مجلة جامعة تشرين للبحوث والدراسات العلمية – سلسلة العلوم الأساسية المجلد (39) العدد (3) 2017
Tishreen University Journal for Research and Scientific Studies - Basic Sciences Series Vol. (39) No. (3) 2017

حل المعادلات الديوفانتية $y^2 = x^3 + Dx$ حيث $D \equiv 5(mod\ 8)$

د. حسن سنكري*
مصطفى بوجقلي**

(تاريخ الإيداع 18 / 12 / 2016. قُبِل للنشر في 3 / 5 /2017)

□ ملخّص □

درسنا في هذا البحث المعادلات الديوفانتية من الشكل $y^2 = x^3 + Dx$ التي تشكل تشاكلات جبرية في الفضاء الإسقاطي و التي تمثل هندسياً أسرة من المنحنيات الاهليلجية في الحقل k إضافة إلى بناء إيزومورفيزم مسطح و غير متشعب بين أسرة هذه المنحنيات الاهليلجية و مجموعة جزئية من حلقة الأعداد الصحيحة و منه إيجاد توسيع أعظمي منتهي غير متشعب للحقل k و تحديد عدد النقاط ذات الرتب المنتهية و الرتبة ∞ لهذه الأسرة و التي استطعنا من خلالها تحديد قيم D التي تكون من أجلها رتبة المنحني الاهليلجي فوق الحقل k تساوي 1 و بالتالي حل المعادلة الديوفانتية $y^2 = x^3 + Dx$ من أجل هذه القيم.

الكلمات المفتاحية: الفضاء الاسقاطي – المنحنيات الاهليلجية – الزمر الهمولوجية – الزمرة المخططة – المورفيزم إيتال – حلقة الأعداد الصحيحة.

* أستاذ مساعد – قسم الرياضيات – كلية العلوم – جامعة تشرين – اللاذقية – سورية
** طالب ماجستير – قسم الرياضيات – كلية العلوم – جامعة تشرين – اللاذقية – سورية

مجلة جامعة تشرين للبحوث والدراسات العلمية – سلسلة العلوم الأساسية المجلد (39) العدد (3) 2017
Tishreen University Journal for Research and Scientific Studies - Basic Sciences Series Vol. (39) No. (3) 2017

Solving the Diophantine equations $y^2 = x^3 + Dx$ where $D \equiv 5(mod\ 8)$

Dr. Hasan Sankari[*]
Mustafa bojakli[**]

(Received 18 / 12 / 2016. Accepted 3 / 5 /2017)

□ ABSTRACT □

In this research, we study the Diophantine equations of the form $y^2 = x^3 + Dx$ which constitute algebraically abelian variety in projective space and represent, in geometric form, family of elliptic curves over field k, besides to building isomorphism between this elliptic curve and subset of ring of integrals, thus find the maximal finite extension for field k and determine the number of points that are finite torsion and torsion ∞ to this family in which we can determine some value of D such that the rank of elliptic curve above the field k equal to one.

Keywords: projective space – elliptic curve – homology group – scheme group – etale morphism – ring of integrals.

[*]**Assistant Professor – Department of Mathematics – Faculty of Science – Tishreen University – Lattakia – Syria.**
[**] **Postgraduate student – Department of Mathematics – Faculty of Science – Tishreen University – Lattakia – Syria .**

مقدمة:

تعتبر المنحنيات الاهليلجية وسيلة هامة وضرورية في إيجاد حلول كثير من المعادلات الديوفانتية حيث قام العالم هنري بوينكاري Henri Poincare في عام 1901 باستخدامها في تصنيف المعادلات التكعيبية والعالم ويلس Wiles في عام 1954 في حل معادلة موردل $y^2 = x^3 + a$ من أجل بعض القيم الصحيحة لـ a، وتعتبر مبرهنة موردل – ويل (Mordell – Weil) $E(k) = E(k)_{tors} \oplus \mathbb{Z}^r$ المبرهنة الأساسية في المنحنيات الاهليلجية حيث أن $E(k)_{tors} = \coprod_{m>1} E[m]$ و r هي رتبة المنحني الاهليلجي حيث أنه لا توجد إلى اليوم طريقة لإيجاد رتبة المنحني الاهليلجي وخوارزمية لتحديد مولدات الزمرة $E(k)$ اللتين تعتبران من المسائل المفتوحة في المنحنيات الاهليلجية.

أهمية البحث وأهدافه:

تكمن أهمية البحث في أن التشاكلات الجبرية والمنحنيات الجبرية لهما نفس البنية الجبرية فكلاهما يشكل زمرة تبديلية ونفس البنية الهندسية فكلاهما منحني إسقاطي أملس.

