مجلة جامعة تشرين للبحوث والدراسات العلمية - سلسلة العلوم الأساسية المجلد (40) العدد (1) 2018
Tishreen University Journal for Research and Scientific Studies - Basic Sciences Series Vol. (40) No. (1) 2018

دراسة معادلة بل باستخدام المرتّبات التّربيعيّة

الدكتور حسن سنكري *
أحمد عيسى **

(تاريخ الإيداع 17/ 9 / 2017. قُبِل للنشر في 4 / 2 /2018)

☐ ملخّص ☐

درسنا في هذا البحث قابليّة حلّ معادلة بل $x^2 - \Delta y^2 = N$ في مجموعة الأعداد الصّحيحة $\mathbb{Z}$ ، حيث أعطينا شرطاً لازما وكافياً لقابليّة حلّ هذه المعادلة بالإعتماد على الإيديالات في مرتّبات الحقول التّربيعيّة الحقيقيّة، كما أعطينا صيغة الإيديال المقابل لكلّ حلّ لهذه المعادلة وذلك من أجل حالات خاصّة لـN وΔ.

الكلمات المفتاحيّة: الحقول التّربيعيّة الحقيقيّة ، المرتّبات التّربيعيّة ، معادلة بل .

* أستاذ- قسم الرياضيات- كلية العلوم- جامعة تشرين- اللاذقية- سورية
** طالبة دراسات عليا (ماجستير)- قسم الرياضيات- كلية العلوم- جامعة تشرين- اللاذقية- سورية

مجلة جامعة تشرين للبحوث والدراسات العلمية – سلسلة العلوم الأساسية المجلد (40) العدد (1) 2018
Tishreen University Journal for Research and Scientific Studies - Basic Sciences Series Vol. (40) No. (1) 2018

Studying Pell's Equation by Using the Quadratic Orders

Dr. Hasan Sankari*
Ahmed Eisa**

(Received 17 / 9 / 2017. Accepted 4/ 2 /2018)

□ ABSTRACT □

In this paper , we will study the ability to solve Pell's equation $x^2 - \Delta y^2 = N$ in the set $\mathbb{Z}$, we give necessary and sufficient conditions to solve this equation , depending on the ideals in orders of the real quadratic fields .We also introduce the formula of the opposite ideal for every solution of this equation , in special cases of N and Δ .

Key words: Real Quadratic Fields, Quadratic Orders, Pell's Equation .

***Assistant Professor, Department of Mathematics, Faculty of Science, Tishreen University, Lattakia, Syria.**
****Postgraduate Student, Department of Mathematics, Faculty of Science, Tishreen University, Lattakia, Syria.**

مقدّمة :

معادلة بل Pell's equation هي معادلة من الشكل $x^2-\Delta y^2=N$ حيث N و Δ عددان صحيحان معلومان وغير صفريّن ، $\Delta>0$ ، وتوجد الحلول (x,y) في مجموعة الأعداد الصّحيحة $\mathbb{Z}$.

تمّ تقديم العديد من الأبحاث لدراسة معادلة بل ، فقد درست كحالة خاصّة من الصّيغ التّربيعيّة Mathews [7]، ودرست باستخدام حقول الأعداد التّربيعيّة Bolker [2] ، ونظريّة الإيديالات Mollin [8] ، كما درس Halter-Koch [5] العلاقة بين حلول المعادلة) $dx^2-d^*y^2=\pm t$ حيث $t\in\{1,2,4\}$ و d, d^* عددان طبيعيان و dd^* ليس مربع كامل) ونظريّة الإيديالات في المرتّبات التّربيعيّة، كما أورد الباحثان Andrica [1] و Andreescu اختبار يبيّن متى معادلة بل غير قابلة للحلّ بالاعتماد على حلقة بواقي الأعداد الصحيحة بالنسبة للمقاس n . حديثا يتم دراسة الزمر الجزئية المولدة بحلول معادلة بل و اختبارات لقابلية حلّ المعادلة، لمزيد من المعلومات يرجى مراجعة [3,6].

سندرس في هذا البحث العلاقة بين حلول معادلة بل والإيديالات النّظاميّة المبهمة في المرتّبات التّربيعيّة ، وذلك من أجل حالات خاصّة لـN و Δ .

أهمية البحث وأهدافه:

يهدف هذا البحث إلى دراسة معادلة بل ، وذلك من أجل حالات خاصّة لـN و Δ ، وتكمن أهميّته في أنّه يعطي شرطاً لازماً وكافياً لقابليّة حلّ هذه المعادلة بالإعتماد على الإيديالات في المرتّبات التربيعية ، كما يعطي صيغة الإيديال المقابل لكلّ حلّ لهذه المعادلة .

طرائق البحث وموادّه:

في هذا البحث نستفيد من خواصّ الإيديالات ، ومن تصنيف الإيديالات النّظاميّة المبهمة في المرتّبات التّربيعيّة [4] ، بالإضافة إلى قابليّة حلّ المعادلة $dx^2-d^*y^2=\pm t; t\in\{1,2,4\}$ بالاعتماد على الإيديالات النّظاميّة المبهمة الرّئيسيّة في المرتّبات التّربيعيّة [5] .

تعاريف ومفاهيم أساسيّة:

تعريف 1:[4]

يُقال عن العدد الصّحيح Δ إنّه مميّز تربيعيّ إذا تحقّق كلّ من الشّرطين التّاليين :

1- Δ ليس مربّع كامل

2- $\Delta\equiv 0 \text{ or } 1 \ (mod 4)$

تعريف 2:[4]

يُقال عن المميّز التّربيعيّ Δ بأنّه مميّز أساسيّ إذا لم يكتب Δ بالصّيغة التّالية :

$\Delta=\Delta_1 f^2$ حيث Δ_1 مميّز تربيعيّ و $f\in\mathbb{Z}$ بحيث $f\geq 2$.

تمهيدية1: [4]

إذا كان Δ مميّز تربيعيّ عندئذ كل من الشّرطين الآتيين متكافئين :

1 - Δ مميّز أساسيّ .

2 – (Δ حرّ من التّربيع و $\Delta \equiv 1 mod 4$) أو ($\Delta = 4D$ حيث D حرّ من التّربيع و $D \equiv 2 or 3 mod 4$).

تعريف3: [4]

ليكن Δ مميّز تربيعيّ و $\mathrm{K} = \mathbb{Q}(\sqrt{\Delta})$ حقل أعداد تربيعيّة.

