two quadratic forms $f = X^T AX$ and $g = Y^T BY$ are called *equivalent* if there is a nonsingular transformation in variables which takes f to g. That means there exists a matrix C whose determinant is nonzero such that $X = CY$.

Follows from that, we have $C^T AC = B$. Therefore, if f and g are equivalent, their determinants differ by a square element of $\mathbb{Z}_p$. Moreover, the number of solutions of the equations $f = 0$ and $g = 0$ is the same.

We say that the quadratic form f represents an element α of $\mathbb{Z}_p$ if the equation $f = \alpha$ has a nonzero solution. It is clear that if f and g are equivalent, f represents α, then g also does. We have the following results.

Proposition 2.3. (*Representations of a quadratic form*). If the quadratic form f (in n variables) represents an element $\alpha \neq 0$ of $\mathbb{Z}_p$, then f is equivalent to a form of the following form

$$\alpha y_1^2 + g \quad (2),$$

where g is also a form in $n-1$ variables.

Proof. We may write f as $f = X^T AX$, where A is a symmetric matrix. Because f represents α, there exists $x = (x_1, ..., x_n)^T \neq 0$ such that $x^T Ax = \alpha$. We can find a nonsingular matrix C whose first column is x. We apply to f the linear substitution whose matrix is C and obtain an equivalent form $f' = X'^T A' X'$ of f whose matrix has α as its very first element. Now, let D be a matrix whose first column is $(1, 0, ..., 0)$ and $n-1$ last columns are column vectors which are a base of the subspace generated by the linear equation $A'[1]x = 0$, where $A'[1]$ is the first row of A'. Apply to f' the linear substitution whose matrix is D, we obtain a form of the form (2) which is equivalent to f.

With this proposition, we easily get the following result.

Corollary 2.4. Every quadratic form can be put in diagonal form by some nonsingular linear substitution.

Proposition 2.5. If the quadratic form f represents zero, then it represents every element of $\mathbb{Z}_p$.

Proof. Two equivalent quadratic forms share the same set of representations. Therefore, it suffices to consider f in diagonal form $f = a_1 x_1^2 + ... + a_n x_n^2$. Suppose that there is $(t_1, ..., t_n) \neq 0$ such that $f(t_1, ..., t_n) = 0$ or $a_1 t_1^2 + a_2 t_2^2 + ... + a_n t_n^2 = 0$, we can assume that $t_1 \neq 0$. We may write n variables $x_1, ..., x_n$ in the new variables t as $x_1 = t_1(t+1)$ and $x_i = t_i(t-1)$ $\forall 1 < i \leq n$. So that we get

$$\begin{aligned} f(t) &= a_1\left(t_1(t-1)\right)^2 + a_2\left(t_2(t+1)\right)^2 + ... + a_n\left(t_n(t+1)\right)^2 \\ &= a_1 t_1^2\left(t^2 - 2t + 1\right) + a_2 t_2^2\left(t^2 + 2t + 1\right) ... + a_n t_n^2\left(t^2 + 2t + 1\right) \\ &= \left(a_1 t_1^2 + a_2 t_2^2 + ... + a_n t_n^2\right)\left(t^2 + 1\right) + (a_1 t_1^2 - a_2 t_2^2 - ... - a_n t_n^2)2t \\ &= 4a_1 t_1^2 t. \end{aligned}$$

Consequently, the equation $f(x_1, ..., x_n) = \alpha$ $(a \neq 0)$ has at least a solution, that is $x_1 = t_1(t^* + 1)$ and $x_i = t_i(t^* - 1)$ $\forall 1 < i \leq n$, where $t^* = \alpha\left(4a_1 t_1^2\right)^{-1}$.

3. Main results

To prove the main results, firstly, we have the following lemmas.

Lemma 3.1. The quadratic form f (in n variables) represents $\alpha \neq 0$ if and only if $-\alpha y^2 + f$ represents zero. In this case, the number of solutions of the equation $f = a$ is equal to $\frac{1}{p-1}(k - l)$ with k, l are the numbers of solutions of equations $-ay^2 + f = 0$ and $f = 0$, respectively.

