Commun. Korean Math. Soc. **25** (2010), No. 2, pp. 167–171
DOI 10.4134/CKMS.2010.25.2.167

THE NUMBERS THAT CAN BE REPRESENTED BY A SPECIAL CUBIC POLYNOMIAL

Doo Sung Park, Seung Jin Bang, and Jung Oh Choi

Abstract. We will show that if d is a cubefree integer and n is an integer, then with some suitable conditions, there are no primes p and a positive integer m such that

$$d \text{ is a cubic residue } \pmod p,\ 3 \nmid m,\ p \parallel n$$

if and only if there are integers x, y, z such that

$$x^3 + dy^3 + d^2z^3 - 3dxyz = n.$$

1. Introduction

The numbers that can be represented by a quadratic polynomial $x^2 + y^2$ is well-known. For an integer n, there are integers x, y satisfying $x^2 + y^2 = n$ if and only if there are no primes p and odd positive integer m such that $p \equiv 3 \pmod 4$ and $p^m \parallel n$ [4, p. 164]. In this paper, we will study the numbers that can be represented by the cubic polynomial

$$x^3 + dy^3 + d^2z^3 - 3dxyz.$$

2. Preliminaries

For a prime p and an integer n such that $\gcd(n, p) = 1$, let n be a cubic residue $\pmod p$ if $p \equiv 1 \pmod 3$ and there are no integer solutions of

$$x^3 \equiv n \pmod p.$$

For a cubefree integer d, let R_d be the set of all algebraic integers in $\mathbb{Q}(\sqrt[3]{d})$ [3, p. 38]. For $\alpha \in R_d$ where $x, y, z \in \mathbb{Q}$ and

$$\alpha = x + y\sqrt[3]{d} + z\sqrt[3]{d^2},$$

let

$$N(\alpha) = x^3 + dy^3 + d^2z^3 - 3dxyz,\ \overline{\alpha} = (x^2 - dyz) + (dz^2 - xy)\sqrt[3]{d} + (y^2 - zx)\sqrt[3]{d^2}.$$

Received June 10, 2009.
2000 *Mathematics Subject Classification.* 11D25.
Key words and phrases. number theory.

Then for any $\alpha, \beta \in R_d$, $N(\alpha)N(\beta) = N(\alpha\beta)$, $N(\alpha) \in \mathbb{Z}$, $N(\alpha) = 0$ if and only if $\alpha = 0$, and $N(\alpha) = 1$ if and only if α is a unit in R_d [3, pp. 21–22]. Also, the following formulas

$$\alpha\overline{\alpha} = N(\alpha),\ N(\overline{\alpha}) = N(\alpha)^2,\ \overline{\overline{\alpha}} = N(\alpha)\alpha,\ \overline{\alpha\beta} = \overline{\alpha}\overline{\beta},\ \overline{\left(\frac{\alpha}{\beta}\right)} = \frac{\overline{\alpha}}{\overline{\beta}}$$

hold by explicit calculations. For a prime p and a positive integer m, let $\mathbb{F}_{p^m}$ be the finite field with order p^m [1, p. 279]. For an integral domain R, let R be a unique factorization domain if the factorization of elements in R exists and is unique up to units [1, p. 137].

3. Results and proofs

Lemma 3.1. *Assume that d is a cubefree integer, p is a prime where $p \equiv 1 \pmod 3$, and d is not a cubic residue $\pmod p$. If integers x, y, z are a solution of*

$$x^3 + dy^3 + d^2z^3 - 3dxyz \equiv 0 \pmod p,$$

then $x \equiv y \equiv z \equiv 0 \pmod p$.