يعرّف المرتّب التّربيعيّ $\mathcal{O}_{\Delta}$ بالشّكل التالي :

$$\mathcal{O}_{\Delta} = [1, w_{\Delta}] = \mathbb{Z}[w_{\Delta}] \, ; w_{\Delta} = \frac{\sigma_{\Delta} + \sqrt{\Delta}}{2} \quad \wedge \ \sigma_{\Delta} = \begin{cases} 0 & if\ \Delta \equiv 0 mod 4 \\ 1 & if\ \Delta \equiv 1 mod 4 \end{cases}$$

تمهيديّة2: [4]

ليكن Δ مميّز تربيعيّ و $\mathrm{K} = \mathbb{Q}(\sqrt{\Delta})$ حقل أعداد تربيعيّة، عندئذ المرتّب التّربيعيّ $\mathcal{O}_{\Delta}$ يعطى بالصّيغة التّالية :

$$\mathcal{O}_{\Delta} = \left\{ \frac{u + v\sqrt{\Delta}}{2} \ ; u , v \in \mathbb{Z} \ \wedge u \equiv v\Delta mod\ 2 \right\}$$

تعريف4:[4]

ليكن Δ مميّز تربيعيّ عندئذ :

1) العنصر $\alpha \in \mathcal{O}_{\Delta}$ يسمى عنصراً بسيطاً في $\mathcal{O}_{\Delta}$ إذا كان $m^{-1}\alpha \notin \mathcal{O}_{\Delta}$ من أجل أيّ عدد صحيح m حيث $m \geq 2$.

2) الإيديال I في $\mathcal{O}_{\Delta}$ يسمّى :

*) إيديال بسيط $(primitive\ ideal)$ في $\mathcal{O}_{\Delta}$ إذا كان $m^{-1}\mathrm{I} \not\subset \mathcal{O}_{\Delta}$ من أجل أيّ عدد صحيح m حيث $m \geq 2$.

*) إيديال نظاميّ $(regular\ ideal)$ في $\mathcal{O}_{\Delta}$ إذا كان بسيطاً وقابلاً للقلب في $\mathcal{O}_{\Delta}$.

3) من أجل الإيديال I المختلف عن الصّفر في $\mathcal{O}_{\Delta}$ يدعى :

$N(\mathrm{I}) = (\mathcal{O}_{\Delta} : \mathrm{I})$ نظيم الإيديال I.

وإذا كان $\alpha \in \mathcal{O}_{\Delta}$ مختلف عن الصّفر عندئذ $N(\alpha\mathcal{O}_{\Delta}) = |n(\alpha)|$.

تمهيديّة3:[4]

ليكن Δ مميّز تربيعيّ و $K = \mathbb{Q}(\sqrt{\Delta})$ حقل أعداد تربيعيّة .

1) ليكن I إيديالاً مختلفاً عن الصّفر في $\mathcal{O}_{\Delta}$ عندئذ يوجد $a, e \in \mathbb{N}$ و $b, c \in \mathbb{Z}$ بحيث يكون :

$$\mathrm{I} = e\left[a, \frac{b + \sqrt{\Delta}}{2}\right] \ \wedge \ \ \Delta = b^2 - 4ac$$

بالإضافة إلى ذلك فإنَّ $N(\mathrm{I}) = ae^2 \in \mathrm{I}$.

2) لتكن a, b, e أعداد صحيحة بحيث أنّ $ae \neq 0$ عندئذ يكون $\mathrm{I} = \left[a, \frac{b + e\sqrt{\Delta}}{2}\right]$ إيديال في $\mathcal{O}_{\Delta}$ إذا وفقط إذا كان $e \mid a \ , \ 2e \mid e\Delta - b \ , \ 4ae \mid b^2 - \Delta e^2$

بالإضافة إلى ذلك فإنّ:

I إيديال بسيط في $\mathcal{O}_{\Delta}$ إذا وفقط إذا $|e| = 1$.

I إيديال نظاميّ في $\mathcal{O}_{\Delta}$ إذا وفقط إذا $\left(a, b, \frac{b^2 - \Delta}{4a}\right) = 1 \ \wedge \ |e| = 1$.

تعريف5:[4]

ليكن Δ مميّز تربيعيّ .

يقال بأنّ I إيديال مبهم $(ambiguous\ ideal)$ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ إذا كان $\mathrm{I} = \acute{\mathrm{I}}$

حيث $\acute{\mathrm{I}} = \{\acute{\alpha}\ ;\ \alpha \in \mathrm{I}\}$.

تمهيديّة4: [4]

ليكن Δ مميّز تربيعيّ .

عندئذ يكون الإيديال النّظاميّ I في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ مبهم إذا وفقط إذا أخذ أحد الصّيغتين التّاليتين :

$$\mathrm{I} = \left[a, \frac{\sqrt{\Delta}}{2}\right];\ a \in \mathbb{N}\ \wedge\ 4a \mid \Delta\ \wedge \left(a, \frac{\Delta}{4a}\right) = 1 \qquad (\mathrm{I})$$

$$\mathrm{I} = \left[a, \frac{a + \sqrt{\Delta}}{2}\right];\ a \in \mathbb{N}\ \wedge\ 4a \mid a^2 - \Delta\ \wedge \left(a, \frac{a^2 - \Delta}{4a}\right) = 1 \qquad (\mathrm{II})$$

وبشكل أكثر خصوصيّة يتحقق الآتي:

1) إذا كان $\Delta \equiv 1 mod 4$

عندئذ لا يوجد إيديال نظاميّ مبهم من النّمط (I) , أمّا الصّيغة (II) تعطى كالآتي:

$$\mathrm{I} = \left[a, \frac{a + \sqrt{\Delta}}{2}\right]; a \in \mathbb{N}\ \wedge\ a \mid \Delta\ \wedge \left(a, \frac{\Delta}{a}\right) = 1$$

2) إذا كان $\Delta = 4D$

عندئذ الإيديالات النّظاميّة المبهمة في $\mathcal{O}_\Delta$ من النّمط (I) تعطى بالصّيغة التّالية :

$$\mathrm{I} = \left[a, \sqrt{D}\right];\ a \in \mathbb{N}\ \wedge\ a \mid D \wedge \left(a, \frac{D}{a}\right) = 1$$

3) إذا كان $\Delta = 4D$ و $D \equiv 3\ mod\ 4$

عندئذ الإيديالات النّظاميّة المبهمة في $\mathcal{O}_\Delta$ من النّمط (II) تعطى بالصّيغة التّالية :

$$\mathrm{I} = \left[2a, a + \sqrt{D}\right];\ a \in \mathbb{N}\ \wedge\ a \mid D\ \wedge \left(a, \frac{D}{a}\right) = 1$$

4) إذا كان $\Delta = 4D$ و $8 \mid D$

عندئذ الإيديالات النّظاميّة المبهمة في $\mathcal{O}_\Delta$ من النّمط (II) تعطى بالصّيغة التّالية:

$$\mathrm{I} = \left[4a, 2a + \sqrt{D}\right];\ a \in \mathbb{N}\ \wedge 4a \mid D\ \wedge \left(a, \frac{D}{4a}\right) = 1$$

5) إذا كان $\Delta = 4D$ و $8 \nmid D$ و $D \not\equiv 3\ mod\ 4$

عندئذ لايوجد أيّ إيديال نظاميّ مبهم من النمط (II) .

