МАТЕМАТИЧКИ ОМНИБУС, 5 (2019), 105 – 129
http://im-pmf.weebly.com/matematicki-omnibus-kniga-5.html

БИНАРНИ КВАДРАТНИ ФОРМИ

Адмир Хусеини [1]

1 ВОВЕД

Во овој труд ќе презентираме неколку теореми во врска со бинарните квадратни форми. Направен е избор на резултати, критериуми за еквиваленција помеѓу две форми и нивна редукција на минимални форми. Доказите се елементарни и се засноваат врз основни факти за групи на матрици.

Со добиените резултати ќе може да се даде одговор на прашањето за претставување на простите броеви преку бинарни квадратни форми. Со дадени целобројни коефициенти a, b, c и непознати x, y може да се дефинира квадратната форма $q(x, y)$. Ако p е прост број, тогаш се бараат сите парови $\binom{x}{y} \in \mathbb{Z}^2$, кои ја задоволуваат равенката

$$p = q(x, y) = ax^2 + bxy + cy^2$$

Ова е интересен проблем на класичната теорија на броеви, којшто добива дефинитивно решение со оваа теорија.

Иако квадратните форми се предмет на разгледување на класичната теорија на броеви, денес тие наоѓаат примена во криптографијата. Еден од најпопуларните алгоритми во полето на криптографија, RSA алгоритмот за енкриптирање со јавни клучеви гарантира сигурност на енкриптираните податоци поради фактот дека факторизирањето на даден цел број како производ на прости броеви е тежок проблем. Некои од најефикасните алгоритми за наоѓање на прости делители на даден цел број или доказ дека даденият број е прост, се засноваат на теоремите и методите на претставување на даден број преку бинарна квадратна форма, [2].

Целта на овој труд е да се даде елементарен приказ на бинарните квадратни форми преку решавање на класичниот проблем на претставување на прост број како сума на квадрати или преку квадратна форма. Некои од класичните проблеми од теоријата на броеви кои се релевантни за нас се:

Проблем 1. Најдете ги сите претставувања на природниот број n како **сума на два квадрати,** каде x, y се цели броеви

$$n = x^2 + y^2$$

Квадратните форми кои може да се запишат како $q(x, y) = x^2 + k \cdot y^2$ каде k е даден цел број се нарекуваат *основни форми*.

Проблем 2. Кои прости броеви p може да се претстават со основни форми: $p = x^2 + 2y^2$, $p = x^2 + 3y^2$, $p = x^2 + 5y^2$.

Во теоријата за редукција на бинарни квадратни форми, овие проблеми се ставени во поширок контекст. Поединечните решенија се добиваат како специјални случаи на општите резултати, од кои може да се конструираат и конкретни алгоритми.

2 ИСТОРИСКИ ЗАБЕЛЕШКИ

Иако проблемот на претставување на даден прост број како сума на два квадрати се древни, тие се познати по името на францускиот математичар **Пијер Ферма** (Pierre Fermat, 1607 - 1665). Тој бил кралски советник во Парламентот на Тулуз, позиција која во денешни услови може да се опише како висок службеник во државната администрација. Очигледно, професијата на Ферма му го обезбедила слободното време потребно за да се занимава со математика. Иако не бил професионален математичар, неговите придонеси кон математиката се значајни.

Неговиот стил на работа бил бавен, писмата кои ги содржат сите неговите важни резултати од теријата на броеви се лаконски и суви. Поголемиот дел од нив биле упатени на математичарот Мерсен. Ферма никогаш не ги запишувал доказите на својствата и теоремите, само еднаш го има опишано својот метод на докажување. Поради ова е тешко да се одреди што Ферма навистина докажал и кои тврдења биле претпоставки врз основа на делумни резултати или нумерички пресметувања. Се покажало дека голем дел од неговите тврдења не може да се докажат лесно, дури и првокласни математичари како Ојлер, имале големи тешкотии со нив. Некои од познатите тврдења на Ферма поврзани со квадратните форми се:

Сума на два квадрати. Секој прост број p од облик $p = 4n + 1$, каде што $n \in \mathbb{N}$ може да се запише како сума на два квадрати $p = x^2 + y^2$, каде што $x, y \in \mathbb{Z}$.

Извадок од писмо до Паскал во 1654:

Секој прост број p од облик $p = 3n + 1$, каде што $n \in \mathbb{N}$ може да се запише како $p = x^2 + 3y^2$, каде $x, y \in \mathbb{Z}$.

Секој прост број p од облик $p = 8n + 1$ или $p = 8n + 3$, каде што $n \in \mathbb{N}$ може да се запише како $p = x^2 + 2y^2$, каде што $x, y \in \mathbb{Z}$.

Францускиот математичар **Жозеф Луи Лагранж** (Joseph Louis Lagrange, 1736 – 1813) бил првиот кој дал докази за повеќе својства на Ферма. Голем број на техниките кои ги развил за оваа цел биле негови оригинални откритија. Неговиот најважен труд од теоријата на броеви, кој е релевантен за нас е „Истражувања по аритметика“ (Recherches d'arithmetique) објавен во 1773 година [3].

Во оваа дело го имаме првото систематско и кохерентно развивање на комплетната аритметичка теорија на бинарните квадратни форми која оди многу подалеку од индивидуалните проблеми на Ферма и Ојлер. Од општата теорија тој меѓу другото, ги дедуцирал и теоремите на Ферма за претставување на простите броеви во форма $x^2 + 2y^2$ и $x^2 + 3y^2$.

На сликата прикажана подолу може да се види во оригинал секцијата каде што го решава проблемот на пресметување на новите коефициенти на квадратната форма после линеарна трансформација на коефициентите.

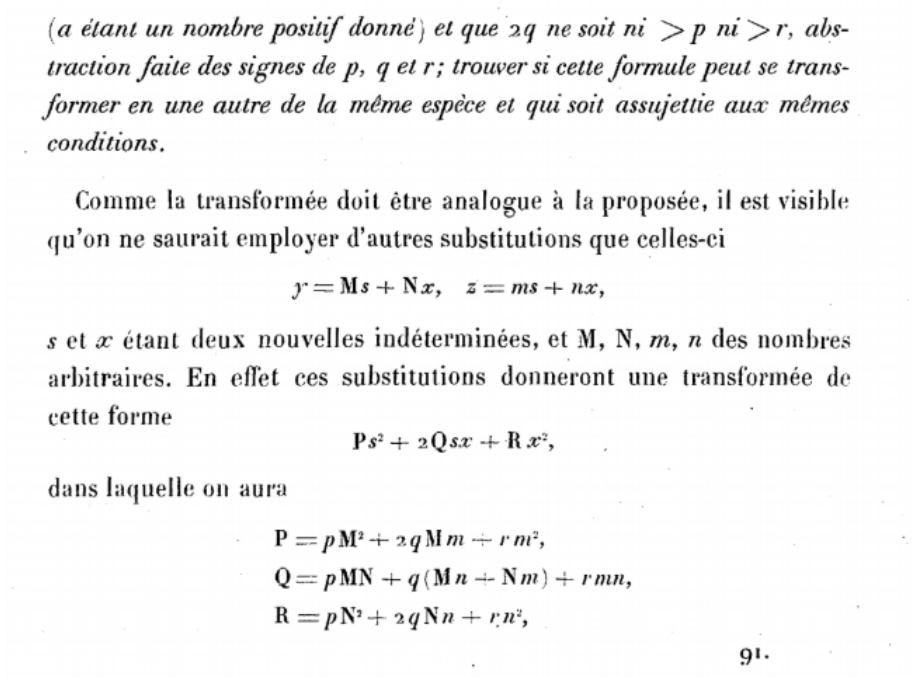
PROBLÈME III.

