ӘОЖ 373

КУБ ҚАЛЫНДЫНЫҢ ШЕШІМДІЛІГІ

Танатар Баягавал
agul_kz@mail.ru
Л. Н. Гумилев атындағы ЕҰУ-дың магистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші- Алгебра және геометрия кафедрасының оқытушысы, физика-математика ғылымдарының кандидаты, Ш.Ө. Абуталипова

Түйіндеме: Бұл жұмыста берілген жай модуль үшін анықталатын куб қалындыға қатысты бүтін сандар сипатталады.

Аннотация: В этой работе описываются целые числа относительно кубических вычетов определенные по простому модулю.

Abstract: This paper describes integers with respect to cubic residues defined by prime modulus.

Түйін сөздер: жай модуль, куб қалынды, Эйзенштейн бүтін сандары, Лежандр символы.

Бұл мақалада $\gamma \in \mathbb{Z}_{[\omega]}$, γ-жай сан модуль бойынша $x^3 \equiv \omega\ (mod\gamma)$ теңдеуі және $\pi \in \left(\frac{\mathbb{Z}}{5\mathbb{Z}[\omega]}\right)^*$, $x^3 \equiv \pi(mod\ 5)$ теңдеуіне қатысты есептер қарастырылған . Есептішешу үшін алдымен $\mathbb{Z}[\omega]$ сақинадағы норма, куб қалынды ұғымы мен Лежандр символының анықтамасын береміз. Алдымен жоғарыда айтылған қажетті негізгі ұғымдар мен нәтижелерді қарастырайық.

Анықтама 1. $\mathbb{Z}[\omega]$ сақинасы $a + b\omega$ түріндегі элементтерден тұрады, мұндағы $a, b \in \mathbb{Z}$, $\omega = \frac{-1+\sqrt{3}}{2}$. $\alpha = a + b\omega$ санының нормасы деп, $N(\alpha) = a^2 - ab + b^2$ санын айтамыз.

Анықтама 2. Егер $\pi \in \mathbb{Z}[\omega]$ жай сан, $N(\alpha) \neq 3$ және $\pi \nmid \alpha$ болса, онда *Лежандр символы* деп,

$$\begin{cases} \left(\frac{\alpha}{\pi}\right)_3 = 0 \text{ егер } \pi \mid \alpha \text{ болса} \\ \left(\frac{\alpha}{\pi}\right)_3 = 1 \text{ егер } x^3 \equiv \alpha(mod\ \pi) \text{ теңдеуінің шешімі бар болса} \end{cases}$$

санын айтамыз.

Анықтама 3. Егер $\pi \in \mathbb{Z}[\omega]$ жай сан, $N(\alpha) \neq 3$ және $\pi \nmid \alpha$ болсын, онда π модулі бойынша α санын куб қалынды деп айтамыз, егер:

(a) $\left(\frac{\alpha}{\pi}\right)_3 = 0$ егер $\pi \mid \alpha$ болса

(b) $\alpha^{\frac{N(\alpha)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 (mod\pi)$, мұндағы $\left(\frac{\alpha}{\pi}\right)_3 = 1,\ \omega,$ немесе ω^2 тең болса.

Теорема 1. $\pi \in \mathbb{Z}[\omega]$ жай сан, $N(\alpha) \neq 3$ және $\pi \nmid \alpha$ болсын,онда

$$\alpha^{\frac{N(\alpha)-1}{3}} \equiv \omega^m(mod\pi)$$

мұндағы $m = 0,\ 1,$ немесе 2 тең болады.

Теорема 2. Егер $\pi \in \mathbb{Z}[\omega]$ жай сан, $N(\alpha) \neq 3$ және $\pi \nmid \alpha$ болсын, онда

(a) $x^3 \equiv \alpha (mod\ \pi)$теңдеуінің шешімі бар, α куб қалынды болса, онда $\left(\frac{\alpha}{\pi}\right)_3 = 1$ тең.

(b) $\alpha^{\frac{N(\alpha)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 (mod\ \pi).$

(c) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\alpha}{\pi}\right)_3.$

(d) Егер $\alpha \equiv \beta(mod \pi)$болса, онда $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3.$

Тұжырым 1. Егер $\gamma \in \mathbb{Z}[\omega]$ жай сан, $\gamma = a + b\omega;\ \ a = 3m - 1;\ \ b = 3n;\ \ \ m, n \in \mathbb{Z}$ болса, онда

$(a)\ \left(\frac{\omega}{\gamma}\right)_3 = 1$ егер $\gamma \equiv 8\left(mod\ 3(1-\omega)\right)$ болса

$(b)\ \left(\frac{\omega}{\gamma}\right)_3 = \omega$ егер $\gamma \equiv 2\left(mod\ 3(1-\omega)\right)$ болса

$(c)\ \left(\frac{\omega}{\gamma}\right)_3 = \omega^2$ егер $\gamma \equiv 5\left(mod\ 3(1-\omega)\right)$ болса

болатын көрсет.