تمهيديّة5:[5]

ليكن $\Delta \in \mathbb{N}$ مميّز تربيعيّ

وبفرض أنّ

- $\Delta = 4D$
- $c \in \{1,2\}$ إذا كان $8 \mid D$ و $c = 1$ إذا كان $8 \nmid D$
- $t \in \{1,2\}$ إذا كان $D \equiv 3\ mod\ 4$ و $t = 1$ إذا كان $D \not\equiv 3\ mod\ 4$

• $D = c^2dd^*$ حيث $d, d^* \in \mathbb{N}$ و $(d, d^*) = 1$

وليكن I معطى بالشكل التّالي :

$$I = \begin{cases} [d, \sqrt{D}] & if ct = 1 \\ [2d, d + \sqrt{D}] & if\ \ t = 2 \\ [4d, 2d + \sqrt{D}] & if\ \ c = 2 \end{cases}$$

عندئذ:

a. I إيديال نظاميّ مبهم في المرتّب التربيعيّ $\mathcal{O}_\Delta$ يحقّق $N(\mathrm{I}) = c^2dt$ وكلّ إيديال نظاميّ مبهم في $\mathcal{O}_\Delta$ من هذا الشكل .

b. I مختزل إذا وفقط إذا $d < d^*$.

c. I إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ إذا وفقط إذا وجد $x, y \in \mathbb{Z}$ بحيث $|dx^2 - d^*y^2| = t$ و $(c, xy) = 1$.

d. ليكن $x, y \in \mathbb{Z}$ بحيث $|dx^2 - d^*y^2| = t$ و $(c, xy) = 1$ عندئذ $\mathrm{I} = (cdx + y\sqrt{D})\mathcal{O}_\Delta$.

تمهيديّة6:[5]

ليكن Δ مميّز تربيعيّ بحيث $\Delta \equiv 1 \bmod 4$ و $\Delta = dd^* \in \mathbb{N}$ بحيث $(d, d^*) = 1$

ولتكن I معطى بالشكل التّالي :

$$\mathrm{I} = \left[d, \frac{d + \sqrt{\Delta}}{2}\right]$$

عندئذ :

a. I إيديال نظاميّ مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ يحقق $N(\mathrm{I}) = d$ وكلّ إيديال نظاميّ مبهم في $\mathcal{O}_\Delta$ من هذا الشكل .

b. I مختزل إذا وفقط إذا $d < d^*$.

c. I إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ إذا وفقط إذا وجد $x, y \in \mathbb{Z}$ بحيث $|dx^2 - d^*y^2| = 4$.

d. ليكن $x, y \in \mathbb{Z}$ بحيث $|dx^2 - d^*y^2| = 4$ عندئذ $\mathrm{I} = (\frac{dx + y\sqrt{\Delta}}{2})\mathcal{O}_\Delta$.

النّتائج والمناقشة:

بالإستفاده من التّعاريف والتّمهيديات السّابقة سوف نقوم بإثبات المبرهنات التّالية :

مبرهنة1:

ليكن p عدداً أوّلياً فردياً.

وليكن $\Delta > 0$ مميّز تربيعيّ بحيث $\Delta \equiv 1 mod4$ و $\Delta = pd$ و $(p, d) = 1$.

عندئذ :

1) $\mathrm{I} = \left[p, \frac{p+\sqrt{\Delta}}{2}\right]$ إيديال نظاميّ مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$.

2) $\mathrm{I} = \left[p, \frac{p+\sqrt{\Delta}}{2}\right]$ إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ إذا وفقط إذا وجد حلّ للمعادلة

$|x^2-\Delta y^2|=4p$.

3) ليكن $x,y\in\mathbb{Z}$ بحيث $|x^2-\Delta y^2|=4p$ عندئذ $\left(\frac{x+y\sqrt{\Delta}}{2}\right)\mathcal{O}_\Delta = \left[p,\frac{p+\sqrt{\Delta}}{2}\right] = \mathrm{I}$.

الإثبات:

إثبات 1:

$\mathrm{I}=\left[p,\frac{p+\sqrt{\Delta}}{2}\right]$ إيديال في المرتّب التّربيعيّ $\mathcal{O}_\Delta$:

لأنّه لدينا $\mathrm{I}=\left[p,\frac{p+1\sqrt{\Delta}}{2}\right]$ ولنضع $a=p,b=p,e=1$

نلاحظ بأنّ $e\mid a$,$2e\mid e\Delta-b$,$4ae\mid b^2-\Delta e^2$ عندئذ I سيكون إيديال في $\mathcal{O}_\Delta$ وذلك حسب التّمهيديّة3.

$\mathrm{I}=\left[p,\frac{p+\sqrt{\Delta}}{2}\right]$ إيديال نظاميّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$:

بما أنّ $(p,d)=1$ عندئذ $\left(a,b,\frac{b^2-\Delta}{4a}\right)=\left(p,p,\frac{p-d}{4}\right)=1$

لأنّه لوكان $\left(p,p,\frac{p-d}{4}=\mathrm{d}_1\right)=p \Leftarrow p\mid \mathrm{d}_1 \Leftarrow p\mid d \Leftarrow (p,d)=p$ وهذا مرفوض

عندئذ بما أنّ $\left(a,b,\frac{b^2-\Delta}{4a}\right)=1$ و $e=1$ بالتالي I سيكون إيديال نظاميّ في $\mathcal{O}_\Delta$ بحسب التّمهيديّة 3.

$\mathrm{I}=\left[p,\frac{p+\sqrt{\Delta}}{2}\right]$ إيديال مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$:

بما أنّ $\mathrm{I}=\left[p,\frac{p+\sqrt{\Delta}}{2}\right]$ إيديال نظاميّ في $\mathcal{O}_\Delta$ عندئذ I سيكون إيديال مبهم وذلك حسب التّمهيديّة 4.

إثبات 2:

لزوم الشّرط:

لدينا $\mathrm{I}=\left[p,\frac{p+\sqrt{\Delta}}{2}\right]$ إيديال رئيسيّ في $\mathcal{O}_\Delta$ عندئذ يوجد $\alpha=\frac{u+v\sqrt{\Delta}}{2}\in\mathcal{O}_\Delta$ بحيث $\mathrm{I}=\alpha\mathcal{O}_\Delta$ ، ونجد أن:

$$p=N(\mathrm{I})=(\mathcal{O}_\Delta:\mathrm{I})=(\mathcal{O}_\Delta:\alpha\mathcal{O}_\Delta)=|n(\alpha)|=\frac{|u^2-\Delta v^2|}{4}\Longrightarrow |u^2-\Delta v^2|=4\,p$$

بالتّالي المعادلة $|x^2-\Delta y^2|=4p$ قابلة للحلّ.