ويهدف البحث إلى:

○معرفة عدد الحلول للمعادلات الديوفانتية ذات الرتب المنتهية والتي تشكل زمرة بالنسبة لعملية الجمع المعرفة على المنحنيات الاهليلجية.

○معرفة عدد النقاط على المنحني الاهليلجي التي رتبتها ∞ والتي تحدد رتبة المنحني الاهليلجي والتي لا تقع ضمن الزمرة $E[m]$.

طرائق البحث ومواده:

يشمل البحث مبرهنات تربط بين الهندسة الجبرية والهمولوجيا ونظرية الأعداد الجبرية والتبولوجيا الجبرية ونظرية الحقول وتستند بشكل أساسي على الزمر الهمولوجية التي عناصرها مورفيزمات لها خواص جبرية وهندسية بالإضافة إلى التوسيعات الجبرية للحقل k عند نقاط في $\mathcal{O}_k$ التي يكون عندها المنحني الاهليلجي شاذاً.

بعض الرموز والمصطلحات المستخدمة في البحث:

إن جميع الرموز والتعاريف المستخدمة في هذه المقالة واردة ومعتمدة في جميع المراجع العلمية المختصة في الجبر ونذكر منها على سبيل المثال **[1]** و**[2]** و**[3]** و**[4]**:

- k حقل و $\overline{k}$ الإغلاق الجبري لـ k.
- $k[X] = k[x_1, \dots, x_n]$ كثيرة حدود بـ n متحول.
- $\mathbb{A}_k^n$ الفضاء الأفيني و $\mathbb{P}_k^n$ الفضاء الاسقاطي.
- $E(k)[m] \coloneqq \{p \in E(k); mp = \infty\}$ النقاط على المنحني الاهليلجي ذات الرتبة m.
- $\mathfrak{C}$: أسرة من المنحنيات الاهليلجية التي لها الشكل $y^2 = x^3 + Dx$ حيث أن D عدد صحيح حر من التربيع.
- $Gal(L,k) \coloneqq \{\sigma \in Aut(L,k); \sigma(k) = k\}$ زمرة غالوا.

- $\mathcal{O}_k := \{\alpha \in k; k$ فوق α صحيح$\}$ حلقة الأعداد الصحيحة.
- $k_v := \{x \in k; v(x) \geq 0\}$ حيث v تابع تقييم.
- $specR$ مجموعة الإيديالات الأولية في حلقة كيفية R، حيث أنها تشكل تبولوجيا جبرية مجموعاتها المغلقة هي $V(I) = \{p \in specR; I \subseteq p\}$.

التعاريف الأساسية:

نذكر فيما يلي مجموعة من التعاريف الأساسية وبعض الملاحظات التي تساعدنا في فهم المصطلحات العلمية الواردة في البحث وتوضيح برهان المبرهنات الواردة فيه.

تعريف (1) المنحني الإهليلجي فوق الحقل k Elliptic curve [1]:

هو منحني إسقاطي غير شاذ له فجوة واحدة بالإضافة إلى نقطة اللانهاية ∞ ويرمز له بالرمز $E(k)$، ويقال إن المنحني الاهليلجي $E(k)$ له تمثيل جيد عند النقطة v إذا كان $\widehat{E}(k)$ منحنياً إهليلجياً غير شاذ حيث $\widehat{E}(k) \cong E(k)(mod\ v)$.

تعريف (2) شبه الحزمة والحزمة presheaf and sheaf [2]:

ليكن X فضاءً تبولوجياً، يقال عن مجموعة الزمرة التبديلية $\mathcal{F}$ المعرفة فوق X إنها شبه حزمة إذا حققت ما يلي:

1) من أجل كل مجموعة جزئية مفتوحة $U \subseteq X$ تكون $\mathcal{F}(U)$ زمرة تبديلية معرفة فوق U

2) ومن أجل كل $V \subseteq U \subseteq X$ يوجد مورفيزم $\rho_{UV}: \mathcal{F}(U) \to \mathcal{F}(V)$ بحيث يحقق الشروط التالية:

a. $\mathcal{F}(\phi) = 0$

b. $\rho_{UU}: U \to U$ التطبيق المطابق

c. من أجل كل $W \subseteq V \subseteq U$ يكون $\rho_{UW} = \rho_{UW} \circ \rho_{UV}$

ويقال عن شبه الحزمة $\mathcal{F}$ إنها حزمة إذا حقق الشرطين التاليين إضافة للشروط السابقة:

d. لتكن U مجموعة مفتوحة و $\{V_i\}$ تغطية للمجموعة U ولتكن$s \in \mathcal{F}(U)$ بحيث أن:

e. لتكن U مجموعة مفتوحة و $\{V_i\}$ تغطية للمجموعة U ولتكن $s_i \in \mathcal{F}(V_i)$ بحيث أن:

عندئذٍ يوجد $s \in \mathcal{F}(U)$ بحيث $s|_{V_i} = s_i$ وذلك مهما تكن i.