Дәлелдеуі: Алдымен γ жай санын түрлендіру арқылы:

$$\gamma = a + b\omega = -1 + 3(m + n\omega) \text{ санын аламыз.}$$

γ санын $(1-\omega)$ саны бойынша модуль аладын болса, онда

$$\gamma \equiv -1 + 3(m+n)(mod\ (1-\omega)) \text{ тең екені анық.}$$

(a)-дағы шарты бойынша $8 = -1 + 3(m+n)$тең. Демек $\gamma = -1 + 9\omega$тең болады. (теорема 1) және (теорема 2) бойынша $\omega^{\frac{N(\alpha)-1}{3}} \equiv \left(\frac{\omega}{\gamma}\right)_3 (mod\gamma)$тең болады, онда $N(\alpha) = 73,$

$\frac{N(\alpha)-1}{3} \equiv\ 0(mod\ 3)$ тең, осыдан $\left(\frac{\omega}{\gamma}\right)_3 = 1$ тең екені шығады.

(b)-дағы шарты бойынша $2 = -1 + 3(m+n)$ тең. Демек $\gamma = -1 + 3\omega$ тең болады. (теорема 1) және (теорема 2) бойынша $\omega^{\frac{N(\alpha)-1}{3}} \equiv \left(\frac{\omega}{\gamma}\right)_3 (mod\gamma)$ тең болады, онда $N(\alpha) = 13,$

$\frac{N(\alpha)-1}{3} \equiv\ 1(mod\ 3)$ тең, осыдан $\left(\frac{\omega}{\gamma}\right)_3 = \omega$ тең екені шығады.

(c)-дағы шарты бойынша $5 = -1 + 3(m+n)$ тең. Демек $\gamma = -1 + 6\omega$ тең болады. (теорема 1) және (теорема 2) бойынша $\omega^{\frac{N(\alpha)-1}{3}} \equiv \left(\frac{\omega}{\gamma}\right)_3 (mod\gamma)$ тең болады, онда $N(\alpha) = 43;\ \ \frac{N(\alpha)-1}{3} \equiv\ 2(mod\ 3)$ тең, осыдан $\left(\frac{\omega}{\gamma}\right)_3 = \omega^2$ тең екені шығады.

Тұжырым 2. Егер $\pi \in \left(\frac{\mathbb{Z}}{5\mathbb{Z}[\omega]}\right)^*,\ \ \pi$ куб қалынды болса, онда

$\pi \equiv 1,\ 2,\ 3,\ 1+2\omega,\ 2+4\omega,\ 3+\omega$ және $4 + 3\omega\ (mod\ 5)$ санға тең екенін көрсет.

Дәлелдеуі: (теорема 1) және (теорема 2) бойынша $\pi^{\frac{N(5)-1}{3}} \equiv \left(\frac{\pi}{5}\right)_3 (mod\ 5)$ тең болады.

$\pi \equiv 1(mod\ 5)$ немесе $\pi = 1$ болса, онда куб қалынды болатыны анық.

$\pi \equiv 2(mod\ 5)$ немесе $\pi = 2$ және $N(5) = 25$ болса, онда $\pi^{\frac{N(5)-1}{3}} \equiv 2^8 \equiv 1(mod\ 5)$,

$\pi \equiv 3(mod\ 5)$ немесе $\pi = 3$ болса, онда $3^8 \equiv 1(mod\ 5)$,

$\pi \equiv 1 + 2\omega(mod\ 5)$ немесе $\pi = 1 + 2\omega$ болса, онда $(1 + 2\omega)^8 \equiv (-3)^4 \equiv 1(mod\ 5)$,

$\pi \equiv 2 + 4\omega(mod\ 5)$ немесе $\pi = 2 + 4\omega = 2(1 + 2\omega)$ болса, онда $2^8 \cdot (1 + 2\omega)^8 \equiv 1(mod\ 5)$,

$\pi \equiv 3 + \omega(mod\ 5)$ немесе $\pi = 3 + \omega$ болса, онда $(3 + \omega)^8 \equiv 3^4 \equiv 1(mod\ 5)$,

$\pi \equiv 4 + 3\omega(mod\ 5)$ немесе $\pi = 4 + 3\omega$ болса, онда $(4 + 3\omega)^8 \equiv (-3)^4 \equiv 1(mod\ 5)$,

осыдан (теорема 2) бойынша π саны куб қалынды болатыны көрсетілді.

Пайдаланылған әдебиеттер тізімі:

1. *J.G.I. Noordsij, Primes of the form $x^2 + ny^2$,Mathematical Institute, Leiden UniversityJune 26, 2015.*
2. *С.А.Бадаев, Сызықтық алгебра мен аналитикалық геометрия. Алматы: Қазақ университеті, 2010.-258 б.*
3. *WissamRaji, An Introductory Course in ElementaryNumber Theory. July 2013*
4. *Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. Мир,1987.-416 с.*
5. *Suzanne Rousseau, Quadratic and cubic reciprocity,Eastern Washington University. 2012.*