22. *Étant donnée la formule*

$$py^2 + 2qyz + rz^2,$$

dans laquelle y *et* z *sont des nombres indéterminés et* p, q, r *sont des nombres positifs ou négatifs, déterminés par ces conditions, que*

$$pr - q^2 = a$$



(a étant un nombre positif donné) et que 2q ne soit ni $>p$ ni $>r$, abstraction faite des signes de p, q et r; trouver si cette formule peut se transformer en une autre de la même espèce et qui soit assujettie aux mêmes conditions.

Comme la transformée doit être analogue à la proposée, il est visible qu'on ne saurait employer d'autres substitutions que celles-ci

$$y = \mathrm{M}s + \mathrm{N}x, \quad z = ms + nx,$$

s et x étant deux nouvelles indéterminées, et M, N, m, n des nombres arbitraires. En effet ces substitutions donneront une transformée de cette forme

$$\mathrm{P}s^2 + 2\mathrm{Q}sx + \mathrm{R}x^2,$$

dans laquelle on aura

$$\mathrm{P} = p\mathrm{M}^2 + 2q\mathrm{M}m + rm^2,$$
$$\mathrm{Q} = p\mathrm{MN} + q(\mathrm{M}n + \mathrm{N}m) + rmn,$$
$$\mathrm{R} = p\mathrm{N}^2 + 2q\mathrm{N}n + rn^2,$$

91.

Слика 1. Слика од страницата 91 на книгата „Истражувања по аритметика“ на Лагранж, [3].

Неговите трудови се напишани во „модерен“ математички стил. Тие се многу читливи, па дури и претставуваат пример за јасна и добро организирана презентација. Лагранж ја развива теоријата на бинарни квадратни форми во речиси истата форма како што ќе биде презентирана во овој труд. За илустрација да дадеме превод од извадок од првата страница на неговиот труд „Истражувања по аритметика“ објавен во 1773:

Овие истражувања се однесуваат на броевите кои може да се напишат во формата

$$Bt^2 + Ctu + Du^2$$

каде B, C, D се цели броеви и t, u се исто така цели броеви, но променливи.

Јас ќе ги определам оние форми кои претставуваат броеви чии делители можат да бидат претставени на ист начин. Подоцна ќе дадам техника која ни дозволува да се намалат овие форми на нивниот најмал број. Ова ќе не доведе до табела за практична употреба: Ќе

покажам како да се користи оваа табела во истражувањето на делители на даден број.

Конечно ќе дадам докази за неколку теореми за прости броеви од формата $Bt^2 + Ctu + Du^2$; некои од овие теореми се познати, но без доказ, а други се сосема нови.

3 БИНАРНИ КВАДРАТНИ ФОРМИ

Функцијата $q(x, y) = ax^2 + bxy + cy^2$ каде што x, y се целобројни променливи, a, b, c се цели броеви се вика *бинарна целобројна квадратна форма* и се запишува како

$$q = (a, b, c).$$

Ако за даден цел број *n* равенката

$$n = q(x, y) = ax^2 + bxy + cy^2$$

има целобројно решение (x, y), тогаш ќе велиме дека (x, y) *го претставува бројот* n *преку* q.

Многу проблеми поврзани со теоријата на квадратни форми се упростуваат, кога ќе се примети дека секоја целобројна форма може да се претстави преку симетрична 2×2 матрица со цели елементи (т.е. матрица во $\mathbb{Z}^{2\times 2}$).

За дадена целобројна форма $q = (a, b, c)$, матрицата $M(q)$ на q се дефинира преку

$$M(q) = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

и квадратната форма може да се претстави како

$$q(x, y) = (x, y)\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

или во пократка форма

$$q(x, y) = v^T M v,$$

каде што $v^T \in (\mathbb{Z}^2)^*$ го претставува транспонираниот вектор на $v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2$, додека со $(\mathbb{Z}^2)^*$ се означува дуалниот векторски простор на $\mathbb{Z}^2$.

Детерминантата на матрицата $M(q)$ помножена со -4 го дава $\Delta(q)$

$$\Delta(q) = -4\det\big(M(q)\big) = b^2 - 4ac$$

и се нарекува *дискриминанта* на q којашто игра важна улога во класификацијата на квадратните форми. Првата груба класификација на формите е според вредностите, кои можат да ги добијат.

Формата q се нарекува *позитивно* односно *негативно дефинитна* ако за секој вектор $\binom{x}{y} \in \mathbb{Z}^2 \setminus (0,0)$ вредноста на $q(x,y)$ е *позитивна* односно *негативна***.** Формата q се нарекува *индефинитна* ако постојат вектори $\binom{x}{y} \in \mathbb{Z}^2$ за кои $q(x,y)$ добива позитивни вредности и вектори $\binom{x}{y} \in \mathbb{Z}^2$ за кои $q(x,y)$ добива негативни вредности**.**

Формата q е позитивно односно негативно дефинитна ако и само ако важи $\Delta(q) < 0$ и $a > 0$ односно $\Delta(q) < 0$ и $a < 0$. Формата q е индефинитна ако и само ако важи $\Delta(q) \geq 0$**.**

Се гледа дека критериумот за дефинитност на квадратна форма е многу сличен со аналогниот критериум за квадратни равенки. Оваа сличност не е случајна, бидејќи $q(x,y)$ е хомоген полином од втор степен и со смената $t = x/y \in \mathbb{Q},\ y \neq 0$ може да се сведе на формата