تعريف (3) الزمرة الهمولوجية Homology group [5]:

لتكن M $-G-$ مودول و $C^n(G,M) = \left\{ f: \underbrace{G \times G \times \cdots \times G}_{\text{مرة } n} \to M \right\}$ زمرة كل التوابع بـ n متحول في M و $\delta_n: C^n(G,M) \to C^{n+1}(G,M)$ هومومرفيزم زمر معرف بالشكل:

$$+\sum_{i=1}^{n}$$

عندئذٍ تعرف الزمرة الهمولوجية النونية $H^n(G,M)$ للزمرة G بمعاملات من M بأنها:

ملاحظة (1) [5]: الزمرة الهومولوجية الصفرية $H^0(G,M)=M^G$، وإذا كان عمل الزمرة G على M تافهاً فإن:

$$H^1(G,M)=Hom(G,M).$$

ملاحظة (2) [5]: إذا كانت H زمرة جزئية نظامية في G عندئذٍ توجد متوالية عكسية صحيحة بالشكل:

تعريف (4) المجموعة الملساء والمورفيزم الأملس Smooth sets and smooth morphism [6، 7]:

لتكن $X\subseteq \mathbb{A}_k^n$ مجموعة جبرية و $I(X)$ إيديال مولد بكثيرات الحدود $f_1,\dots f_r$ و $p\in X$، يقال عن X إنها مجموعة ملساء عند النقطة p إذا كانت رتبة مصفوفة جاكوبي $\mathcal{J}=\left(\frac{\partial f_i}{\partial x_j}\right)_{\substack{1\le i\le r\\ 1\le j\le n}}$ تساوي $n-\dim X$ ولا تساوي 0، ويقال عن المورفيزم $f:X\to Y$ إنه مورفيزم أملس إذا كان المجموعة X ملساء عند كل نقاط $y\in Y$.

تعريف (5) المودول المسطح والمورفيزم المسطح Flat module and flat morphism [2]:

لتكن R حلقة تبديلية و M $R-$ مودول، يقال عن M إنه مودول مسطح إذا وفقط إذا كان التطبيق $m\otimes M\to M$ متبايناً من أجل كل إيديال m منتهي التوليد في R، ويقال عن المورفيزم $f:X\to Y$ إنه مورفيزم مسطح إذا كان Y هو $X-$ مودول مسطح.

تعريف (6) التوسيع غير المتشعب والمورفيزم غير المتشعب Unramified extension and unramified morphism [6، 8]:

لتكن R حلقة تقييم منفصل و K حقل كسور R و m إيديال أعظمي في R و $k=R/m$ حقل الرواسب و K' توسيعاً لِـ K و R' الإغلاق الصحيح لِـ R في K' و m' إيديال أعظمي في R' و $k'=R'/m'$، يقال عن التوسيع K' لِـ K إنه غير متشعب إذا كان $\left[K':K\right]=\left[k':k\right]$، ويقال عن المورفيزم $f:X\to Y$ إنه غير متشعب إذا كان f مورفيزماً من النمط المنتهي و $\Omega_{X/Y}=0$ حيث أن $\Omega_{X/Y}$ مودول المشتقات **the module of Kähler differential**. ويقال عن المورفيزم $f:X\to Y$ إنه مورفيزم إيتال **(e′tale)** إذا كان f مسطحاً وغير متشعب.

تعريف (7) الفضاء الحلقي والزمرة المخططة Ringed space and scheme group [2,10]:

يعرف الفضاء الحلقي بأنه الثنائية (X,O_X) حيث X فضاء تبولوجي و O_X حزمة من الحلقات. ويقال عن الفضاء الحلقي $(X,\mathcal{O}_X)$ إنه مخطط إذا كان حيزياً (locally) وإيزومورفياً مع $(specR,O_{specR})$ حيث R حلقة كيفية، ويقال عن G إنها زمرة مخططة فوق X إذا كانت G هي $X-$ مخطط معرف عليها مورفيزمين $m:G\times_X G\to G$ و $i:G\to G$ ونقطة كسرية $e\in G(k)$ وتحقق شروط الزمرة.