Proof. A polynomial $t^3 - d$ is irreducible in $\mathbb{F}_p$, so $\mathbb{F}_{p^3}$ is a splitting field over $\mathbb{F}_p$ of the polynomial $t^3 - d$ [1, p. 280]. Consider $\mathbb{F}_{p^3}$ as $\mathbb{F}_p[t]/(t^3 - d)$ [1, p. 234]. Also, let $\alpha = x + yt + zt^2 \in \mathbb{F}_{p^3}$. Then in $\mathbb{F}_{p^3}$,

$$0 = x^3 + dy^3 + d^2z^3 - 3dxyz = N(\alpha) = \alpha\overline{\alpha}.$$

If $\alpha = 0$, then $x = y = z = 0$ in $\mathbb{F}_p$. If $\overline{\alpha} = 0$, then $x^2 = dyz$, $dz^2 = xy$, $y^2 = zx$ in $\mathbb{F}_p$. If $x = 0$ in $\mathbb{F}_p$, then $y = z = 0$ in $\mathbb{F}_p$. If $x \neq 0$ in $\mathbb{F}_p$, then in $\mathbb{F}_p$,

$$x^4 = d^2y^2z^2 = dxy^3,$$

so there is an integer m such that $m^3 = d$ in $\mathbb{F}_p$. A contradiction. □

Theorem 3.2. *Let d be a cubefree integer. Consider an integer n such that there is an integral solution of*

$$x^3 + dy^3 + d^2z^3 - 3dxyz = n.$$

Then $n = \mu^3\nu$ for some integer μ and a cubefree integer ν such that for any prime factor p of ν where $p \equiv 1 \pmod 3$, d is a cubic residue $\pmod p$.

Proof. If p is a prime factor of n such that $p \equiv 1 \pmod 3$ and d is not a cubic residue $\pmod p$, then by the previous lemma, $x \equiv y \equiv z \equiv 0$. Then $p^3 \mid n$, so

$$\left(\frac{x}{p}\right)^3 + d\left(\frac{y}{p}\right)^3 + d^2\left(\frac{z}{p}\right)^3 = \frac{n}{p^3}.$$

By iterating this argument, we see that for some positive integer m, $p^{3m} \parallel n$. It means this theorem. □

Lemma 3.3. *Let p be a prime and t an integer such that* $\gcd(t,p)=1$. *Then there are integers x,y,z such that*

$$|x|,|y|,|z|<\sqrt[3]{p},\ (x,y,z)\neq(0,0,0),\ x+ty+t^2z\equiv 0 \pmod p.$$

Proof. The number of all pairs (x,y,z) such that $0<x,y,z<\sqrt[3]{p}+1$ is bigger than p, so by the pigeonhole principle, for some integers $0<x_1,x_2,y_1,y_2,z_1,z_2<\sqrt[3]{p+1}$ such that $(x_1,y_1,z_1)\neq(x_2,y_2,z_2)$,

$$x_1+ty_1+t^2z_1\equiv x_2+ty_2+t^2z_2 \pmod p.$$

Let $x=x_1-x_2$, $y=y_1-y_2$, $z=z_1-z_2$. Then x,y,z satisfy the conditions. □

Theorem 3.4. *Let d be a cubefree integer. Assume that R_d is a unique factorization domain and for any prime $p<1+4d+d^2$ except the cases when $d\equiv 1$* (mod p) *and d is not a cubic residue* (mod p) *or when p divides d, there is an integral solution of*

$$x^3+dy^3+d^2z^3-3dxyz=p.$$

Then for any integer $n=\mu^3\nu$ where μ is an integer and ν is a cubefree integer such that d is a cubic residue (mod p) *for any prime factor p of ν where $p\equiv 1$* (mod 3)*, there is an integral solution of*

$$x^3+dy^3+d^2z^3-3dxyz=n.$$

Proof. We will first prove this theorem when n is a prime $p\geq 1+4d+d^2$. If $p\equiv 1 \pmod 3$, then d is a cubic residue . Also, $p>2,3,d$. If $p\equiv 5 \pmod 6$, then $\mathbb{F}_p^*$ is a cyclic group of order $p-1$ [1, p. 279], so there is an integer t such that $t^3\equiv d \pmod p$ because $\gcd(p-1,3)=1$. Therefore, in any cases, we can choose an integer such that $t^3\equiv d \pmod p$. Then because $\gcd(t,p)=1$, by the previous lemma, we can choose integers x_0,y_0,z_0 such that

$$|x_0|,|y_0|,|z_0|<\sqrt[3]{p},\ (x_0,y_0,z_0)\neq(0,0,0),\ x_0+ty_0+t^2z_0\equiv 0 \pmod p.$$