$$q(x,y) = y^2(at^2 + bt + c) = y^2 p(t).$$

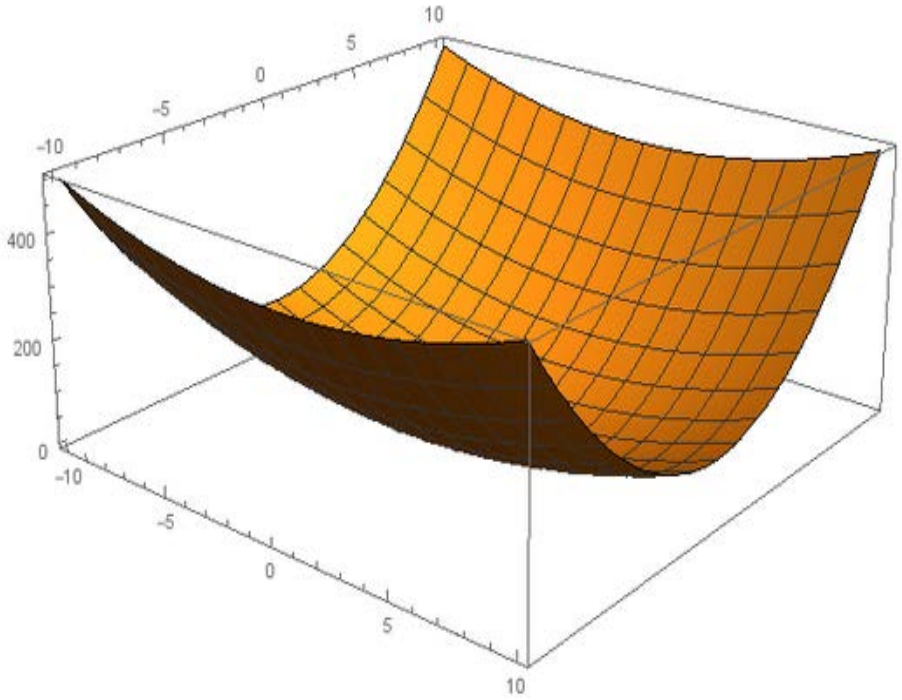
Јасно е дека $y^2 > 0$, а знакот на полиномот $p(t) \in \mathbb{Q}[t]$ зависи од вредноста на дискриминанатата Δ, каде со $\mathbb{Q}[t]$ се назначува полето на полиноми со една непозната t и рационални коефициенти.

3.1 ГЕОМЕТРИЈАТА НА КВАДРАТНИТЕ ФОРМИ

Пред да се продолжи со трансформацијата на квадратните форми и нивните класи на еквиваленција, би било убаво да се стекнеме со геометриска слика за нив. Сликите на квадратната форма може лесно да се визуализираат со компјутерскиот програм *Wolfram Mathematica* [6]. За генерирање на сликите во овој труд, користена е бесплатната веб верзија *Wolfram Programming Cloud* [7].

Графикот на реалната функција $q(x,y) = x^2 + 4y^2$ е даден на Слика 2

```
Plot3D[{x^2+4*y^2}, {x, -10, 10}, {y, -10, 10}]
```

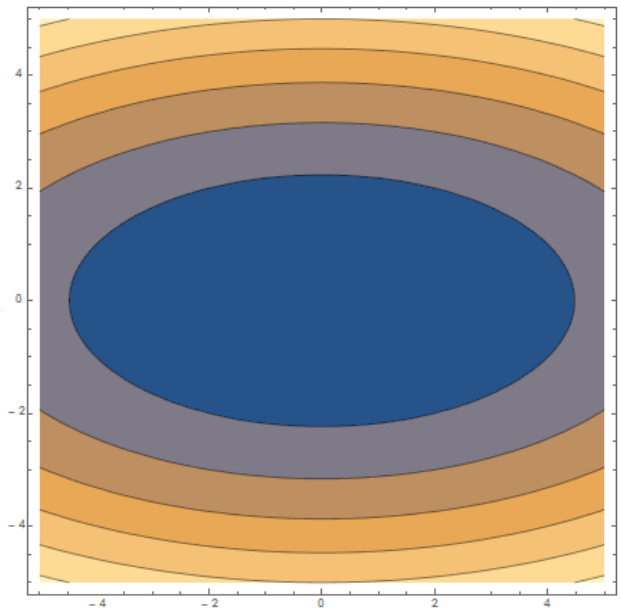


Слика 2. График на позитивно дефинитна форма.

Се гледа јасно дека во овој случај графикот е параболоид и неговите пресеци со рамнините $x =$ const. како и $y =$ const. претставуваат параболи. За нас поинтересни и порелевантни се пресеците на графикот со хоризонталната рамнина $z =$ const. Овие пресеци се визулизираат со помош на контурни цртежи како на Слика 3:

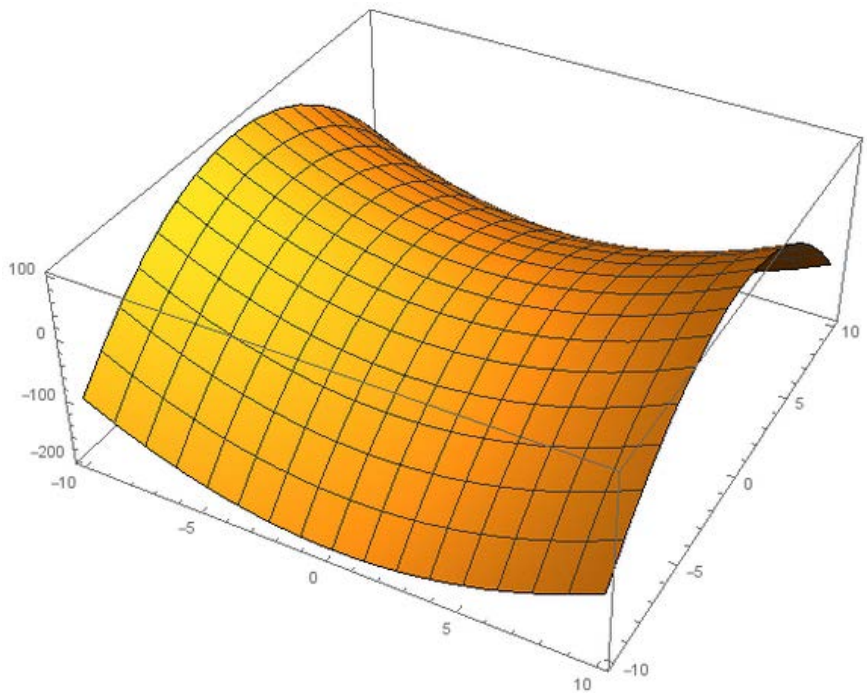
Се гледа јасно дека пресеците претставуваат елипси дадени со равенките $x^2 + 4y^2 =$ const. Ова е типичен случај на позитивно дефинитна форма, додека индефинитната форма $q(x,y) = x^2 - 2y^2$ изгледа како на Слика 4, со контурни цртежи како на Слика 5.

```
ContourPlot[{x^2 + 4*y^2}, {x, -5, 5}, {y, -5, 5}]
```



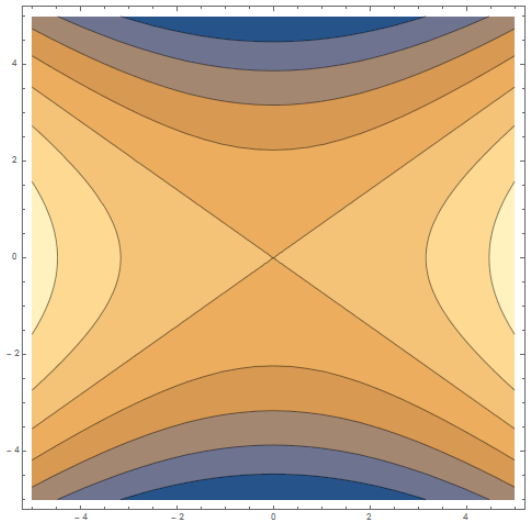
Слика 3. Контурни цртежи на позитивно дефинитна форма.

```
Plot3D[{x^2 - 2*y^2}, {x, -10, 10}, {y, -10, 10}]
```



Слика 4. График на индефинитна форма.