Proof. Left implies right is clear, it suffices to show that if $-ay^2 + f$ represents 0, then f represents α. Indeed, let $(y_0, x_1, ..., x_n) \neq 0$ such that $-\alpha y_0^{\,2} + f(x_1, .., x_n) = 0$. If $y_0 = 0$, then f represents 0, so that it represents α. Otherwise, if $y_0 \neq 0$, then $f(x_1 y_0^{-1}, ..., x_n y_0^{-1}) = \alpha$. Furthermore, for each nonzero solution $(a_1, ..., a_n)$ of the equation $f = a$, we get exactly $p-1$ distinct nonzero solutions of the equation $-ay^2 + f = 0$, that are $(y_0, y_0 a_1, ..., y_0 a_n)$ where $y_0 \in \mathbb{Z}_p \setminus \{0\}$, which are not solutions of the equation $f = 0$. Therefore, the number of solutions of the equation $f = a$ is equal to $\frac{1}{p-1}(k-l)$ with k, l are the numbers of solutions of equations $-ay^2 + f = 0$ and $f = 0$, respectively.

Lemma 3.2. If the form f (in $n \geq 2$ variables) represents zero, then it is equivalent to the form of the following type

$$y_1 y_2 + g \quad (3),$$

where g is also a form in $n-2$ variables.

Proof. Because f represents zero, f also represents 1 (by Proposition 2.5). So, f is equivalent to a form of the type $y^2 + f'$. Therefore f' represents -1 and that f is equivalent to the form of the type $y^2 - z^2 + g$ (by Lemma 3.1). Set $y_1 = y + z$ and $y_2 = y - z$, we get f equivalent to the form of the type (3).

Lemma 3.3. The equation $f(x_1, ..., x_n) = 0$, where f is a quadratic form over the field $\mathbb{Z}_p$, has a nonzero solution if $n \geq 3$.

Proof. It suffices to prove the statement for the case $n = 3$ and $f = x_1^{\,2} + x_2^{\,2} - u x_3^{\,2}$. The equation $x_1^{\,2} + x_2^{\,2} - u x_3^{\,2} = 0$ is equivalent to $x_1^{\,2} + x_2^{\,2} = u x_3^{\,2}$. Consider the set

$$S = \left\{1^2 + b^2 \mid 0 \leq b < p\right\}.$$

If S contains a multiplicity of p, say $1 + b_0^{\,2}$, then $(1, b_0, 0)$ is a nonzero solution of f. Assume that S does not contain any multiplicity of p, we have $|S| = p$. Consequently, if S only contains square numbers modulo p, then by pigeonhole principle, there exists at least $\left[\frac{p-1}{(p-1)/2} + 1\right] = 3$ elements of S, which is in the same residue class modulo p (it is not true). Using similar reasoning, if S only contain non-square numbers modulo p, we obtain that there are square and non-square numbers modulo p in S. With this remark, we can find $b_0 \in \mathbb{Z}_p \setminus \{0\}$ such that

$$\left(\frac{1+b_0^2}{p}\right)=\left(\frac{u}{p}\right),$$

so $\left(1+b_0^2\right)u^{-1}=b_1^2$ for some $b_1\in\mathbb{Z}_p$. We get a nonzero solution of f, that is $\left(1,b_0,b_1\right)$.

Lemma 3.4. The number of nonzero solutions of the equation $f=0$ when $n=2$ is $p-1+\left(\frac{-d}{p}\right)(p-1)$, where d is the determinant of f.

Proof. By Corollary 2.4, f is equivalent to the form ax^2+by^2, noting that $\left(\frac{-d}{p}\right)=\left(\frac{-ab}{p}\right)$ and the number of solutions of $f=0$ and $ax^2+by^2=0$ are the same. If $ax^2+by^2=0$ has a nonzero solution, says $x=x_0, y=y_0$, then $-ab^{-1}=(x^{-1}y)^2$. It follows that if $\left(-d/p\right)=-1$, then f does not have any nonzero solution, the statement is true. For the case $\left(-d/p\right)=1$. We write $-ab^{-1}=u^2$ for some $u\in\mathbb{Z}_p$ and

$$ax^2+by^2=0\Leftrightarrow u^2x^2=y^2\Leftrightarrow y=ux\vee y=-ux.$$

So the statement still holds for this case.

Now, we can state and prove our main results.

Theorem 3.5. The number of nonzero solutions of the congruence

$$f\left(x_1,...,x_n\right)\equiv 0\left(\mathrm{mod}\ p\right),$$

where f is a homogeneous quadratic polynomial (in n variables) over $\mathbb{Z}$, is equal to

$$\begin{cases} p^{n-1}-1+(p-1)\left(\dfrac{(-1)^{n/2}d}{p}\right)p^{n/2-1} & \text{for } n \text{ even},\\ p^{n-1}-1 & \text{for } n \text{ odd}, \end{cases}$$

where d denotes the determinant of f.