كفاية الشّرط:

لدينا المعادلة $|x^2-\Delta y^2|=4p$ قابلة للحلّ عندئذ يوجد $u,v\in\mathbb{Z}$ بحيث $|u^2-\Delta v^2|=4p$

وبما أنّ $p\mid(u^2-\Delta v^2)$ و $p\mid\Delta v^2$ بالتّالي $p\mid u^2$ و $p\mid u$

$$\left|p\left(\frac{u}{p}\right)^2-dv^2\right|=4$$

نضع $X=\frac{u}{p}$ و $Y=v$ بالتّالي $|pX^2-dY^2|=4$

بما أنّ $\Delta\equiv 1mod4$ عندئذ $\mathcal{O}_\Delta$ يحوي إيديالات نظاميّة مبهمة معطاة بالصّيغة (II) فقط وذلك حسب التّمهيديّة 4

أيّ إنّ الإيديالات تعطى بالصّيغة الآتية : $\left(a,\frac{\Delta}{a}\right)=1\ \wedge\ a\mid\Delta\ \wedge\ a\in\mathbb{N}\ ;\left[a\,,\frac{a+\sqrt{\Delta}}{2}\right]$.

ولدينا $\mathrm{I}=\left[p,\frac{p+\sqrt{\Delta}}{2}\right]$ إيديال نظاميّ مبهم معطى بالصّيغة (II) .

وبما أنّه يوجد $Y,X \in \mathbb{Z}$ بحيث $|pX^2 - dY^2| = 4$ بالتّالي حسب التّمهيديّة 6 يكون I إيديال رئيسيّ في $\mathcal{O}_\Delta$.

إثبات 3:

لدينا $x,y \in \mathbb{Z}$ بحيث $|x^2 - \Delta y^2| = 4p$ عندئذ x,y زوجيان معا أوفرديان معا بالتّالي $2 \mid x - y$

بما أنّ $p \mid (x^2 - \Delta y^2)$ و $p \mid \Delta y^2$ بالتّالي $p \mid x^2$ و $p \mid x$

ينتج عن ذلك أنّ

$$x = px_1 \; ; \; x_1 \in \mathbb{Z}$$

$$\Rightarrow \frac{x + y\sqrt{\Delta}}{2} = \frac{px_1 + y\sqrt{\Delta}}{2} = p\left(\frac{x_1 - y}{2}\right) + y\left(\frac{p + \sqrt{\Delta}}{2}\right) \in \mathrm{I} = \left[p, \frac{p + \sqrt{\Delta}}{2}\right]$$

$$\Rightarrow \left(\frac{x + y\sqrt{\Delta}}{2}\right)\mathcal{O}_\Delta \subset \mathrm{I}$$

من جهة أخرى:

$$\mathrm{N}\left(\left(\frac{x + y\sqrt{\Delta}}{2}\right)\mathcal{O}_\Delta\right) = \left(\mathcal{O}_\Delta : \left(\frac{x + y\sqrt{\Delta}}{2}\right)\mathcal{O}_\Delta\right) = \frac{|x^2 - \Delta y^2|}{4} = p = \mathrm{N}(\mathrm{I})$$

$$\Rightarrow \left(\mathcal{O}_\Delta : \left(\frac{x + y\sqrt{\Delta}}{2}\right)\mathcal{O}_\Delta\right) = (\mathcal{O}_\Delta : \mathrm{I}) \Rightarrow \mathrm{I} = \left(\frac{x + y\sqrt{\Delta}}{2}\right)\mathcal{O}_\Delta$$

مبرهنة2:

ليكن p عدداً أوّليّاً فرديّاً .

وليكن $\Delta = 4D > 0$ مميّز تربيعي بحيث $D \equiv 1 mod4$ و $D = pd$ و $(p,d) = 1$.

عندئذ :

1) $\mathrm{I} = [p, \sqrt{D}]$ إيديال نظاميّ مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$.

2) $\mathrm{I} = [p, \sqrt{D}]$ إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ إذا وفقط إذا وجد حلّ للمعادلة $|x^2 - Dy^2| = p$.

3) ليكن $x,y \in \mathbb{Z}$ بحيث $|x^2 - Dy^2| = p$ عندئذ $\mathrm{I} = [p, \sqrt{D}] = (x + y\sqrt{D})\mathcal{O}_\Delta$.

الإثبات:

إثبات1:

<u>$\mathrm{I} = [p, \sqrt{D}]$إيديال في المرتّب التّربيعيّ $\mathcal{O}_\Delta$</u> :

لأنّه لدينا $\mathrm{I} = [p, \sqrt{D}] = \left[p, \frac{0 + \sqrt{\Delta}}{2}\right]$ ولنضع $a = p, b = 0, e = 1$

ونلاحظ بأنّ $e \mid a \,,\; 2e \mid e\Delta - b \,, 4ae \mid b^2 - \Delta e^2$ عندئذ I إيديال في $\mathcal{O}_\Delta$ وذلك حسب التّمهيديّة 3.

<u>$\mathrm{I} = [p, \sqrt{D}]$إيديال نظاميّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$</u> :

لأنّه لدينا $\left(a, b, \frac{b^2 - \Delta}{4a}\right) = \left(p, 0, \frac{b^2 - \Delta}{4a} = -d\right) = 1$ و $e = 1$ بالتّالي I إيديال نظاميّ في $\mathcal{O}_\Delta$ وذلك حسب التّمهيديّة 3 .

$\mathrm{I}=[p,\sqrt{D}]$إيديال مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$:

لأنّه لدينا $\mathrm{I}=[p,\sqrt{D}]$ إيديال نظاميّ في $\mathcal{O}_\Delta$ عندئذ I سيكون إيديال مبهم وذلك حسب التّمهيديّة 4.

إثبات2:

لزوم الشّرط:

لدينا $\mathrm{I}=[p,\sqrt{D}]$ إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ عندئذ يوجد $\alpha=\frac{x_1+y_1\sqrt{\Delta}}{2}\in\mathcal{O}_\Delta$ بحيث $\mathrm{I}=\alpha\mathcal{O}_\Delta$

بما أنّ $\alpha\in\mathcal{O}_\Delta$ عندئذ $x_1,y_1\in\mathbb{Z}$ و $x_1\equiv y_1\Delta mod2$

$\Longrightarrow 2\mid x_1-y_1\Delta\Longrightarrow 2\mid x_1$

نضع $\frac{x_1}{2}=u$ و $y_1=v$

$$\Longrightarrow\alpha=\frac{x_1+y_1\sqrt{\Delta}}{2}=\frac{x_1}{2}+y_1\sqrt{D}=u+v\sqrt{D}\Longrightarrow\mathrm{I}=\left(u+v\sqrt{D}\right)\mathcal{O}_\Delta$$

$$p=N(\mathrm{I})=(\mathcal{O}_\Delta:\mathrm{I})=(\mathcal{O}_\Delta:\alpha\mathcal{O}_\Delta)=|n(\alpha)|=|u^2-Dv^2|$$

بالتّالي المعادلة $|x^2-Dy^2|=p$ قابلة للحلّ.

