ӘОЖ 373

ЖАЙ МОДУЛЬ БОЙЫНША ҚАЛЫНДЫЛАРДАҒЫ КВАДРАТ ҮШМҮШЕНІҢ ТҮБІРЛЕРІНІҢ САНЫ

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 квадрат қалындыға қатысты Гаусс леммасын қолданып, бүтін сандардағы квадрат үшмүшенің түбірлері сипатталады.

Аннотация: В этой работе описываются корни квадратного трехчлена в целых числах с использованием леммы Гаусса, рассматривающая квадратичные вычеты по простому модулю.

Abstract: This paper describes the roots of a quadratic trinomial in integers using Gauss's lemma, which considers quadratic residues modulo prime.

Түйін сөздер: жай модуль, квадрат қалынды, Эйлер критерийі, Лежандр символы, Гаусс леммасы.

Бұл мақалада a саны мен p жай модуль үшін $ax^2 + bx + c \equiv 0(mod\ p)$ теңдеуі түбірлерін табуға байланысты есеп қарастырылады. Есепті тұжырымдау үшін алдымен квадрат қалынды ұғымы мен Лежандр символының анықтамасы, содан кейін квадрат қалындының Эйлер критерийі мен олардың саны жайлы Гаусс леммасын береміз. Жұмыстың өн бойында a мен p бүтін сандары өзара жай дегенді $(p, a) = 1$ теңдігімен белгілейтін боламыз. Алдымен жоғарыда айтылған қажетті негізгі ұғымдар мен нәтижелерді қарастырайық.

Анықтама 1. $p, a \in \mathbb{Z}$ және $(p, a) = 1$ болсын. Онда

1. $x^2 \equiv a(modp)$ теңдеуінің шешімі бар болса, a санын *квадрат қалынды* деп атаймыз.

2. $x^2 \equiv a(modp)$ теңдеуінің шешімі жоқ болса, a санын *квадрат қалынды* емес деп атаймыз.

Анықтама 3. $p \neq 2$ жай сан болсын, онда *Лежандр символы* деп,

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{егер } a \text{ саны 0 немесе } p \text{ болса} \\ 1, & \text{егер } a \text{ саны } \textit{квадрат қалынды болса} \\ -1, & \text{егер } a \text{ саны } \textit{квадрат қалынды бол маса} \end{cases}$$

санын айтамыз.

Теорема 3. Егер $p \neq 2$ жай сан болса, онда дәл $\frac{(p-1)}{2}$ квадрат қалынды және $\frac{(p-1)}{2}$ квадрат емес қалынды болады.

Теорема 4. *(Эйлер критериі)* Егер $p \neq 2$ жай сан, a бүтін оң сан және $(p, a) = 1$ болса, онда

$$\left(\frac{a}{p}\right) \equiv a^{\frac{\varphi(p)}{2}}(modp),$$

мұндағы $\varphi(p)$ Эйлер функциясының p нүктесіндегі мәні.

Лемма 4. *(Гаусс леммасы)* $p \neq 2$ жай саны және $(p, a) = 1$ болсын. Егер $a; 2a; 3a; \ldots; \left(\frac{p-1}{2}\right)a$ оң қалындылары және $\frac{p}{2}$ санынан үлкен болатын қалындылар санын k болса, онда $\left(\frac{a}{p}\right) = (-1)^k$ тең болады.

Енді жұмыстың негізгі нәтижесіне көшейік.

Тұжырым. Егер $p \nmid a$ болса, онда

$$ax^2 + bx + c \equiv 0(modp) \qquad (1)$$

теңдеудің түбірлер саны $1 + \left(\frac{b^2-4ac}{p}\right)$ болады.