Proof. We may consider the equation $f\left(x_1,...,x_n\right)=0$ over the field $\mathbb{Z}_p$. We shall prove the case n even by induction on n as follows.

For $n=2$, by Lemma 3.4, the statement is true. For an arbitrary even number $n>2$, by Lemma 3.3, the equation $f=0$ has at least a nonzero solution. Using Lemma 3.2, f is equivalent to some form y_1y_2+g. By that, we have $d=\left(-1/4\right)d_g$, where d_g is the determinant of g, so $\left(d/p\right)=\left(-d_g/p\right)$. Consider the equation $y_1y_2+g(y_3,...,y_n)=0$ (4), we have three following cases.

For each nonzero value of y_1, for each set of values $(y_3,...,y_n)$, there uniquely exists a value y_2 which satisfies (4), that is $y_2 = -g(y_3,...,y_n)/y_1$. Therefore, we get $(p-1)p^{n-2}$ nonzero solutions of (4) in this case.

Let $y_1 = 0$, for each nonzero value a, the number of nonzero solutions of (4) for which $y_1 = 0$ and $y_2 = a$ is equal to the number of solutions of $g = 0$. Therefore, the number of nonzero solutions of (4) in the case $y_1 = 0, y_2 \neq 0$ is equal to

$$(p-1)\left(p^{n-3} + \left((-1)^{(n-2)/2} d_g / p\right) p^{(n-2)/2-1}\right).$$

In the last case, when $y_1 = y_2 = 0$, the number of nonzero solutions of (4) is equal to the number of nonzero solutions of $g = 0$ and that is equal to

$$p^{n-3} - 1 + \left((-1)^{(n-2)/2} d_g / p\right) p^{(n-2)/2-1}.$$

Combining these above cases, the number of nonzero solutions of (4) shall be equal to

$$p^{n-1} - 1 + (p-1)\left((-1)^{(n-2)/2} d_g \Big/ p\right) p^{n/2-1} = p^{n-1} - 1 + (p-1)\left((-1)^{n/2} d \Big/ p\right) p^{n/2-1}.$$

For the case n odd, we use similar reasoning by induction n.

For $n = 1$, the statement is true. For an arbitrary odd number $n > 2$, by Lemma 3.3, the equation $f = 0$ has at least a nonzero solution. Using Lemma 3.2, f is equivalent to some form $y_1 y_2 + g$. Consider the equation $y_1 y_2 + g(y_3,...,y_n) = 0$ (4), we have three following cases.

For each nonzero value of y_1, for each set of values $(y_3,...,y_n)$, there uniquely exists a value y_2 which satisfies (4), that is $y_2 = -g(y_3,...,y_n)/y_1$. Therefore, we get $(p-1)p^{n-2}$ nonzero solutions of (4) in this case.

Let $y_1 = 0$, for each nonzero value a, the number of nonzero solutions of (4) for which $y_1 = 0$ and $y_2 = a$ is equal to the number of solutions of $g = 0$. Therefore, the number of nonzero solutions of (4) in the case $y_1 = 0, y_2 \neq 0$ is equal to $(p-1)p^{n-3}$.

In the last case, when $y_1 = y_2 = 0$, the number of nonzero solutions of (4) is equal to the number of nonzero solutions of $g = 0$ and that is equal to $p^{n-3} - 1$.

Combining these above cases, the number of nonzero solutions of (4) shall be equal to

$$p^{n-1} - 1.$$

The statement is proven.

Theorem 3.6. Let a be an integer which is not divisible by p, then the number of solutions of the congruence

$$f\left(x_1,...,x_n\right)\equiv a\left(\mathrm{mod}\ p\right),$$

where f is a homogeneous quadratic polynomial (in n variables) over $\mathbb{Z}$, is equal to

$$\begin{cases} p^{n-1}-\left(\dfrac{(-1)^{n/2}d}{p}\right)p^{n/2-1} & \text{for } n \text{ even,} \\ p^{n-1}-\left(\dfrac{(-1)^{(n+1)/2}ad}{p}\right)p^{(n+1)/2-1} & \text{for } n \text{ odd,} \end{cases}$$

where d denotes the determinant of f.

Proof. We may consider the equation $f\left(x_1,...,x_n\right)=a$ over the field $\mathbb{Z}_p$.