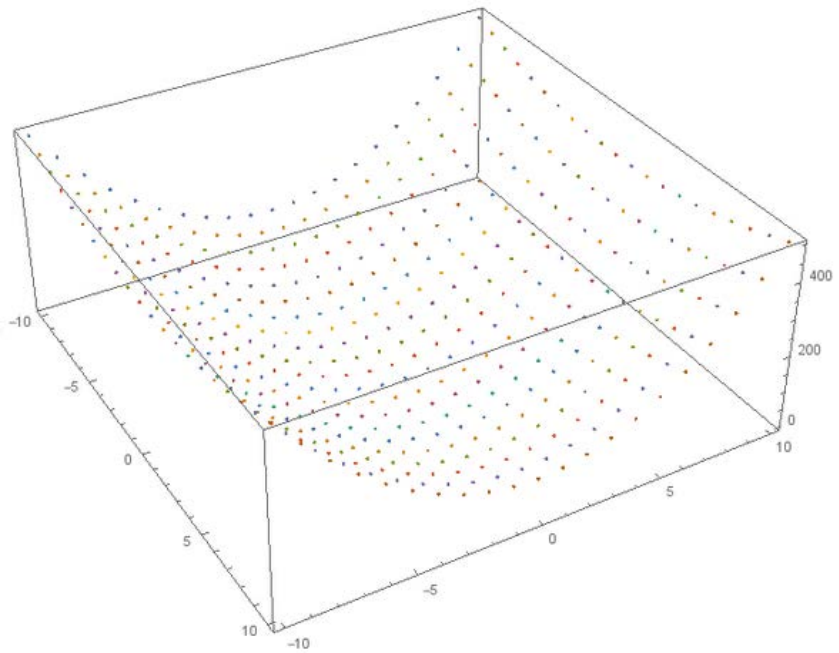
```
ContourPlot[{x^2 - 2*y^2}, {x, -5, 5}, {y, -5, 5}]
```



Слика 5. Контури на индефинитна форма.

Се гледа дека во овој случај контурните линии се хиперболи дадени со равенката $x^2 - 2y^2 = \text{const}$.

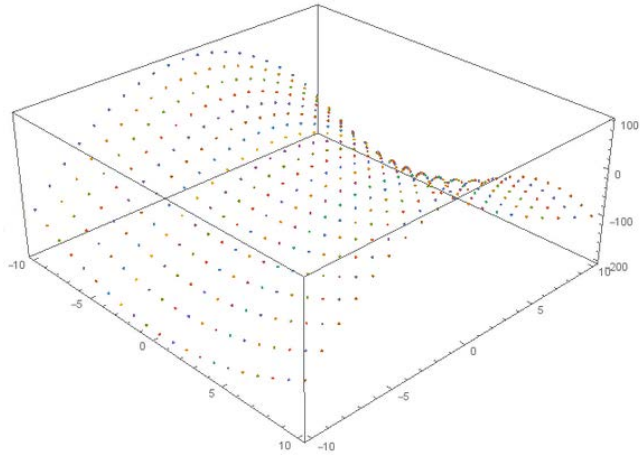
```
ListPointPlot3D[Table[{x, y, x^2 + 4*y^2}, {x, -10, 10, 1}, {y, -10, 10, 1}]]
```



Слика 6. Дискретен график за целобројни вредности на позитивно дефинитна форма.

Додека за втората форма се добива следнава Слика 7:

```
ListPointPlot3D[Table[{x, y, x^2 - 2*y^2}, {x, -10, 10, 1}, {y, -10, 10, 1}]]
```

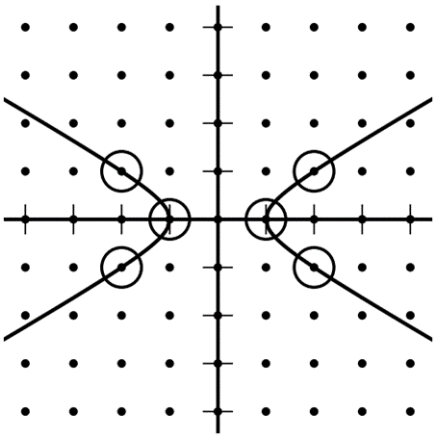


Слика 7. Дискретен график за целобројни вредности на индефинитна форма.

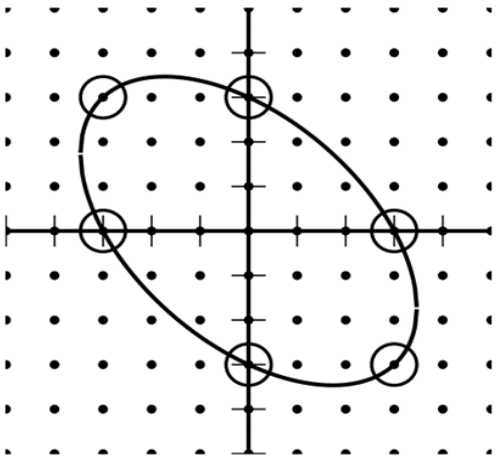
Равенката, која нè интересира

$$n = q(x, y) = ax^2 + bxy + cy^2$$

геометриски може да се интерпретира како барање на заеднички точки меѓу решетката $\mathbb{Z}^2$ на вектори $\begin{pmatrix} x \\ y \end{pmatrix}$ од цели броеви со пресекот на графикот со рамнината $z = const.$, каде што z е цел број. За позитивно дефинитни и индефинитни форми се добиваат следниве преставувања на Слика 8 и Слика 9.



Слика 8. Претставувања на бројот 9 преку формата $\boldsymbol{x^2 + xy + y^2}$.



Слика 9. Претставувања на бројот 9 преку формата $\boldsymbol{x^2 - 3y^2}$.

4 ЕКВИВАЛЕНТНИ ФОРМИ

За дадена форма $q(x,y) = ax^2 + bxy + cy^2$ ќе ја пресметаме формата која се добива со линеарна трансформација на непознатите

$$\begin{cases} x' = sx + ty \\ y' = ux + vy \end{cases}$$

За

$$U = \begin{bmatrix} s & \mathrm{t} \\ u & v \end{bmatrix} \in \mathbb{Z}^{2\times 2}$$

запишуваме

$$U(x,y) = (sx + ty, ux + vy).$$

Од каде се добива

$$(Uq)(x,y) = (x,y)\, U^{\mathrm{T}}\mathrm{M(q)}U \begin{pmatrix} x \\ y \end{pmatrix}$$

За формата Uq ќе велиме дека е *трансформација* на q добиена со матрицата U. Две форми се викаат *еквивалентни* ако постои трансформација U која едната форма ја пресликува во друга.

