МАТЕМАТИЧКИ ВЕСНИК
65, 3 (2013), 383–386
September 2013

оригинални научни рад
research paper

DECOMPOSITION OF AN INTEGER AS A SUM OF TWO CUBES TO A FIXED MODULUS

David Tsirekidze and Ala Avoyan

Abstract. The representation of any integer as the sum of two cubes to a fixed modulus is always possible if and only if the modulus is not divisible by seven or nine. For a positive non-prime power there is given an inductive way to find its remainders that can be represented as the sum of two cubes to a fixed modulus N. Moreover, it is possible to find the components of this representation.

1. Introduction

Any odd prime number p can be written as the sum of two squares if and only if it is of the form $p = 4k+1$, where $k \in N$. Generally, number n can be represented as a sum of two squares if and only if in the prime factorization of n, every prime of the form $4k+3$ has even exponent [2]. There is no such nice characterization for the sum of two cubes. In this paper we give an inductive method which allows to find the representation of a non-prime integer as a sum of two cubes to a given modulus.

Definition 1.1. For $N \geq 2$ let

$$\delta(N) = \frac{\#\{n \in \{1,\dots,N\} : n \equiv x^3 + y^3 \pmod{N} \text{ has a solution}\}}{N}.$$

Broughan [1] proved the following theorem.

Theorem 1.1. 1. *If* $7 \mid N$ *and* $9 \nmid N$ *then* $\delta(N) = 5/7$*;*
2. *If* $7 \nmid N$ *and* $9 \mid N$ *then* $\delta(N) = 5/9$*;*
3. *If* $7 \mid N$ *and* $9 \mid N$ *then* $\delta(N) = 25/63$*;*
4. *If* $7 \nmid N$ *and* $9 \nmid N$ *then* $\delta(N) = 1$.

In the last case $\delta(N) = 1$, and therefore, in this case any integer can be represented as a sum of two cubes to a fixed modulus N.

2010 Mathematics Subject Classification: 11A07, 11B50, 11D25
Keywords and phrases: Sum of two cubes; Diophantine equation.

By Theorem 1.1, for all N we can compute the number of its residues that can be decomposed as a sum of two cubes. In this paper we introduce the way to find these remainders and also their decompositions as a sum of two cubes to a fixed modulus N in case when we know the factorization of this number.

2. Main results

Theorem 2.1. *Let us consider an equation* $n \equiv u^3 + v^3 \pmod N$, $n \in [0, N-1]$. *Then it has solution in integers in the following congruences:*

1. $7 \mid N$, $9 \nmid N$ *and* $n \equiv 0, 1, 2, 5, 6 \pmod 7$*;*
2. $7 \nmid N$, $9 \mid N$ *and* $n \equiv 0, 1, 2, 7, 8 \pmod 9$*;*
3. $7 \mid N$, $9 \mid N$ *and* $n \equiv 0, 1, 2, 7, 8, 9, 16, 19, 20, 26, 27, 28, 29, 34, 35, 36, 37, 43, 44, 47, 54, 55, 56, 61, 62 \pmod{63}$*;*
4. $7 \nmid N$, $9 \nmid N$ *and* $\forall n \in [0, N-1]$.

Proof. For simplicity, we prove only the first case of the theorem. One can easily verify that cube of any integer number can have the following remainders modulo 7: 0, 1, 6. Therefore, the sum of two cubes can have remainders 0, 1, 2, 5, 6 modulo 7. The number of positive integers with these remainders is $(5/7) \cdot N$ in the interval $[0, N-1]$. There is no other number n for which the equation has a solution. Hence, from Theorem 1.1 the first case of Theorem 2.1 is proved. Other two cases can be proved analogously. ∎

Definition 2.1. Let us denote the set of all values of $n \in [0, N-1]$ for which $n \equiv u^3 + v^3 \pmod N$ by $A(N)$.

Theorem 2.2. *If* $(N, M) = 1$, *then* $\delta\ (MN) = \delta(M) \cdot \delta(N)$.

Proof. Suppose

$$m \equiv u^3 + v^3 \pmod M, \quad m \in [0, M-1] \tag{1}$$

$$n \equiv x^3 + y^3 \pmod N. \tag{2}$$

Let X be such that $M \mid X$ and $N \mid X - 1$. By the Chinese Remainder Theorem such an X always exists.

Let us construct X^*, A and B in the following manner

$$X^* \equiv X \cdot n - (X-1) \cdot m \pmod{MN} \tag{3}$$

$$A = X \cdot x - (X-1) \cdot u \tag{4}$$

$$B = X \cdot y - (X-1) \cdot v. \tag{5}$$

We claim that $X^* \equiv A^3 + B^3 \pmod{MN}$.