كفاية الشّرط:

لدينا المعادلة $|x^2-Dy^2|=p$ قابلة للحلّ عندئذ يوجد $u,v\in\mathbb{Z}$ بحيث $|u^2-Dv^2|=p$

وبما أن $p\mid(u^2-Dv^2)$ و $p\mid Dv^2$ بالتّالي $p\mid u^2$ و $p\mid u$

$$\left|p\left(\frac{u}{p}\right)^2-dv^2\right|=1$$

نضع $X=\frac{u}{p}$ و $Y=v$ بالتالي $|pX^2-dY^2|=1$

لدينا $\Delta=4D$ و $D\not\equiv 3mod4$ و $8\nmid D$ عندئذ $\mathcal{O}_\Delta$ لايحوي إيديالات نظاميّة مبهمة معطاة بالصّيغة (II) وذلك حسب التّمهيديّة 4 .

وبما أنّ $\Delta=4D$ عندئذ $\mathcal{O}_\Delta$ يحوي إيديالات نظاميّة مبهمة معطاة بالصّيغة (I) وذلك حسب التّمهيديّة 4

أيّ إنّ الإيديالات تعطى بالصّيغة الآتية : $\left[a,\sqrt{D}\right];a\in\mathbb{N}\wedge a\mid D\wedge\left(a,\frac{D}{a}\right)=1$

ولدينا $\mathrm{I}=[p,\sqrt{D}]$ إيديال نظاميّ مبهم معطى بالصّيغة (I).

وبما أنّه يوجد $Y,X\in\mathbb{Z}$ بحيث $|pX^2-dY^2|=1$ و $(1,YX)=1$ عندئذ حسب التّمهيديّة 5 نجد بأنّ I إيديال رئيسيّ في $\mathcal{O}_\Delta$

إثبات 3:

لدينا $x,y\in\mathbb{Z}$ بحيث $|x^2-Dy^2|=p$ وبما أنّ $p\mid(x^2-\mathrm{D}y^2)$ و $p\mid\mathrm{D}y^2$ بالتّالي $p\mid x^2$ و $p\mid x$

$\Longrightarrow x=px_1;x_1\in\mathbb{Z}$

$$\Longrightarrow x+y\sqrt{D}=px_1+y\sqrt{D}\in\mathrm{I}=[p,\sqrt{D}]\Longrightarrow\left(x+y\sqrt{D}\right)\mathcal{O}_\Delta\subset\mathrm{I}=[p,\sqrt{D}]$$

$$\mathrm{N}\left(\left(x+y\sqrt{D}\right)\mathcal{O}_\Delta\right)=\left(\mathcal{O}_\Delta:\left(x+y\sqrt{D}\right)\mathcal{O}_\Delta\right)=|x^2-Dy^2|=p=\mathrm{N}(\mathrm{I})$$

$$\Longrightarrow\left(\mathcal{O}_\Delta:\left(x+y\sqrt{D}\right)\mathcal{O}_\Delta\right)=(\mathcal{O}_\Delta:\mathrm{I})\Longrightarrow\mathrm{I}=\left(x+y\sqrt{D}\right)\mathcal{O}_\Delta$$

مبرهنة3:

ليكن p عدداً أوّليّاً بحيث $p \equiv 3mod4$ و $8 \nmid (p+1)$.

وليكن $\Delta = 4D$ مميّز أساسيّ بحيث $D \equiv 2mod4$ و $D = pd$.

عندئذ :

1) $\mathrm{I} = [p, \sqrt{D}]$ إيديال نظاميّ مبهم في المرتّب التربيعيّ $\mathcal{O}_\Delta$.

2) $\mathrm{I} = [p, \sqrt{D}]$ إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ إذا وفقط إذا وجد حلّ للمعادلة $x^2 - Dy^2 = p$.

3) ليكن $x, y \in \mathbb{Z}$ بحيث $x^2 - Dy^2 = p$ عندئذ $\mathrm{I} = [p, \sqrt{D}] = (x + y\sqrt{D})\mathcal{O}_\Delta$.

الإثبات:

إثبات1:

<u>$\mathrm{I} = [p, \sqrt{D}]$إيديال في المرتّب التّربيعيّ $\mathcal{O}_\Delta$</u> :

لأنّه لدينا $\mathrm{I} = [p, \sqrt{D}] = \left[p, \frac{0+\sqrt{\Delta}}{2}\right]$ ولنضع $a = p, b = 0, e = 1$

نلاحظ بأنّ $e \mid a\ ,\ \ 2e \mid e\Delta - b\ , 4ae \mid b^2 - \Delta e^2$ عندئذ I سيكون إيديال في $\mathcal{O}_\Delta$ بحسب التّمهيديّة 3.

<u>$\mathrm{I} = [p, \sqrt{D}]$إيديال نظاميّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$</u> :

لأنّه لدينا $\Delta = 4D$ مميّز أساسيّ عندئذ $D = pd$ حرّ من التّربيع بالتّالي $(p, d) = 1$

وبما أنّ $\left(a, b, \frac{b^2-\Delta}{4a}\right) = \left(p, 0, \frac{b^2-\Delta}{4a} = -d\right) = 1$ و $e = 1$ بالتّالي I سيكون إيديال نظاميّ في $\mathcal{O}_\Delta$ بحسب التّمهيديّة 3.

<u>$\mathrm{I} = [p, \sqrt{D}]$إيديال مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$</u> :

بما أنّ $\mathrm{I} = [p, \sqrt{D}]$ إيديال نظاميّ في $\mathcal{O}_\Delta$ بالتالي I سيكون مبهم وذلك حسب التّمهيديّة 4.

إثبات 2:

لزوم الشّرط:

$\mathrm{I} = [p, \sqrt{D}]$ إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ عندئذ يوجد $\alpha = \frac{x_1 + y_1\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta$ بحيث $\mathrm{I} = \alpha\mathcal{O}_\Delta$

بما أنّ $\alpha \in \mathcal{O}_\Delta$ عندئذ $x_1, y_1 \in \mathbb{Z}$ و $x_1 \equiv y_1\Delta mod2$

$\Rightarrow 2 \mid x_1 - y_1\Delta \Rightarrow 2 \mid x_1$

نضع $\frac{x_1}{2} = u$ و $y_1 = v$

$$\Rightarrow \alpha = \frac{x_1 + y_1\sqrt{\Delta}}{2} = \frac{x_1}{2} + y_1\sqrt{D} = u + v\sqrt{D} \Rightarrow \mathrm{I} = (u + v\sqrt{D})\mathcal{O}_\Delta$$

$$p = N(\mathrm{I}) = (\mathcal{O}_\Delta : \mathrm{I}) = (\mathcal{O}_\Delta : \alpha\mathcal{O}_\Delta) = |n(\alpha)| = |u^2 - Dv^2|$$

بالتّالي $u^2 - Dv^2 = p$ فقط

لأنّه لوكان $u^2 - Dv^2 = -p$ عندئذ (u فرديّ و v زوجيّ) و (u فرديّ و v فرديّ)

فإذا كان u فرديّاً و v زوجيّاً :

عندئذ $v^2 \equiv 0or4mod8$ و $u^2 \equiv 1mod8$ بالتّالي $Dv^2 \equiv 0mod8$

$$Dv^2 = u^2 + p \equiv 1 + pmod8 \Longrightarrow 0 \equiv 1 + pmod8$$

وبالتّالي $(p+1) \mid 8$ وهذا مرفوض .