Пример 1. Да ја земеме формата

$$q(x,y) = 13x^2 + 36xy + 25y^2$$

и да ја трансформираме со матрицата $U = \begin{bmatrix} -4 & 3 \\ 3 & -2 \end{bmatrix}$. Ако ги помножиме матриците во равенката

$$\mathrm{M}(Uq) = U^{\mathrm{T}}\mathrm{M(q)}U$$

се добива

$$\mathrm{M}(Uq) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, (Uq)(x,y) = x^2 + y^2 \,.$$

Трансформацијата на матрицата се пресметува како подолу

$$U^{\mathrm{T}}\mathrm{M(q)}U = \begin{bmatrix} -4 & 3 \\ 3 & -2 \end{bmatrix}\begin{bmatrix} 13 & 18 \\ 18 & 25 \end{bmatrix}\begin{bmatrix} -4 & 3 \\ 3 & -2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} -4 & 3 \\ 3 & -2 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Пример 2. Формата $q(x,y) = x^2 + y^2$ е еквивалентна на

$$q(2x + y, 3x + 2y) = 13x^2 + 16xy + 5y^2$$

добиена со трансформацијата $U = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$. Имено, за матрицата $M(q) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ важи

$$U^{\mathrm{T}}\mathrm{M(q)}U = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 13 & 8 \\ 8 & 5 \end{bmatrix}.$$

Пример 3. Формата $q(x,y) = 50x^2 + 214xy + 229y^2$ е еквивалентна на

$$q(2x + 15y, -x - 7y) = x^2 + y^2$$

добиена со трансформацијата $U = \begin{bmatrix} 2 & 15 \\ -1 & -7 \end{bmatrix}$.

За матрицата $M(q) = \begin{bmatrix} 50 & 107 \\ 107 & 229 \end{bmatrix}$ важи

$$U^{\mathrm{T}}\mathrm{M(q)}U = \begin{bmatrix} 2 & -1 \\ 15 & -7 \end{bmatrix}\begin{bmatrix} 50 & 107 \\ 107 & 229 \end{bmatrix}\begin{bmatrix} 2 & 15 \\ -1 & -7 \end{bmatrix}$$
$$= \begin{bmatrix} -7 & -15 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 2 & 15 \\ -1 & -7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Функцијата $q(x,y) = ax^2 + bxy + cy^2$ каде што x, y се реални променливи, a, b, c се реални броеви се вика *бинарна реална квадратна форма.*

Од реалните матрици ни е познато дека секоја реална бинарна квадратна форма е еквивалентна на дијагонална форма

$$\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

Ова следува од теоремата за дијагонализација на реалните симетрични матрици [1]. Броевите λ_1, λ_2 може да бидат и нула и во овој случај се вели дека бинарната квадратна форма е *дегенерирана*. Имено, за секоја реална форма q, постои трансформација $U \in GL_2(\mathbb{R})$, каде

$$GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\},$$

така што за $\lambda_1, \lambda_2 \in \mathbb{R}$ важи

$$(Uq)(x, y) = \lambda_1 \cdot x^2 + \lambda_2 \cdot y^2.$$

Интуитивно оваа теорема кажува дека за секоја дадена крива од втор ред, може да се најде координатен систем, каде што таа е прикажана во најпростата можна форма.

Од алгебарска гледна точка, класификацијата на квадратните форми во случајот на реални коефициенти е релативно прост проблем и сите форми се сведуваат на дијагонални. Ова е можно, бидејќи групата $GL_2(\mathbb{R})$ ја содржи како подгрупа групата

$$O_2(\mathbb{R}) = \{O \in GL_2(\mathbb{R}) | \; O^{-1} = O^T\}$$

на ортогонални матрици. Според спектралната теорема за линеарни пресликувања, за секоја симетрична матрица M може да се најде елемент $U \in O_2(\mathbb{R})$ со

$$U^{-1} M U = U^T M U = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

Инспирирани од оваа аналогија би сакале да најдеме слични прости претставувања и за целобројните квадратни форми. Може да се шпекулира дека некоја ваква аналогија можеби била почетна точка на Лагранж за да ја развие теоријата на редукција. Тој бил и одличен теоретски физичар и има трудови во областа на механиката. Ако за даден проблем може да се најде соодветниот координатен систем, каде равенките се презентираат во најпростата можна форма, тогаш може полесно да се развијат општите методи за решение.

4.1 ОПЕРАЦИЈАТА НА ГРУПАТА $SL_2(\mathbb{Z})$

Според денешното разбирање, пристапот на Лагранж е стандарден и се заснова во интуитивно разбирање на операцијата на дискретната група

$$GL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0, \;\; a, b, c, d \in \mathbb{Z} \right\}$$

врз множеството на симетрични матрици. Според тоа, за да ги разбереме класите на еквиваленција на целобројните форми, мораме да стекнеме подобро разбирање на групата $GL_2(\mathbb{Z})$. Поради практични причини, покорисно е да се работи со подгрупата $SL_2(\mathbb{Z})$ на матрици со детерминанта еднаква на еден,

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc = 1, \;\; a, b, c, d \in \mathbb{Z} \right\}.$$

Операцијата * на $SL_2(\mathbb{Z})$ врз множеството на бинарни квадратни форми може да се дефинира на следниот начин. Ако q е целобројна бинарна форма со матрица $M(q)$, тогаш важи

$$* : SL_2(\mathbb{Z}) \times M \to M$$

$$U * M(q) \longmapsto U^{\mathrm{T}}\mathrm{M(q)}U$$

која дадена симетрична матрица $M(q)$ ја пресликува во матрица конјугирана со U. Тоа дефинира операција на групата $SL_2(\mathbb{Z})$ на множеството на бинарни квадратни форми. Со оваа операција множеството Q се дели на класи на еквивалентност.

За да ги разбереме подобро овие класи ќе ја разгледаме подетално групата $SL_2(\mathbb{Z})$, која е дискретна подгрупа на $SL_2(\mathbb{R})$ и е генерирана од следните елементи

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ и } T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Овие елементи генерираат циклични подгрупи за кои важи

$$S^4 = I \text{ , } (ST)^6 = I,$$

каде I е единичната матрица

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Матрицата T генерира слободна циклична група

$$\Gamma = \left\{ T^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} | n \in \mathbb{Z} \right\}$$

Операторот T се нарекува *поместувачки оператор* (анг. *shift operator*) и ги извршува следниве трансформации:

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ го трансформира } q(x,y) \text{ во } q(x+y,y)$$

$$T^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \text{ го трансформира } q(x,y) \text{ во } q(x+n\cdot y,y)$$

Операторот S се нарекува *превртувачки оператор* (анг. *flip operator*) и ја извршува следнава трансформација:

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ го трансформира } q(x,y) \text{ во } q(-y,x)$$

Користејќи ги овие два оператори, може да се конструира алгоритам, кој во секоја класа ќе го најде најпростиот претставник. Сите општи прашања во врска со квадратните форми може да се редуцираат на овие редуцирани прости форми.