تعريف (8) المورفيزم المندمج المفتوح والمترابط هندسياً Open immersion and geometrically connected morphism [2,6]:

ليكن X, Y مجموعتين مخططتين، يقال عن $f: X \to Y$ إنه مندمج مفتوح إذا كان $X \cong U$ حيث $U \subseteq Y$، ويقال عن f إنه مترابط هندسياً إذا كان يملك نقاط فيبر $X_y = X \times_y speck(y)$ مترابط هندسياً من أجل كل $y \in Y$.

النتائج والمناقشة:

لنعرف على المنحني الاهليلجي $E(\bar{k})$ التطبيق $[m]: E(\bar{k}) \to E(\bar{k})$ بالشكل التالي $[m](p) = mp$ حيث أن $m \in \mathbb{Z}$ و $p \in E(k)$. وسنرمز بـ V للمنحني الاهليلجي $E(k)$ في المنطلق وبـ W للمنحني الاهليلجي $E(k)$ في المستقر.

مبرهنة مساعدة (1) **[4]**: لتكن V, W مجموعتين جبريتين و $k[V], k[W]$ حلقتي إحداثيات، إذا وجد هومومرفيزم $\varphi: V \to W$ فإنه يوجد هومومرفيزم حلقات $\varphi^*: k[W] \to k[V]$.

❖ سنبرهن في المبرهنة الأولى أن التطبيق $[m]$ هومومرفيزم غامر وليس متباين.

مبرهنة 1: التطبيق $[m]: E(\bar{k}) \to E(\bar{k})$ هومومرفيزم زمر غامر ونواته $E(\bar{k})[m]$.

البرهان:

○ $[m]$ هومومرفيزم زمر: $[m](p + p') = m(p + p') = mp + mp' = [m]p + [m]p'$.

○ $[m]$ غامر: لدينا V, W مجموعتين جبريتين و $k[V], k[W]$ حلقتي الاحداثيات، ولتكن $q = (u, v) \in W$ نقطة كيفية عندئذٍ حسب نظرية الأصفار لهلبرت **[11]** فإنه يوجد تقابل 1−1 بين النقطة $q = (u, v)$ وبين الايديال الأعظمي $Q = (x_1 - u, x_2 - v) \in k[W]$ وحسب المبرهنة المساعدة (1) فإنه يوجد هومومرفيزم $[m]^*: k[W] \to k[V]$ معرف بالشكل:

$[m]^*Q = [$

وحسب نظرية الأصفار لهلبرت فإنه يوجد تقابل 1−1 بين الإيديال الأعظمي $P = (x_1 - \alpha, x_2 - \beta)$ وبين النقطة $(\alpha, \beta) \in V$)، وبالتالي نستطيع تشكيل المخطط التالي

-

$\downarrow \quad \leftarrow \quad \downarrow$

ومنه $\forall q \in W\ \exists p \in V; [m]p = mp = q$.

○ نواة $[m]$: $\ker[m] = \{p \in V, mp = \infty\} = E(\bar{k})[m]$.

ملاحظة: ليكن L توسيعاً للحقل k و $Gal(L, k)$ زمرة غالوا و $[m]: E(L) \twoheadrightarrow E(L)$ هومومرفيزم زمر غامر معرف بالشكل $[m]p = mp$ عندئذٍ حسب المبرهنة (1) فإنه من أجل كل $q \in E(k) \subseteq E(L)$ يوجد $p \in E(L)$ بحيث يكون $mp = q$ و $\forall \sigma \in Gal(L, k), \forall q \in k\ \sigma(q) = q$ وبالتالي:

mp

مبرهنة مساعدة (2) **[12]:** لتكن $0 \to A \to B \to C \to 0$ متوالية صحيحة قصيرة، عندئذٍ نستطيع تعريف متوالية صحيحة طويلة بالشكل:

$$0 \to H^0(G,A) \to$$
$$\to$$

❖ سنبين في المبرهنة التالية أن ${}^{E(k)}\!/_{mE(k)}$ منتهٍ في حال الحقل k محتوى في حقل L.

مبرهنة 2: ليكن L توسيعاً للحقل k والتطبيق $\phi: {}^{E(k)}\!/_{mE(k)} \to {}^{E(L)}\!/_{mE(L)}$ ، إذا كان ${}^{E(L)}\!/_{mE(L)}$ منتهٍ فإن ${}^{E(k)}\!/_{mE(k)}$ منتهٍ.