وإذا كان u فرديّاً و v فرديّاً :

عندئذ $u^2 \equiv 1mod4$ و $v^2 \equiv 1mod4$ بالتّالي $-p = u^2 - Dv^2 \equiv 1 - 2 \times 1mod4$

بالتّالي $p \equiv 1mod4$ وهذا أيضاً مرفوض .

ممّا سبق نجد بأنّ المعادلة $x^2 - Dy^2 = p$ قابلة للحلّ فقط.

كفاية الشّرط:

لدينا المعادلة $x^2 - Dy^2 = p$ قابلة للحلّ عندئذ يوجد $u, v \in \mathbb{Z}$ بحيث $u^2 - Dv^2 = p$

وبما أنّ $p \mid (u^2 - \mathrm{D}v^2)$ و $p \mid \mathrm{D}v^2$ عندئذ $p \mid u^2$ و $p \mid u$

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

نضع $X = \frac{u}{p}$ و $Y = v$ بالتالي $pX^2 - dY^2 = 1$

لدينا $\Delta = 4D$ و $D \not\equiv 3mod4$ و $8 \nmid D$ عندئذ $\mathcal{O}_\Delta$ لايحوي إيديالات نظاميّة مبهمة معطاة بالصّيغة (II) وذلك حسب التّمهيديّة 4.

بما أنّ $\Delta = 4D$ عندئذ حسب التّمهيديّة 4 المرتّب التّربيعيّ $\mathcal{O}_\Delta$ يحوي إيديالات نظاميّة مبهمة معطاة بالصّيغة (I)أيّ الإيديالات المعطاة بالصّيغة التّالية : $\left(a, \frac{D}{a}\right) = 1 \ \wedge \ a \mid D \wedge a \in \mathbb{N} ; [a, \sqrt{D}]$.

ولدينا $\mathrm{I} = [p, \sqrt{D}]$ إيديال نظاميّ مبهم معطى بالصّيغة (I)

وبما أنّه يوجد $Y, X \in \mathbb{Z}$ بحيث $pX^2 - dY^2 = 1$ و $(1, YX) = 1$ عندئذ حسب التّمهيديّة 5 نجد بأنّ I إيديال رئيسيّ في $\mathcal{O}_\Delta$.

إثبات 3:

لدينا $x, y \in \mathbb{Z}$ بحيث $x^2 - Dy^2 = p$ وبما أنّ $p \mid (x^2 - \mathrm{D}y^2)$ و $p \mid \mathrm{D}y^2$ بالتّالي $p \mid x^2$ و $p \mid x$

$$\Longrightarrow x = px_1 ; x_1 \in \mathbb{Z}$$

$$\Longrightarrow x + y\sqrt{D} = px_1 + y\sqrt{D} \in \mathrm{I} = [p, \sqrt{D}] \Longrightarrow (x + y\sqrt{D})\mathcal{O}_\Delta \subset \mathrm{I} = [p, \sqrt{D}]$$

$$\mathrm{N}\left((x + y\sqrt{D})\mathcal{O}_\Delta\right) = \left(\mathcal{O}_\Delta : (x + y\sqrt{D})\mathcal{O}_\Delta\right) = |x^2 - Dy^2| = p = \mathrm{N}(\mathrm{I})$$

$$\Longrightarrow \left(\mathcal{O}_\Delta : (x + y\sqrt{D})\mathcal{O}_\Delta\right) = (\mathcal{O}_\Delta : \mathrm{I}) \Longrightarrow \mathrm{I} = (x + y\sqrt{D})\mathcal{O}_\Delta$$

مبرهنة 4 :

ليكن p عدداً أوّليّاً بحيث $p \equiv 3mod4$.

وليكن $\Delta = 4D$ مميّز أساسيّ بحيث $D \equiv 3mod4$ و $D = pd$.

عندئذ :

1) $\mathrm{I} = [p, \sqrt{D}]$ إيديال نظاميّ مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$.

2) $\mathrm{I} = [p, \sqrt{D}]$ إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ إذا وفقط إذا وجد حلّ للمعادلة

.$x^2 - Dy^2 = -p$

3) ليكن $x, y \in \mathbb{Z}$ بحيث $x^2 - Dy^2 = -p$ عندئذ $I = [p, \sqrt{D}] = (x + y\sqrt{D})\mathcal{O}_\Delta$

الإثبات:

إثبات 1:

$I = [p, \sqrt{D}]$ إيديال في المرتّب التّربيعيّ $\mathcal{O}_\Delta$:

لأنّه لدينا $I = [p, \sqrt{D}] = \left[p, \frac{0+\sqrt{\Delta}}{2}\right]$ ولنضع $a = p, b = 0, e = 1$

نلاحظ بأنّ $e \mid a\,,\ 2e \mid e\Delta - b\,, 4ae \mid b^2 - \Delta e^2$ عندئذ سيكون I إيديال في $\mathcal{O}_\Delta$ بحسب التّمهيديّة 3 .

$I = [p, \sqrt{D}]$ إيديال نظاميّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$:

لأنّه لدينا $\Delta = 4D$ مميّز أساسيّ عندئذ $D = pd$ حّرمن التّربيع بالتّالي $(p, d) = 1$

وبما أنّ $\left(a, b, \frac{b^2-\Delta}{4a}\right) = \left(p, 0, \frac{b^2-\Delta}{4a} = -d\right) = 1$ و $e = 1$ بالتّالي I سيكون نظامي في $\mathcal{O}_\Delta$ بحسب التّمهيديّة 3 .

$I = [p, \sqrt{D}]$ إيديال مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$:

بما أنّ $I = [p, \sqrt{D}]$ إيديال نظاميّ في $\mathcal{O}_\Delta$عندئذ I سيكون إيديال مبهم وذلك حسب التّمهيديّة 4 .