Indeed,

$$\begin{aligned}
&X^* - (A^3 + B^3) \\
&\quad \equiv X \cdot n - (X-1) \cdot m - (X^3 \cdot x^3 - (X-1)^3 \cdot u^3 + X^3 \cdot y^3 - (X-1)^3 \cdot v^3) \\
&\quad \equiv X \cdot n - (X-1) \cdot m - (X^3(x^3 + y^3) - (X-1)^3(u^3 + v^3)) \\
&\quad \equiv X \cdot (n - X^2(x^3 + y^3)) + (X-1) \cdot ((X-1)^2(u^3 + v^3) - m) \pmod{MN}.
\end{aligned}$$

Because,

$n - X^2(x^3+y^3) \equiv (x^3+y^3)(1-X)(1+X) \equiv 0 \pmod N$ and $X \equiv 0 \pmod M$

and $(N, M) = 1$, we obtain

$$X \cdot (n - X^2(x^3+y^3)) \equiv 0 \pmod{MN}.$$

Similarly,

$$(X-1)^2(u^3+v^3) - m \equiv (u^3+v^3) \cdot ((X-1)^2 - 1) \equiv 0 \pmod M$$
$$\text{and } \; X - 1 \equiv 0 \pmod N$$

which implies, as $(N, M) = 1$

$$(X-1) \cdot ((X-1)^2(u^3+v^3) - m) \equiv 0 \pmod{MN}.$$

Finally,

$$\begin{aligned} X^* - (A^3+B^3) &\equiv X \cdot (n - X^2(x^3+y^3)) + (X-1) \cdot ((X-1)^2(u^3+v^3) - m) \\ &\equiv 0 \pmod{MN}. \end{aligned}$$

For any $m \in A(M)$ and any $n \in A(N)$, there exists an $X^* \in A(MN)$. Obviously, $X^* \equiv n \pmod N$ and $X^* \equiv m \pmod M$. Thus, for different pairs (m_1, n_1) and (m_2, n_2) we cannot obtain the same X^* (by Chinese Remainder Theorem).

Now take any element X^* from the set $A(MN)$, $X^* \equiv A^3 + B^3 \pmod{MN}$. Suppose the pairs $(x, y), (u, v)$ are the solutions of the following Diophantine equation [3]:

$$A = X \cdot x - (X-1) \cdot u,$$
$$B = X \cdot y - (X-1) \cdot v.$$

If we define

$$m \equiv (u^3+v^3) \pmod M \text{ and } n \equiv (x^3+y^3) \pmod N,$$

then $X^* \equiv A^3 + B^3 \pmod{MN}$. Therefore, there is one-to-one correspondence between the elements of the set $A(MN)$ and pairs of elements from the sets $A(M)$ and $A(N)$. Hence, we have proved that $\delta(MN) = \delta(M) \cdot \delta(N)$ ■

Remark 2.1. Let us assume we are given any number K and suppose we know the representation of any element in each set $A(1), A(2), \ldots, A(K-1)$ as a sum of two cubes to a fixed modulus. And our task is to find the representation of the elements of $A(K)$. Let K be a non-prime power number and $K = M \cdot N$, where $(M, N) = 1$ and $N, M > 1$. Suppose $m \in A(M)$, $n \in A(N)$ and (1),(2) hold. Solve Diophantine equation $M \cdot q - N \cdot l = 1$, let $X = Mq$ and construct X^*, A, B according to (3),(4),(5). As it was shown above

$$X^* \equiv A^3 + B^3 \pmod K.$$

Therefore $X^* \in A(K)$ and (6) is a representation for X^* as a sum of two cubes to a fixed modulus K.

3. Conclusion

This paper is an attempt to explicitly find the way to solve the equation $n \equiv a^3 + b^3 \pmod{K}$. Using inductive method that is given in this paper it is possible to construct the set $A(K)$ and represent any element of this set as a sum of two cubes to a fixed non-prime modulus K.

Acknowledgement. The authors thank the anonymous referee for valuable comments and suggestions. Also we are very grateful for Akaki Mamageishvili's helpful discussions.

REFERENCES

[**1**] K.A. Broughan, *Characterizing the sum of two cubes*, J. Integer Seq. **6** (2003), Article 03.4.6, 7 pages.

[**2**] E. Grosswald, *Representation of Integers as Sums of Squares*, Springer, New York, 1985.

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

(received 23.08.2011; in revised form 24.02.2012; available online 10.06.2012)

David Tsirekidze, Stanford University, USA

E-mail: david19@stanford.edu

Ala Avoyan, International School of Economics (ISET), Georgia

E-mail: a.avoyan@iset.ge