البرهان: لدينا المتوالية الصحيحة التالية:

$$0 \to E(L)[m] \to E(L) \xrightarrow{m} mE(L) \to 0 \qquad (1)$$

نطبق المبرهنة المساعدة (2) على المتوالية (1) على اعتبار أن $G = Gal(L,k)$ فنجد:

$$0 \to H^0(Ga$$
$$\xrightarrow{\delta} H^1(Gal(L,k),E$$

وبالتالي نحصل على المتوالية:

$$0 \to E(k)$$

ومنه يوجد تطبيق:

حيث $H^1(Gal(L,k),E(L)[m]) = \{f: Gal(L,k) \to E(L)[m]; f(\sigma) = \sigma(p) - p\}$

ولنبرهن أنه متباين:

$$\forall\, q, q' \in$$

$$\Rightarrow q -$$

وبما أن زمرة غالوا منتهية و $E(L)[m]$ منتهية بالتالي $H^1(Gal(L,k),E(L)[m])$ منتهية وعليه تكون ${}^{mE(L)\cap E(k)}\!/_{mE(k)}$ منتهية.

من جهة ثانية: لدينا الزمرة ${}^{mE(L)\cap E(k)}\!/_{mE(k)}$ هي نواة التطبيق:

وبالتالي نشكل المتوالية الصحيحة من اليسار

$$0 \to$$

ومنه $E(k)/mE(k)$ تقع بين زمرتين منتهيتين بالتالي هي منتهية.

مبرهنة مساعدة (3) **[1]:** ليكن k حقلاً و $\mathcal{O}_k$ حلقة الأعداد الصحيحة و S مجموعة منتهية من الأعداد الأولية في $\mathcal{O}_k$، من أجل $m \geq 1$ يكون التوسيع التبديلي الأعظمي لـ k غير المتشعب خارج S منتهياً.

❖ سنبين في المبرهنة التالية أن $E(k)/mE(k)$ منتهه من أجل كل $m \geq 1$.

مبرهنة 3: ليكن $E(k)$ منحنياً إهليلجياً معرفاً فوق الحقل k عندئذٍ $E(k)/mE(k)$ منتهه وذلك مهما تكن $m \geq 1$.

البرهان: لدينا المتوالية الصحيحة التالية:

$$0 \to E(\bar{k})[m] \to E(\bar{k}) \xrightarrow{m} E(\bar{k}) \to 0 \qquad (2)$$

نطبق المبرهنة (2) على المتوالية (2) على اعتبار أن $G = Gal(\bar{k}, k)$ فنجد:

0

وبالتالي يوجد تطبيق: $\delta_1 : E(k)/mE(k) \to H^1(Gal(\bar{k}, k), E(\bar{k})[m])$.

وبما أن عمل زمرة غالوا $Gal(\bar{k}, k)$ على $E(\bar{k})[m]$ تافه فإن:

ليكن L توسيعاً منتهياً لـ k بحيث أن $k \subseteq L \subseteq \bar{k}$ و L يحوي الحقل k مع جميع العناصر $p \in E(\bar{k})$ بحيث $p \notin E(k)$ وبالتالي بتطبيق المبرهنة (2) على السلسلة (2) على اعتبار $G = Gal(\bar{k}, L)$ نجد أن:

0

وبالتالي يوجد تطبيق: $\delta_2 : E(L)/mE(L) \to H^1(Gal(\bar{k}, L), E(\bar{k})[m])$.

وبما أن عمل زمرة غالوا $Gal(\bar{k}, L)$ على $E(\bar{k})[m]$ تافه فإن:

ولدينا $Gal(\bar{k}, L)$ زمرة جزئية نظامية في $Gal(\bar{k}, k)$، فباستخدام تعريف المتوالية الصحيحة العكسية نحصل على المخطط التالي:

0 0 0

0 – – –

0 – H – H $\xrightarrow{\gamma}$ H

ومنه $H^1(Gal(L, k), E(\bar{k})[m]) = Hom(Gal(L, k), E(\bar{k})[m])$

ومن المخطط لدينا

حيث أن δ معرف بالشكل التالي:

$\Longrightarrow \delta_1(x) =$

بما أن $b \in E(\bar{k})$ فإنه حسب تعريف L يكون $b \in E(L)$ وبالتالي $\delta_2(x) = \sigma(b) - b = 0$ وبالتالي

δ_1

وبالتالي يمكن تحديد الحقل L بأنه عبارة عن الحقل k بالإضافة إلى العناصر $b \in E(\bar{k})$ التي تحقق أن $m(b) = a$، إضافة إلى ذلك فإن الحقل L هو التوسيع الأعظمي للحقل k من المرتبة m. وبقي أن نبرهن أن هذا التوسيع منتهي.

من المبرهنة المساعدة (3) سوف نبحث عن مجموعة منتهية S ونبين أن L غير متشعب خارج S. ولذلك يكفي برهان أن $\mathfrak{E}$ زمرة مخططة تبديلية فوق S **[6]**.