Then $x_0^3+dy_0^3+d^2z_0^3-3dx_0y_0z_0=kp$ for some integer k. Because $N(\alpha)\neq 0$ where

$$\alpha=x_0+y_0\sqrt[3]{d}+z_0\sqrt[3]{d^2},$$

so k is not zero. Also, $k<1+4d+d^2$. Therefore, $\gcd(k,p)=1$. Because R_d is a unique factorization domain, there are $\beta,\gamma\in R_d$ such that

$$\alpha=\beta\gamma,\ \gcd(\gamma,p)\neq 1,\ \gcd(\gamma,k)=1.$$

Then $N(\gamma)$ divides $N(p)=p^3$. If p^2 divides $N(\gamma)$, then p^2 divides $N(\alpha)=kp$. A contradiction. Therefore, $N(\gamma)$ divides p. Also, γ is not a unit, so $N(\gamma)\neq 1$. Therefore, $N(\gamma)=\pm p$, so we can choose integers x,y,z such that

$$N(x+y\sqrt[3]{d}+z\sqrt[3]{d^2})=p,$$

and then $x^3+dy^3+d^2z^3-3dxyz=p$.

Also, for any $\alpha, \beta \in R_d$, $N(\alpha\beta) = N(\alpha)N(\beta)$, and for any prime p, $N(p) = p^3$. By multiplying elements in R_d what we have earned, for an integer n satisfying the conditions, there are integers x, y, z such that

$$N(x + y\sqrt[3]{d} + z\sqrt[3]{d^2}) = n,$$

and then $x^3 + dy^3 + d^2z^3 - 3dxyz = n$. □

By combining Theorems 3.2 and 3.4, we get the following result.

Corollary 3.5. *Let n be an integer. Under the assumptions in Theorem 3.4, there is an integral solution of*

$$x^3 + dy^3 + d^2z^3 - 3dxyz = n$$

if and only if there are an integer μ and a cubefree integer ν such that $n = \mu^3\nu$ and d is a cubic residue $\pmod p$ for any prime factor of p where $p \equiv 1 \pmod 3$.

Consider the case of $d = 2$. Then R_2 is a unique factorization domain [3, p. 149], so it is easy to see that the assumptions of Theorem 3.2 is satisfied. Also, by the cubic reciprocity, for any prime p such that $p \equiv 1 \pmod 3$, 2 is a cubic residue $\pmod p$ if and only if there are integers a, b such that $p = a^2 + 27b^2$ [2, p. 210]. Therefore, we get the following easy application.

Corollary 3.6. *Let p be a prime. Then there is an integral solution of*

$$x^3 + 2y^3 + 4z^3 - 6dxyz = p$$

if and only if $p \equiv 0, 2 \pmod 3$ or $p = a^2 + 27b^2$ for some integers a, b.

Remark 3.7. We can consider other cases by same ways with some calculations and the cubic reciprocity. For the cubic reciprocity, see [2, pp. 209–234].

References

[1] T. Hungerford, *Algebra*, Holt, Rinehart and Winston, Inc., New York-Montreal, Que.-London, 1974.
[2] F. Lemmermeyer, *Reciprocity Laws*, Springer-Verlag, Berlin, 2000.
[3] D. A. Marcus, *Number Fields*, Springer-Verlag, New York-Heidelberg, 1977.
[4] I. Niven, H. S. Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc., New York, 1991.

Doo Sung Park
Department of Mathematics
California Institute of Technology
California 91125, USA
E-mail address: parkd@caltech.edu

Seung Jin Bang
Department of mathematics
Ajou University
Suwon 443-749, Korea
E-mail address: emath@naver.com

Jung Oh Choi
Saetbyeol Middle School
Gyeonggi-do 463-020, korea
E-mail address: setfree1@hanmail.net