إثبات 2:

لزوم الشّرط:

$I = [p, \sqrt{D}]$ إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ عندئذ يوجد $\alpha = \frac{x_1+y_1\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta$ بحيث $I = \alpha\mathcal{O}_\Delta$

بما أنّ $\alpha \in \mathcal{O}_\Delta$ عندئذ $x_1, y_1 \in \mathbb{Z}$ و $x_1 \equiv y_1\Delta mod 2$

$\Rightarrow 2 \mid x_1 - y_1\Delta \Rightarrow 2 \mid x_1$

نضع $\frac{x_1}{2} = u$ و $y_1 = v$

$$\Rightarrow \alpha = \frac{x_1 + y_1\sqrt{\Delta}}{2} = \frac{x_1}{2} + y_1\sqrt{D} = u + v\sqrt{D} \Rightarrow I = (u + v\sqrt{D})\mathcal{O}_\Delta$$

$$p = N(I) = (\mathcal{O}_\Delta : I) = (\mathcal{O}_\Delta : \alpha\mathcal{O}_\Delta) = |n(\alpha)| = |u^2 - Dv^2|$$

بالتّالي $u^2 - Dv^2 = -p$ فقط

لأنّه لوكان $u^2 - Dv^2 = p$ عندئذ إما (u زوجيّ و v فرديّ) أو (u فرديّ و v زوجيّ).

فإذا كان u زوجيّاً و v فرديّاً عندئذ $v^2 \equiv 1 mod 4$ و $u^2 \equiv 0 mod 4$

$$\Rightarrow p = u^2 - Dv^2 \equiv (0 - 3 \times 1) mod 4$$

بالتّالي $p \equiv 1 mod 4$ وهذا مرفوض .

وإذا كان u فرديّاً و v زوجيّاً عندئذ $v^2 \equiv 0 mod 4$ و $u^2 \equiv 1 mod 4$

$$\Rightarrow p = u^2 - Dv^2 \equiv (1 - 3 \times 0) mod 4$$

بالتّالي $p \equiv 1 mod 4$ وهذا أيضاً مرفوض .

مما سبق نجد بأنّ المعادلة $x^2 - Dy^2 = -p$ قابلة للحلّ فقط .

كفاية الشّرط:

لدينا المعادلة $x^2 - Dy^2 = -p$ قابلة للحلّ عندئذ يوجد $u, v \in \mathbb{Z}$ بحيث $u^2 - Dv^2 = -p$

وبما أنّ $p \mid (u^2 - \mathrm{D}v^2)$ و $p \mid \mathrm{D}v^2$ بالتّالي $p \mid u^2$ و $p \mid u$

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

لدينا $\Delta = 4D$ عندئذ $\mathcal{O}_\Delta$ يحوي إيديالات نظاميّة مبهمة معطاة بالصّيغة ($\mathbb{I}$) وذلك حسب التّمهيديّة 4

أيّ إنّ الإيديالات تعطى بالصّيغة: $[a, \sqrt{D}]\,; a \in \mathbb{N} \wedge a \mid D \wedge \left(a, \frac{D}{a}\right) = 1$

ولدينا $\mathrm{I} = [p, \sqrt{D}]$ إيديال نظاميّ مبهم معطى بالصّيغة ($\mathbb{I}$) .

وبما أنّه يوجد $Y, X \in \mathbb{Z}$ بحيث $pX^2 - dY^2 = -1$ و $(1, YX) = 1$ عندئذ حسب التّمهيديّة 5 نجد بأن I إيديال رئيسيّ في $\mathcal{O}_\Delta$.

إثبات 3:

لدينا $x, y \in \mathbb{Z}$ بحيث $x^2 - Dy^2 = -p$ وبما أنّ $p \mid (x^2 - \mathrm{D}y^2)$ و $p \mid \mathrm{D}y^2$ بالتّالي $p \mid x^2$ و $p \mid x$

$$\Rightarrow x = px_1\,; x_1 \in \mathbb{Z}$$

$$\Rightarrow x + y\sqrt{D} = px_1 + y\sqrt{D} \in \mathrm{I} = [p, \sqrt{D}] \Rightarrow (x + y\sqrt{D})\mathcal{O}_\Delta \subset \mathrm{I} = [p, \sqrt{D}]$$

$$\mathrm{N}\left((x + y\sqrt{D})\mathcal{O}_\Delta\right) = \left(\mathcal{O}_\Delta : (x + y\sqrt{D})\mathcal{O}_\Delta\right) = |x^2 - Dy^2| = p = \mathrm{N}(\mathrm{I})$$

$$\Rightarrow \left(\mathcal{O}_\Delta : (x + y\sqrt{D})\mathcal{O}_\Delta\right) = (\mathcal{O}_\Delta : \mathrm{I}) \Rightarrow \mathrm{I} = (x + y\sqrt{D})\mathcal{O}_\Delta$$

مبرهنة5 :

ليكن p عدداً أوّليّاً فرديّاً .

وليكن $\Delta = 4D$ مميّز أساسيّ بحيث $D \equiv 3 mod4$ و $D = pd$.

عندئذ :

1) $\mathrm{I} = [2p, p + \sqrt{D}]$ إيديال نظاميّ مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$.

2) $\mathrm{I} = [2p, p + \sqrt{D}]$ إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ إذا وفقط إذا وجد حلّ للمعادلة $|x^2 - Dy^2| = 2p$.

3) ليكن $x, y \in \mathbb{Z}$ بحيث $|x^2 - Dy^2| = 2p$ عندئذ $\mathrm{I} = [2p, p + \sqrt{D}] = (x + y\sqrt{D})\mathcal{O}_\Delta$

الإثبات: نثبت اولا 1:

<u>$\mathrm{I} = [2p, p + \sqrt{D}]$إيديال في المرتّب التّربيعيّ $\mathcal{O}_\Delta$:</u>

لأنّه لدينا $\mathrm{I} = [2p, p + \sqrt{D}] = \left[2p, \frac{2p + \sqrt{\Delta}}{2}\right]$ ولنضع $a = 2p, b = 2p, e = 1$

نلاحظ بأنّ $e \mid a,\ \ 2e \mid e\Delta - b\,, 4ae \mid b^2 - \Delta e^2$ عندئذ يكون I إيديال في $\mathcal{O}_\Delta$ بحسب التّمهيديّة 3.

<u>$\mathrm{I} = [2p, p + \sqrt{D}]$إيديال نظاميّ في المرتّب التربيعيّ $\mathcal{O}_\Delta$:</u>

لأنّه لدينا $\Delta = 4D$ مميّز أساسيّ عندئذ $D = pd$ حرّ من التّربيع بالتّالي $(p, d) = 1$

وبما أنّ $\left(2p, 2p, \frac{p-d}{2}\right) = 1$ و $\left(a, b, \frac{b^2-\Delta}{4a}\right)$ و $e = 1$ بالتّالي I سيكون إيديال نظاميّ في $\mathcal{O}_\Delta$ بحسب التّمهيديّة 3.

إيديال مبهم في المرتّب التّربيعيّ $\mathcal{O}_\Delta$: $I = [2p, p + \sqrt{D}]$

بما أنّ $I = [2p, p + \sqrt{D}]$ إيديال نظاميّ في $\mathcal{O}_\Delta$ عندئذ I سيكون مبهم بحسب التّمهيديّة 4.