Considering the case n even, by Theorem 3.5, the number of solutions of the equation $f=0$ is equal to $p^{n-1}-1+\left((-1)^{n/2}d\big/p\right)p^{n/2-1}$ and the number of solutions of the equation $-ay^2+f=0$ is equal to p^n-1. By Lemma 3.1, the number of solutions of the equation $f=a$ shall be equal to

$$\begin{aligned} &\frac{1}{p-1}\left(p^n-1-p^{n-1}+1-(p-1)\left((-1)^{n/2}d\big/p\right)p^{n/2-1}\right) \\ &=\frac{1}{p-1}\left(p^n-p^{n-1}-(p-1)\left((-1)^{n/2}d\big/p\right)p^{n/2-1}\right) \\ &=p^{n-1}-\left((-1)^{n/2}d\big/p\right)p^{n/2-1}. \end{aligned}$$

Considering the case n odd, with similar reasoning, the number of solutions of the equation $f=0$ is equal to $p^{n-1}-1$ and the number of solutions of the equation $-ay^2+f=0$ is equal to $p^n-1+(p-1)\left(\dfrac{(-1)^{(n+1)/2}(-a)d}{p}\right)p^{(n+1)/2-1}$. By Lemma 3.1, the number of solutions of the equation $f=a$ shall be equal to

$$\begin{aligned} &\frac{1}{p-1}\left(p^n-1+(p-1)\left(\frac{(-1)^{(n+1)/2}(-a)d}{p}\right)p^{(n+1)/2-1}-p^{n-1}+1\right) \\ &=\frac{1}{p-1}\left(p^n-p^{n-1}-(p-1)\left(\frac{(-1)^{(n+1)/2}ad}{p}\right)p^{(n+1)/2-1}\right) \\ &=p^{n-1}-\left(\frac{(-1)^{(n+1)/2}ad}{p}\right)p^{(n+1)/2-1}. \end{aligned}$$

The statement is proven.

4. Conclusion

With elementary knowledge at the undergraduate level, we stated and proved the formula to calculate the number of solutions of the congruence $f(x_1,...,x_n) \equiv a \pmod{p}$, where f is a homogeneous quadratic polynomial and p is a prime. Furthermore, the research results also demonstrate that all these solutions are entirely determined by applying algebraic transformations to quadratic forms.

- ***Conflict of Interest:*** *Author have no conflict of interest to declare.*
- ***Acknowledgement:*** *I sincerely thank Professor My Vinh Quang for giving individual guidance and support. This work was supported by HCMUE Foundation of Science and Technology.*

REFERENCES

Borevich, Z. I., & Shafarevich, I. R. (1966). *Number Theory*. Academic Press Inc.

Bowers, J. (2000). *Matrices and Quadratic Forms*. Butterworth-Heinemann.

Davenport, H. (2008). *The higher Arithmetic: An Introduction to the Theory of Numbers*. Cambridge University Press.

SỐ NGHIỆM CỦA PHƯƠNG TRÌNH ĐỒNG DƯ THUẦN NHẤT BẬC 2 THEO MODULO NGUYÊN TỐ

Lê Văn Mạnh

Trường Đại học Sư phạm Thành phố Hồ Chí Minh, Việt Nam

Tác giả liên hệ: Lê Văn Mạnh– Email: 4601101084@student.hcmue.edu.vn

Ngày nhận bài: 01-02-2024; ngày nhận bài sửa: 04-3-2024; ngày duyệt đăng: 06-3-2024

TÓM TẮT

Nội dung chính của bài báo là chứng minh công thức về số nghiệm của phương trình đồng dư $f(x_1,...,x_n) \equiv a \pmod{p}$, trong đó $f(x_1,...,x_n)$ là đa thức thuần nhất bậc 2 với hệ số nguyên và p là số nguyên tố (gọi tắt là phương trình đồng dư thuần nhất bậc 2 theo modulo nguyên tố). Nghiên cứu tiếp cận vấn đề một cách tự nhiên thông qua các kết quả tương đối sơ cấp, bao gồm các kết quả của số học và dạng toàn phương, để xây dựng công thức tính số nghiệm của phương trình đồng dư nói trên. Khác với các chứng minh khác bằng kiến thức cao cấp, kết quả của nghiên cứu không chỉ đưa ra công thức tính số nghiệm mà còn chỉ ra rằng các nghiệm của phương trình hoàn toàn được xác định thông qua việc áp dụng các biến đổi đại số cho các dạng toàn phương.

Từ khóa: phương trình đồng dư; dạng toàn phương bậc hai; modulo nguyên tố