За да го разбереме алгоритмот за редукција, прво да ги примениме трансформациите S , T на квадратната форма.

$$q(x+n\cdot y,y) = a(x+n\cdot y)^2 + b(x+n\cdot y)y + cy^2$$
$$= a(x^2 + 2nxy + n^2y^2) + bxy + bny^2 + cy^2$$
$$= ax^2 + (b+2an)xy + (an^2 + bn + c)y^2$$
$$q(-y,x) = a(-y)^2 + b(-y)x + cx^2 = cx^2 - bxy + ay^2$$

Тоа значи дека T^n, S оперираат како

$$T^n\colon (a,b,c) \to (a, b+2an, an^2+bn+c)$$
$$S\colon (a,b,c) \to (c,-b,a)$$

Алгоритам за редукција на Лагранж. За која било дадена форма (a,b,c) се повторуваат следниве чекори:

1. Редукција на средниот коефициент.
   Со делење со остаток на b со $2a$ се добива $b = 2a\cdot n + r$.
   Новата вредност b' на редуцираната форма се пресметува со
   $$b' = \begin{cases} b - 2an = r & \text{, ако } r < a \\ b - 2a\cdot(n+1) = r - 2a & \text{, ако } r > a \end{cases}$$
   Во двата случаја важи $|b'| < |a|$. Во првиот случај $r < a$ се применува T^n а во вториот случај $r > a$ се применува T^{n+1} и се добива еквивалентна форма (a,b',c').
2. Ако $|c'| < |a|$, тогаш се применува превртувачкиот оператор S и се повторува првиот чекор со еквивалентната форма

$(c', -b', a)$.

Ако $|a| < |c'|$, тогаш алгоритмот е завршен и (a, b', c') е бараната редуцирана форма.

Бидејќи апсолутната вредност на a, b, c се намалува со секој чекор, оваа постапка ќе заврши после конечен број на чекори. Со ова ја докажавме следната

Теорема 1. (Теорема на Лагранж) За секоја квадратна форма $q = (a, b, c)$ постои еквивалентна редуцирана форма $q' = (a', b', c')$ таква што $|b'| \leq |a'| \leq |c'|$ којашто се нарекува *редуцирана форма на Лагранж* .

Пример 4. Ќе ја најдеме редуцираната форма на Лагранж за $q = (4, -24,39)$.

$$(4, -24,39) \rightarrow (4, -24 + 2 \cdot 3 \cdot 4, 4 \cdot 3^2 - 24 \cdot 3 + 39) = (4,0,3)$$
$$\rightarrow (3,0,4).$$

За $q(x, y) = 4x^2 - 24xy + 39y^2$ се добиваат следниве промени на непознатите: со трикратна операција на поместување се добива

$$q(x + 3 \cdot y, y) = 4(x + 3 \cdot y)^2 - 24(x + 3 \cdot y) \cdot y + 39y^2 = 4x^2 + 3y^2.$$

После една трансформација на превртување се добива редуцираната форма на Лагранж

$$q(-y, x + 3 \cdot y) = 3x^2 + 4y^2.$$

Се гледа дека постапката за наоѓање на редуцираната форма на Лагранж е многу едноставна и може да се спроведе рачно. Генијалноста на Лагранж се состои во фактот дека тој прв ги согледал бинарните квадратни форми како целина, ги разбил на класи на еквивалентност користејќи линеарни промени на непозатите и нашол лесен алгоритам за да стигне до наједноставниот претставник на секоја класа. Иако редуцираната форма на Лагранж не е толку проста како диагонализацијата $\lambda_1 \cdot x^2 + \lambda_2 \cdot y^2$, сепак тоа е најмногу што може да се очекува во дадените околности.

Користејќи ги условите за коефициентите на редуцираната форма на Лагранж лесно може да се докажат следниве неравенства:

Теорема 2. За дадена квадратна форма $q = (a, b, c)$ со дискриминанта $\Delta = \Delta(q) = b^2 - 4ac$, коефициентите на редуцираната форма на Ларгарнж ги задоволуваат следните неравенства

$$|b|^2 \leq -\frac{\Delta}{3}, \qquad |a|^2 \leq -\frac{\Delta}{3}, \qquad |c| \leq \frac{1-\Delta}{4}, \qquad \text{ако } \Delta < 0,$$

$$|b|^2 \leq -\frac{\Delta}{5}, \qquad |a|^2 \leq -\frac{\Delta}{2}, \qquad |c| \leq \frac{\Delta}{4}, \qquad \text{ако } \Delta > 0.$$

Од овие неравенства следува дека бројот на редуцираните форми на Ларгарнж за дадена дискриминанта е конечен. Со овие неравенства и фактот дека a, b, c се цели броеви, лесно е да се пресметаат редуцираните форми за мали вредности на Δ.

Пример 5. Нека $\Delta = -4 \cdot 65 = -260$.

Од $|b|^2 \leq -\frac{\Delta}{3} = \frac{260}{3} = 86{,}6$ следува дека $|b| \leq 9$. Аналогно $|a| \leq 9$ и $|c| \leq 65$.

Од $b \equiv \Delta \equiv 0 \ (mod\ 2)$ следува дека $b \in \{0, \pm 2, \pm 4, \pm 6, \pm 8\}$.

Од $a \cdot c = \frac{b^2 - \Delta}{4}$ се наоѓаат вредностите за a и c пресметувајќи ги сите факторизации на $\frac{b^2-\Delta}{4}$. Користејќи го условот за редукција $|b| < |a| < |c|$ се наоѓаат сите редуцирани форми за дадена вредност на b.

- $b = 0$, $a \cdot c = 65$, која ги дава формите (1, 0, 65) и (5, 0, 13),
- $b = \pm 2$, $a \cdot c = 66$, која ги дава формите (2, ± 2, 33), (3, ± 2, 22) и (6, ± 2, 11),
- $b = \pm 4$, $a \cdot c = 69 = 3 \cdot 23$, која не дава редуцирани форми ($|a| = 3 < 4 = |b|$),
- $b = \pm 6$, $a \cdot c = 74 = 2 \cdot 37$, која исто така не дава редуцирани форми,
- $b = \pm 8$, $a \cdot c = 81$, која ја дава редуцираната форма (9, ± 8, 9).

Редуцираните форми на Лагранж со дискриминанта $\Delta = -4 \cdot 65 = -260$ се:

(1, 0, 65), (5, 0, 13), (2, ± 2, 33), (3, ± 2, 22), (6, ± 2, 11), (9, ± 8, 9).

Подолу даваме табела на редуцирани форми за мали позитивни и негативни вредности на дискриминантата Δ.

Δ	Редуцирани форми на Лагранж
−3	(1,±1,1)
−4	(1,0,1)
−7	(1,±1,2)
−8	(1,0,2)
−11	(1,±1,3)
−12	(1,0,3),(2,±2,2)
−15	(1,±1,4),(2,±1,2)
−16	(1,0,4),(2,0,2)

Δ	Редуцирани форми на Лагранж
5	(1,±1,−1),(−1,±1,1)
8	(1,0,−2),(−1,0,2)
12	(1,0,−3),(−1,0,3)
13	(1,±1,−3),(−1,±1,3)
17	(1,±1,−4),(−1,±1,4), (±2,1,∓2),(±2,−1,∓2)
20	(1,0,−5),(−1,0,5),(2,±2,−2)
21	(1,±1,−5),(−1,±1,5)

Табела 1. Листа на редуцирани форми на Лагранж за дадена вредност на Δ.

Читателите кои се повеќе заинтересирани, може да најдат повеќе информации во [4].