مبرهنة مساعدة (4) **[12]**: لتكن $R[X]$ حلقة كثيرات الحدود بـ n متحول نيوترية و $m = \langle f_i \rangle$ إيديال أعظمي في $R[X]$ و $\mathcal{J}$ مصفوفة جاكوبي عندئذٍ $\dim {}^{m}/_{m^2} + rk(\mathcal{J}) = \dim R[X]$.

مبرهنة مساعدة (5) **[6]**: لتكن S مجموعة كيفية و U مجموعة متممة لـِ S، يقال عن $\mathfrak{E}$ إنها زمرة مخططة تبديلية فوق S إذا وجد تطبيق $\mathfrak{E} \to U$ مسطح وأملس ويملك نقاط فيبر مترابطة هندسياً.

❖ سنبين بالمبرهنة (4) أن يوجد تقابل $1-1$ بين المنحنيات الاهليلجية ومجموعة جزئية من الإيديالات الأولية في $\mathcal{O}_k$، ثم سنحدد في المبرهنة (5) عدد النقاط التي رتبتها تساوي m.

مبرهنة 4: الموروفيزم $\mathfrak{f}: \mathfrak{E} \to U; U \subseteq Spec(\mathcal{O}_k)$ مسطح وأملس ويملك نقاط فيبر مترابطة هندسياً.

البرهان: ليكن E منحنياً إهليلجياً من أسرة المنحنيات الاهليلجية $\mathfrak{E}$ وبالتالي تشاكلاً جبرياً، حسب نظرية الأصفار الاسقاطية لهلبرت يوجد تقابل $1-1$ بين التشاكلات الجبرية في $\mathbb{P}_k^n$ والايديالات الأولية في $k[X]$ بحيث

ومنه يوجد مورفيزم $f: \mathfrak{E} \to Spec(k[X])$ معرف بالشكل $f(E) = I = \langle E \rangle$

من جهة ثانية لدينا $\mathcal{O}_k \subseteq k$ وبالتالي يوجد تطبيق $Speck[X] \twoheadrightarrow Spec\mathcal{O}_k[X]$ **[6]** ومنه يوجد تطبيق من $\mathfrak{E} \to Spec(\mathcal{O}_k[X])$ ولدينا $Spec\mathcal{O}_k[X] \twoheadrightarrow Spec(\mathcal{O}_k)$ وبالتالي يوجد مورفيزم $\mathcal{F}: \mathfrak{E} \to Spec(\mathcal{O}_k)$ معرف بالشكل: $\mathcal{F}(E) = e$.

○ $\mathfrak{f}$ مسطح: ليكن J إيديالاً كيفياً في $\mathcal{O}_k[X]$ عندئذٍ ${}^{\mathcal{O}_k[X]}/_{J}$ هو $\mathcal{O}_k$ مودول ولبرهان أن $\mathfrak{f}$ مسطح يكفي أن نبرهن أن ${}^{\mathcal{O}_k[X]}/_{J}$ هو $\mathcal{O}_k$ مودول مسطح **[2]** ومنه يجب برهان أن التطبيق

$\mathfrak{p} \otimes {}^{\mathcal{O}_k[X]}/_{J} \to {}^{\mathcal{O}_k[X]}/_{J}$ متباين حيث أن $\mathfrak{p}$ إيديال كيفي في $\mathcal{O}_k$.

بما أن $\mathcal{O}_k$ ساحة ديدكند بالتالي ساحة نيوترية ومنه كل إيديال فيه منتهي التوليد **[3]** وبالتالي يمكن تعريف التطبيق $\wp \otimes {}^{\mathcal{O}_k[X]}/_{J} \to {}^{\mathcal{O}_k[X]}/_{J}$ بالشكل $(p, f(x) + J) \to pf(x) + J$ ولنبرهن أنه متباين:

وحسب وحدانية تحليل الحلقة $\mathcal{O}_k$ فإن $pf(x) = 0$ ومنه $p = 0$ وبالتالي ${}^{\mathcal{O}_k[X]}/_{J}$ حر من الالتفاف في $\mathcal{O}_k$ وبالتالي ${}^{\mathcal{O}_k[X]}/_{J}$ هو $\mathcal{O}_k$ مودول مسطح، وبالتالي المورفيزم $\mathcal{F}: \mathfrak{E} \to Spec(\mathcal{O}_k)$ مسطح ومنه $\mathfrak{f}: \mathfrak{E} \to U$ مسطح.