إثبات2:

لزوم الشرط:

إيديال رئيسيّ في المرتّب التّربيعيّ $\mathcal{O}_\Delta$ عندئذ يوجد $\alpha = \frac{x_1+y_1\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta$ بحيث $I = [2p, p + \sqrt{D}]$

$I = \alpha\mathcal{O}_\Delta$

وبما أنّ $\alpha \in \mathcal{O}_\Delta$ عندئذ $x_1, y_1 \in \mathbb{Z}$ و $x_1 \equiv y_1 \Delta mod 2$

يؤدي ذلك إلى أنّ

$2 \mid x_1 - y_1\Delta \Rightarrow 2 \mid x_1$

نضع $\frac{x_1}{2} = u$ و $y_1 = v$

$$\Rightarrow \alpha = \frac{x_1 + y_1\sqrt{\Delta}}{2} = \frac{x_1}{2} + y_1\sqrt{D} = u + v\sqrt{D} \Rightarrow I = \left(u + v\sqrt{D}\right)\mathcal{O}_\Delta$$

$$2p = N(I) = (\mathcal{O}_\Delta : I) = (\mathcal{O}_\Delta : \alpha\mathcal{O}_\Delta) = |n(\alpha)| = |u^2 - Dv^2|$$

بالتّالي المعادلة $|x^2 - Dy^2| = 2p$ قابلة للحلّ .

كفاية الشّرط:

لدينا المعادلة $|x^2 - Dy^2| = 2p$ قابلة للحلّ عندئذ يوجد $u, v \in \mathbb{Z}$ بحيث $|u^2 - Dv^2| = 2p$

وبما أنّ $p \mid (u^2 - Dv^2)$ و $p \mid Dv^2$ بالتّالي $p \mid u^2$ و $p \mid u$

$$\left|p\left(\frac{u}{p}\right)^2 - dv^2\right| = 2$$

نضع $X = \frac{u}{p}$ و $Y = v$ بالتّالي $|pX^2 - dY^2| = 2$

لدينا $\Delta = 4D$ و $D \equiv 3 mod 4$ عندئذ $\mathcal{O}_\Delta$ يحوي إيديالات نظاميّة مبهمة معطاة بالصّيغة (II) بحسب التّمهيديّة 4 .

أيّ أنّ الإيديالات تأخذ الصّيغة : $I = [2a, a + \sqrt{D}];\ \ a \in \mathbb{N} \wedge a \mid D \wedge \left(a, \frac{D}{a}\right) = 1$

ولدينا $I = [2p, p + \sqrt{D}]$ إيديال نظاميّ مبهم معطى بالصّيغة (II) .

وبما أنّه يوجد $Y, X \in \mathbb{Z}$ بحيث $|pX^2 - dY^2| = 2$ و $(1, YX) = 1$ عندئذ حسب التّمهيديّة 5 نجد أنّ I إيديال رئيسيّ في $\mathcal{O}_\Delta$.

إثبات 3:

لدينا $x, y \in \mathbb{Z}$ بحيث $|x^2 - Dy^2| = 2p$ وبما أنّ $p \mid (x^2 - Dy^2)$ و $p \mid Dy^2$ بالتّالي $p \mid x^2$ و $p \mid x$

يؤدي ذلك إلى أنّ:

$x = px_1 ; x_1 \in \mathbb{Z}$

وبما أنّ المعادلة $|x^2 - Dy^2| = 2p$ قابلة للحلّ عندئذ x, y فرديّان معاً بالتّالي x_1 فرديّ ومنه نجد أنّ

$$x_1 - y = 2u$$

يؤدي ذلك

$$x + y\sqrt{D} = px_1 + y\sqrt{D} = p(2u + y) + y\sqrt{D} = 2pu + y(p + \sqrt{D}) \in \mathrm{I}$$
$$\Rightarrow (x + y\sqrt{D})\mathcal{O}_\Delta \subset \mathrm{I}$$
$$\mathrm{N}\left((x + y\sqrt{D})\mathcal{O}_\Delta\right) = \left(\mathcal{O}_\Delta : (x + y\sqrt{D})\mathcal{O}_\Delta\right) = |x^2 - Dy^2| = 2p = \mathrm{N(I)}$$
$$\Rightarrow \left(\mathcal{O}_\Delta : (x + y\sqrt{D})\mathcal{O}_\Delta\right) = (\mathcal{O}_\Delta : \mathrm{I}) \Rightarrow \mathrm{I} = (x + y\sqrt{D})\mathcal{O}_\Delta$$

الاستنتاجات والتّوصيات:

توصلنا في هذه المقالة إلى شروط لازمة وكافية لقابليّة حلّ معادلة بل $x^2 - \Delta y^2 = N$ بالإعتماد على الإيديالات في المرتّبات التّربيعيّة ، كما أعطينا صيغة الإيديال المقابل لكلّ حلّ لهذه المعادلة وذلك من أجل بعض الحالات الخاصّة لـ N و Δ .

أمّا بالنّسبة للتّوصيات: نوصي بدراسة قابليّة حلّ معادلة بل في حالات أكثر عموميّة (مثلاً $\Delta = 4D$ مميّز تربيعيّ و $D = dd^*$) بالاعتماد على نظريّة الإيديالات في المرتّبات التّربيعيّة .

المراجع

1) ANDREESCU, T., ANDRICA, D., *Quadratic Diophantine Equations*, Springer, New York, London, 2015.

2) BOLKER, E. D. *Elementary Number Theory*, An Algebraic Approach, W. A. Bedjamin, Inc. New York, 1970.

3) COVILL. E., JAVAHERI, M., KRYLO. N., *On the Subgroup Generated by Solutions of Pell's Equation*, Arxiv: 1609.00440vol.1, math. NT, 2Sep,2016.

4) HALTER-KOCH. F. *Quadratic Irrationals: An introduction to Classical Number Theory*, Taylor & Francis Group, University of Graz Austria, 2013.

5) HALTER-KOCH. F. *Diophantine Equations of Pellian Type*, J. Number Theory, vol131,2011,pp.1597-1615.

6) HOQUE. A and CHAKRABORTY. K., *Pell-Type Equations and Class Number of The Maximal Real Subfield of A Cyclotomic Field*, Arxiv: 1710.09760, vol.1 ,math. NT, 26Oct, 2017.

7) MATTHEWS, K. *The Diophantine Equation* $ax^2 + bxy + cy^2 = N, D = b^2 - 4ac > 0$, J. Th'eor. Numbres Bordeaux, vol.14, no.1,2002, pp.257-270.

8) MOLLIN, R.A. *Ideal Criteria for Both* $x^2 - Dy^2 = m_1$ *and* $x^2 - Dy^2 = m_2$ *to Have Primitive Solutions for any Integers* m_1 , m_2 *Prime to* $D > 0$, Serdica Math. J, vol.28, 2002, pp. 175-188.