5 ПРЕТСТАВУВАЊЕ НА ПРОСТИ БРОЕВИ

5.1 КВАДРАТНИ ОСТАТОЦИ И ОСНОВНИ КВАДРАТНИ ФОРМИ

Сега да се вратиме на проблемот на претставување на простите броеви преку квадратни форми. Од $\Delta = b^2 - 4ac \equiv b^2 \ (mod\ 4)$ следува

$$\begin{cases} \Delta \equiv 0 \ (mod\ 4) & \Rightarrow \ \Delta = 4m \\ \Delta \equiv 1 \ (mod\ 4) & \Rightarrow \ \Delta = 1 - 4m \end{cases}$$

за некој цел број m. Во овој случај се важни следните квадратни форми

$$q_0(x,y) = \begin{cases} x^2 + m \cdot y^2, & \Delta = 4m \\ x^2 + xy + m \cdot y^2, & \Delta = 1 - 4m \end{cases}$$

кои се редуцирани форми на Лагранж и се викаат *основни* квадратни форми со дискриминанта Δ.

Целиот број $a \in \mathbb{Z}$ е *квадратен остаток* $mod\, p$ ако конгруенцијата $x^2 \equiv a\ (mod\, p)$ има целобројно решение. $a \in \mathbb{Z}$ не е квадратен остаток $mod\, p$ ако конгруенцијата $x^2 \equiv a\ (mod\, p)$ нема целобројно решение.

Централен резултат за претставување на прости броеви преку квадратни форми е следната теорема.

Теорема 3. За дадена дискриминанта Δ, следните тврдења се еквивалентни

1. $p \mid q_0(a, b)$ за даден пар на заемно прости броеви a, b.
2. Δ е квадратен остаток $mod\, p$.
3. Постои квадратна форма $q = (p, b, c)$ со дискриминанта Δ.
4. Постои квадратна форма q со $p = q(a, b)$, со пар на заемно прости броеви a, b.

Ако се комбинираат тврдењата 1 и 3 со редукцијата на Лагранж на квадратните форми, се добива следниот централен резултат на Лагранж, кој целосно го решава проблемот на Ферма.

Теорема 4. (Теорема на Лагранж) Ако Δ е квадратен остаток $mod\, p$, тогаш постои редуцирана форма на Лагранж q со дискриминанта Δ, која го претставува простиот број p.

Со оваа теорема проблемот на Ферма за дадена основна форма

$$q_0(x, y) = x^2 + m \cdot y^2, \ \ \Delta = 4m$$

се редуцира на наоѓањето на сите прости броеви p, така што Δ е квадратен остаток $mod\, p$. И за доказите на горенаведените тврдења заинтересираните читатели ги упатувам на [4].

5.2 СИМБОЛОТ НА ЛЕЖАНДР

Пред да ги најдеме критериумите за Δ да биде квадратен остаток $mod\ p$ ќе треба да кажеме и неколку зборови за симболот на Лежандр и неговото најважно својство, имено квадратната реципрочност.

За работа со квадратни остатоци се користи *симболот на Лежандр*, кој е дефиниран само за непарните прости броеви ($p \neq 2$).

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & a \text{ е квадратен остаток } mod\ p \text{ и } a \not\equiv 0\ (mod\ p) \\ -1, & a \text{ не е квадратен остаток } mod\ p \\ 0, & \text{ако } a \equiv 0\ (mod\ p) \end{cases}$$

За овој симбол важат следниве равенства:

- $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\ p)$
- $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ ако $a \equiv b\ (mod\ p)$
- $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
- *Квадратна реципрочност*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Бидејќи p и q се прости броеви важи $q \not\equiv 0\ (mod\ p)$, такашто $\left(\frac{p}{q}\right)$ прима вредности од множеството {-1, 1}, па затоа $\left(\frac{p}{q}\right)^2 = 1$. Ако се помножат и двете страни на горното равенство со $\left(\frac{p}{q}\right)$, се добива следната форма, која ќе ја користиме во подолните пресметувања

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

Доказите на горните тврдења може да се најдат во [5].

Пример 6. Подолу ќе ги пресметаме вредностите на симболот на Лежандр за конкретни вредности на p и q за да добиеме појасна слика за начинот на којшто се користи за да се одреди дали даден број p е квадратен остаток по даден модул q.

а) $\left(\frac{1}{p}\right) \equiv (1)^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$.

Симболот на Лежандр секогаш прима вредности од множеството {-1, 0, 1}, па затоа $\left(\frac{1}{p}\right) = 1$ за било кој непарен прост број p.

б) $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv \begin{cases} +1,\ p \equiv 1\ (mod\ 4) \\ -1,\ p \equiv 3\ (mod\ 4) \end{cases}$. Со истиот аргумент како погоре, од овде следува дека

$$\left(\frac{-1}{p}\right) = \begin{cases} +1,\ p \equiv 1\ (mod\ 4) \\ -1,\ p \equiv 3\ (mod\ 4) \end{cases}$$

в) $\left(\frac{2}{p}\right) = \begin{cases} +1,\ p \equiv 1 \text{ или } p \equiv 7\ (mod\ 8) \\ -1,\ p \equiv 3 \text{ или } p \equiv 5\ (mod\ 8) \end{cases}$. Доказот може да се најде во [5].

г) $\left(\frac{3}{97}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{97-1}{2}} \cdot \left(\frac{97}{3}\right) = \left(\frac{97}{3}\right) = \left(\frac{1}{3}\right) = 1$

д) $\left(\frac{880}{863}\right) = \left(\frac{2^4 \cdot 5 \cdot 11}{863}\right) = \left(\frac{2}{863}\right)^4 \cdot \left(\frac{5}{863}\right) \cdot \left(\frac{11}{863}\right)$

$$= 1 \cdot (-1)^{\frac{5-1}{2}\cdot\frac{863-1}{2}} \cdot \left(\frac{863}{5}\right) \cdot (-1)^{\frac{11-1}{2}\cdot\frac{863-1}{2}} \cdot \left(\frac{863}{11}\right)$$

$$= \left(\frac{3}{5}\right) \cdot (-1) \cdot \left(\frac{5}{11}\right) = (-1) \cdot (-1)^{\frac{5-1}{2}\cdot\frac{3-1}{2}} \cdot \left(\frac{5}{3}\right) \cdot (-1)^{\frac{5-1}{2}\cdot\frac{11-1}{2}} \cdot \left(\frac{11}{5}\right)$$

$$= (-1) \cdot \left(\frac{2}{3}\right) \cdot \left(\frac{1}{5}\right) = (-1) \cdot (-1) \cdot 1 = 1$$

Користејќи го симболот на Лежандр за мали вредности на Δ, критериумите кои треба да ги исполнат непарните прости броеви p за Δ да биде квадратен остаток по модулот p може да се дадат преку конгруенции.