○ $\mathfrak{f}$ أملس: ليكن $E \in \mathfrak{E}$ منحنياً إهليلجياً كيفياً و $I = \langle E \rangle$ ايديال في $Spec(k[X])$ وبالتالي يكون المنحني الاهليلجي أملساً عند الأعداد الأولية t_i حيث $\langle t_i \rangle \in Spec\mathcal{O}_k$ باستثناء عدد منتهٍ من الأعداد الأولية وبالتالي $rk(\mathcal{J}) = 1 \neq 0$، وبقي أن نبرهن أن رتبة مصفوفة جاكوبي من أجل كل $\mathfrak{E}$ لا تساوي الصفر عند $\langle t_i \rangle \in Spec\mathcal{O}_k$ باستثناء عدد منتهٍ من الأعداد الأولية. لدينا من المبرهنة المساعدة (4)

بما أن $\mathcal{O}_k$ حلقة تقييم منفصل فإن $\dim \mathcal{O}_k = 1$ وبالتالي $\dim \mathcal{O}_k[X] = n + 1$ و $\dim {}^{\mathcal{M}}/_{\mathcal{M}^2} = 1$ حيث أن $\mathcal{M}$ إيديال أعظمي في $\mathcal{O}_k$. ومنه تصبح $rk(\mathcal{J}) = n \neq 0$ وبالتالي $\mathfrak{f}$ أملس على مجموعة جزئية من $Spec\mathcal{O}_k$ ولتكن U ومنه $\mathfrak{f}: \mathfrak{E} \to U$ أملس.

○ $\mathfrak{f}$ يملك نقاط فيبر مترابطة: لدينا E زمرة مخططة فوق k **[13]** و $E = \mathfrak{E}_k = \mathfrak{E} \otimes_k k$ **[6]** ولدينا دوماً التطبيق $\mathfrak{E}_k \to \mathfrak{E}$ مندمج مفتوح **[2]** و $\mathfrak{f}: \mathfrak{E} \to Spec\mathcal{O}_k$ فبتالي E ايزومورفي مع مجموعة جزئية في $spec\mathcal{O}_k$ ومنه من أجل $\mathfrak{E}$ فإن $\mathfrak{E}$ إيزومورفي مع مجموعة جزئية في $spec\mathcal{O}_k$ ولنبرهن أنها U.

إن وجود المورفيزم $\mathfrak{f}: \mathfrak{E} \to U$ يؤدي إلى وجود المورفيزم $\mathfrak{f}^{\#}: O_U \to \mathfrak{f}_* O_{\mathfrak{E}}$ المعرف بالشكل:

$$\mathfrak{f}^{\#}(V) = \mathfrak{f}_* O_{\mathfrak{E}}(V) = O_{\mathfrak{E}}\left(\mathfrak{f}^{-1}(V)\right)$$ حيث أن $V \subseteq U$.

لدينا السلسلة الصحيحة التالية: $0 \to \mathfrak{I} \to O_U \to \mathfrak{f}_* O_{\mathfrak{E}} \to 0$ حيث أن $\mathfrak{I}$ نواة $\mathfrak{f}$ ومنه

بما أن $\mathfrak{f}$ فعلي غير تافه عندئذٍ $\mathfrak{f}_* O_{\mathfrak{E}}$ هو O_U مودول مترابط **[6]** ومنه $\mathfrak{f}_* O_{\mathfrak{E}}(U) = O_{\mathfrak{E}}(\mathfrak{E})$ هو $\mathcal{O}_k'$ مودول منتهي التوليد **[2]** حيث أن $U = spec(\mathcal{O}_k')$ وبالتالي (U, O_U) فضاء حلقي مخطط حيث أن $U = spec(\mathcal{O}_k')$ تشكل تغطية لنفسها وبما أن $\mathfrak{f}$ مسطح و $E \in \mathfrak{E}$ تشاكل جبري فإن $O_{\mathfrak{E}}(\mathfrak{E})$ هو $\mathcal{O}_k'$ مودول حر قياسه يساوي 1 وبالتالي $O_{\mathfrak{E}}(\mathfrak{E}) = k$، ولدينا $O_U(U) \cong \mathcal{O}_k$ **[2]** و $\mathcal{O}_k \hookrightarrow k$ ومنه $\mathfrak{I}(U) = 0$ وبالتالي $\mathfrak{I} = 0$ وعليه يكون $\pi_*(\mathcal{O}_{\mathcal{A}}) \cong O_U$ وبالتالي π تملك نقاط فيبر مترابطة وبما أن E منحني أملس على U فإن π يملك نقاط فيبر مترابطة هندسياً ومنه حسب المبرهنة المساعدة (5) تكون $\mathfrak{E}$ زمرة مخططة تبديلية فوق S، حيث أن S مجموعة منتهية من الأعداد الأولية التي متممتها U.

نتيجة 1: تتألف المجموعة S من الأعداد الأولية v التي تحقق $v|m$ إضافة إلى الأعداد الأولية v التي يكون من أجلها $E \in \mathfrak{E}$ منحنياً شاذاً.