Дәлелдеуі: (1) теңдеудің сол жағын түрлендіріп, оған мәндес

$$4a^2\left(x + \frac{b}{2a}\right)^2 \equiv (b^2 - 4ac)(mod\ p),$$

$$\left(2a\left(x + \frac{b}{2a}\right)\right)^2 \equiv (b^2 - 4ac)(mod\ p). \qquad (2)$$

теңдеуді аламыз. Лежандр символы бойынша егер (2) теңдеудің шешімі бар болса, онда $\left(\frac{b^2-4ac}{p}\right) = 1$ немесе $\left(\frac{b^2-4ac}{p}\right) = 0$ деген сөз. Демек (2) теңдеудің түбірлер саны $1 + \left(\frac{b^2-4ac}{p}\right) = 2$ немесе $1 + \left(\frac{b^2-4ac}{p}\right) = 1$ екені түсінікті. Ал егер (2) теңдеудің шешімі жоқ болса, онда $\left(\frac{b^2-4ac}{p}\right) = -1$ деген сөз. Демек (2) теңдеудің түбірлер саны $1 + \left(\frac{b^2-4ac}{p}\right) = 0$ тең және (2) теңдеудің түбірі жоқ. Осыдан (1) теңдеудің түбірлер саны $1 + \left(\frac{b^2-4ac}{p}\right)$ болатындығы шығады.

Тұжырым 2: Егер $p, a \in \mathbb{Z}$ болса, онда

$$x^2 - y^2 \equiv a(mod\ p) \qquad (3)$$

теңдеуінің түбірлер саны

$$\sum_{k=0}^{p-1}\left(1+\left(\frac{k^2+a}{p}\right)\right) \qquad (5)$$

тең болады.

Дәлелдеуі: (3) теңдеуін түрлендіру арқылы оған мәндес

$$x^2 \equiv (y^2-a)(mod\ p) \qquad (4)$$

теңдеуін аламыз. (4) теңдеуінің түбірлер саны $1+\left(\frac{y^2+a}{p}\right)$ тең екені анық. $y \equiv k(mod\ p)$, мұндағы $k=\{0;1;2;\dots(p-1)\}$ сандар ретінде алатын болсақ, онда (4) теңдеуінің түбірлер саны (5) тең екені анық. Демек (3) теңдеуінің түбірлер сан (5) тең екені шығады.

Тұжырым 3: (3) теңдеуінің түбірлер бар болған жағдайда оның саны:

(a) Егер $p \nmid a$ болса, онда дәл $p-1$ тең,

(b) Егер $p \mid a$ болса, онда дәл $2p-1$ тең болады.

Дәлелдеуі: (3) теңдеуін түбірлер саны (5) тең екенін білеміз.

(a) Егер $p \nmid a$ болса, онда $y \equiv k(mod\ p)$, мұндағы $k=\{0;1;2;\dots(p-1)\}$ сандар ретінде алатын болсақ, онда теорема 3 бойынша (4) теңдеуінің шешімдері болатын $\frac{p-1}{2}$ сан бар екені анық және (4) теңдеуінің шешімі бар болса, онда екі түбірі болатынын білеміз. Демек (3) теңдеуінің түбірлер саны

$$\sum_{k=0}^{p-1}\left(1+\left(\frac{k^2+a}{p}\right)\right)=2\cdot\frac{(p-1)}{2}=(p-1)$$

санға тең болады.

(b) Егер $p \mid a$ болса, онда (4) теңдеуін түрлендіру арқылы оған мәндес

$$x^2 \equiv y^2(mod\ p) \qquad (6)$$

теңдеуін аламыз. (6) теңдеуінің шешімдері болатын p сан бар екені анық және $y \equiv 0(mod\ p)$ болғанда (6) теңдеуінің бір түбірі болады және $k=\{1;2;\dots(p-1)\}$ болған кезде (6) теңдеуінің екі түбірі болатынын білеміз. Демек (3) теңдеуінің түбірлер саны

$$\sum_{k=0}^{p-1}\left(1+\left(\frac{k^2+a}{p}\right)\right)=1+\sum_{k=1}^{p-1}\left(1+\left(\frac{k^2+a}{p}\right)\right)=1+2(p-1)=2p-1$$

санға тең болады.

Пайдаланылған әдебиеттер тізімі:

1. *Kyle Miller, Quadratic residues and quadratic nonresidues, Feb 17, 2017.*
2. *С.А.Бадаев, Сызықтық алгебра мен аналитикалық геометрия. Алматы: Қазақ университеті, 2010.-258 б.*
3. *Wissam Raji, An Introductory Course in Elementary Number 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.*