На сличен начин, кога се дадени мали вредности на p и Δ преку елиминација на сите можни случаи се добиваат конкретни критериуми во форма на конгруенции за да се најде вредноста на $\left(\frac{\Delta}{p}\right)$. Во подолната табела ги даваме критериумите за вредностите на $-12 \leq \Delta \leq 12$:

Δ	Критериум за Δ да биде квадратен остаток *mod p*	Δ	Критериум за Δ да биде квадратен остаток *mod p*
1	Секој прост број	**−1**	$p \equiv 1 \pmod 4$
2	$p \equiv 1, 7 \pmod 8$	**−2**	$p \equiv 1, 3 \pmod 8$
3	$p \equiv 1, 11 \pmod{12}$	**−3**	$p \equiv 1 \pmod 3$
4	Секој прост број	**−4**	$p \equiv 1 \pmod 4$
5	$p \equiv 1, 4 \pmod 5$	**−5**	$p \equiv 1, 3, 7, 9 \pmod{20}$
6	$p \equiv 1, 5, 19, 23 \pmod{24}$	**−6**	$p \equiv 1, 5, 7, 11 \pmod{24}$
7	$p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$	**−7**	$p \equiv 1, 2, 4 \pmod 7$
8	$p \equiv 1, 7 \pmod 8$	**−8**	$p \equiv 1, 3 \pmod 8$
9	Секој прост број	**−9**	$p \equiv 1 \pmod 4$
10	$p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \pmod{40}$	**−10**	$p \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40}$
11	$p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}$	**−11**	$p \equiv 1, 3, 4, 5, 9 \pmod{11}$
12	$p \equiv 1, 11 \pmod{12}$	**−12**	$p \equiv 1 \pmod 3$

Табела 2. Критериуми со конгруенции за Δ да биде квадратен остаток *mod p.*

Пример 7. Да ги најдеме условите кои треба да ги исполни даден непарен прост број p, така што 3 е квадратен остаток по модулот p

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right).$$

Разгледувајќи ги еден по еден релевантните случаи $p\ (mod\ 4)$ за знакот на $(-1)^{\frac{p-1}{2}}$ како и $p\ (mod\ 3)$ за знакот на $\left(\frac{p}{3}\right)$ се добива дека $\left(\frac{3}{p}\right) = 1$ ако и само ако $p \equiv 1\ (mod\ 12)$ или $p \equiv 11 \equiv -1\ (mod\ 12)$. Еквивалентно може да се запише $p \equiv \pm 1\ (mod\ 12)$.

Овие конгруенции заедно со теоријата на редукција на квадратните форми и горенаведените теореми се суштината на тврдењата на Ферма. Овој пристап ни дава не само објаснување туку и алгоритамски

методи за пресметување на претставувањата на простите броеви преку квадратни форми.

Уште еден важен заклучок од теоремата на Лагранж е дека е многу поприродно да се земаат предвид сите нееквивалентни редуцирани форми за дадена дискриминанта.

Користејќи ги Табелите 1 и 2 како и теоремата на Лагранж, може да ги дадеме следните критериуми за вредностите на Δ, за кои постои само една редуцирана форма на Лагранж

Теорема 5. За прости броеви p важи

1. Ако $p \equiv 1 \pmod 3$ тогаш
   $p = x^2 + xy + y^2$, за $x, y \in \mathbb{Z}$, $(\Delta = -3)$
2. Ако $p \equiv 1 \pmod 4$ тогаш
   $p = x^2 + y^2$, за $x, y \in \mathbb{Z}$, $(\Delta = -4)$
3. Ако $p \equiv 1, 3 \pmod 8$ тогаш
   $p = x^2 + 2y^2$, за $x, y \in \mathbb{Z}$, $(\Delta = -8)$
4. Ако $p \equiv 1, 4 \pmod 5$ тогаш
   $p = x^2 + xy - y^2$, за $x, y \in \mathbb{Z}$, $(\Delta = 5)$

За илустрација да го докажеме само првото тврдење. Останатите три се аналогни и читателот може да ги најде во [4]. Се гледа дека $\Delta = -3 = 1 - 4 \cdot 1$, и бидејќи класата на -3 има единствена редуцирана форма, таа ќе биде основната форма $x^2 + xy + y^2 (m = 1)$. Според теоремата 4 на Лагранж простиот број може да се претстави преку оваа редуцирана форма ако и само ако $\left(\frac{\Delta}{p}\right) = \left(\frac{-3}{p}\right) = 1$. Од горната табела се гледа дека ова е можно ако и само ако $p \equiv 1 \pmod 3$.

Пример 8. Претставување на конкретни прости броеви преку редуцирани форми на Лагранж:

а) $p = 7, \quad 7 \equiv 1 \,(mod\ 3) \Rightarrow 7 = 2^2 + 2 \cdot 1 + 1^2$

б) $p = 17, 17 \equiv 1 \,(mod\ 4) \Rightarrow 17 = 4^2 + 1^2$

$17 \equiv 1 \,(mod\ 8) \Rightarrow 17 = 3^2 + 2 \cdot 2^2$

в) $p = 19, 19 \equiv 3 \,(mod\ 8) \Rightarrow 19 = 1^2 + 2 \cdot 3^2$

$19 \equiv 4 \,(mod\ 5) \Rightarrow 19 = 4^2 + 4 \cdot 1 - 1^2$

6 ЗАКЛУЧОК

Наизглед простиот проблем на претставување на прост број како сума на два квадрати не доведе до теоријата на Лагранж за редукција на квадратни форми. Таа ни даде не само целосно решение на проблемот туку и конкретни алгоритми како да стигнеме до нив.

После продлабочувањето на разбирањата од теоријата на редукција на квадратни форми, дојдовме во заклучок дека проблемите на Ферма се специјални случаи, и се однесуваат само на една специфична класа на редуцирани форми. Воедно за да се даде целосно решение на проблемот, треба да се воведе концептот на редуцирани форми и проблемот да се формулира пошироко за сите редуцирани форми за дадена дискриминанта. После овој чекор, конкретните критериуми за претставување на прост број преку квадратна форма се сведуваат на една табела за редуцирани форми и друга за квадратни остатоци по даден модул.

Оваа теорија и решението на проблемот на Ферма претставуваат брилијантно достигнување на големиот математичар Лагранж во теоријата на броеви. Теоретскиот дел се базира на книгите [4] и [5].

Благодарност. Трудот е посветен на моите професори проф. д-р Ристо Малчески, проф. д-р Костадин Тренчевски и акад. проф. д-р Дончо Димовски, од кои ја имам научено основата на теоријата на броеви.

ЛИТЕРАТУРА

[1] L. Beshaj, T. Shaska, E. Zhupa, *Advances on superelliptic curves and their applications*, 84-116, IOS Press, 2015.

[2] Dr. R.Hartung, *Computational Problems of Quadratic Forms*, PhD Thesis, Johann Wolfgang von Goethe University, Frankfurt, Germany, 2007.

[3] J. L. Lagrange, *Recherches d'arithmetique*, Nouv. Mem. Acad. Berlin (1773), 265-312, in Oeuvres de Lagrange III, 695-795.

[4] F.Lemmermeyer, Binary quadratic forms, www.rzuser.uni-heidelberg.de/~hb3/publ/bf.pdf

[5] A. Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer-Verlag Berlin Heidelberg, 2007.

[6] Wolfram Mathematica: Modern Technical Computing https://www.wolfram.com/mathematica/

[7] Wolfram Programming Lab (Open Cloud) https://lab.open.wolframcloud.com/app/

[1] RISAT – Research Institute of Science and Technology,
530 Church St, Ann Arbor, MI 48109, USA
e-mail: huseini@risat.org

Примен: 4.03.2019
Поправен: 26.05.2019
Одобрен: 30.05.2019
Објавен на интернет: 5.06.2019