نتيجة 2: لدينا E منحني إهليلجي وبالتالي تشاكل جبري وليكن $V \subset E$ ولنعرف $O_E(V)$ بالشكل:

عندئذٍ $O_E(V)$ تشكل حزمة من الحلقات.

مبرهنة مساعدة [6] **[14]:** ليكن E تشاكلاً تبديلياً فوق k و $[m]: E \to E$ تطبيق معرف بالشكل $[m]p = mp$ عندئذٍ درجة التطبيق $[m]$ تساوي $m^{2\dim_k E}$.

مبرهنة 5: التطبيق $[m]: \mathfrak{E} \to \mathfrak{E}$ غامر وإيتال منتهي درجته $m^{2\dim_k E}$.

البرهان: التطبيق $[m]: \mathfrak{E} \to \mathfrak{E}$ هو توسيع للتطبيق $[m]: E \to E$

○بما أن التطبيق $[m]$ غامر من أجل كل $E \in \mathfrak{E}$ فإن التطبيق $[m]: \mathfrak{E} \to \mathfrak{E}$ غامر، وبما أن $[m]$ هومومرفيزم فإن $[m]$ منتهي.

○$[m]$ مسطح: لدينا من المبرهنة (4) $\mathfrak{E}$ زمرة مسطحة وبالتالي $[m]$ مسطح.

○$[m]$غير متشعب لأن $\Omega_{\mathfrak{E}/\mathfrak{E}} = 0$

وبالتالي التطبيق $[m]: \mathfrak{E} \to \mathfrak{E}$ إيتال وبما أن $[m]$ منتهٍ فإن $[m]$ إيتال منتهي وبالتالي حسب المبرهنة المساعدة (6) فإن درجته منتهية وتساوي درجة كل فيبر جزئي منه $[m]: E \to E$ وبالتالي درجة التطبيق $[m]: \mathfrak{E} \to \mathfrak{E}$ تساوي $m^{2\dim_k E}$.

نتيجة 3: بما أن التطبيق $[m]: \mathfrak{E} \to \mathfrak{E}$ إيتال منتهي فإن نواته منتهية وبالتالي إذا كانت $m = 3$ فإن

مبرهنة مساعدة (7) **[3]:** ليكن $CL(k)$ زمرة صفوف الايديال و $CL^S(k)$ $-S$ زمرة صفوف الايديال، إذا كان $n \nmid CL(k)$فإن $H^1(Gal(\bar{k},k),\mathbb{Z}_n;S) = Hom\left(CL^S(k),\mathbb{Z}_n\right) = 0$.

❖ سنقوم في المبرهنتين (6) و (7) بإيجاد قيم D التي تجعل رتبة المنحني الاهليلجي تساوي 1.

مبرهنة (6): إذا كان $\mathfrak{E}(k)[3] = \mathfrak{E}(\mathbb{Q})[3]$ و $3 \nmid CL(k)$ فإنّ $D \equiv 1(mod\ 4)$.

البرهان: بما أن المنحني الاهليلجي يملك نقاطاً رتبتها تساوي 3 فإنّ المتوالية التالية صحيحة:

$$0 \to \mathbb{Z}_3 \to E[3] \to \mu_3 \to 0 \qquad (3)$$

بتطبيق المبرهنة المساعدة (2) على المتوالية (3) على اعتبار $G = Gal(\bar{k},k)$ فنجد:

$$0 \to H^1\left(Gal(\bar{k},k),\mathbb{Z}_3\right) \to H^1\left(Gal(\bar{k},k),E[3]\right) \to H^1\left(Gal(\bar{k},k),\mu_3\right). \qquad (4)$$

ومن أجل S مجموعة منتهية من الأعداد الأولية في k و M زمرة كيفية يكون:

$H^1(G$

عندئذٍ من المتوالية (4) نجد المتوالية التالية:

(5)

$$0 \to H^1\left(Gal(\bar{k},k),\mathbb{Z}_3;S\right) \to H^1\left(Gal(\bar{k},k),E[3]:S\right) \to H^1\left(Gal(\bar{k},k),\mu_3;S\right).$$

لدينا من الفرض $3 \nmid CL(k)$وحسب المبرهنة المساعدة (8) يكون $H^1(Gal(\bar{k},k),\mathbb{Z}_3;S) = 0$.

ومنه تصبح المتوالية (5) بالشكل:

$$0 \to H^1\left(Gal(\bar{k},k),E[3]:S\right) \to H^1\left(Gal(\bar{k},k),\mu_3;S\right). \qquad (6)$$

من ناحية ثانية حسب **[1]** لدينا $Sel^{(3)}(E,k) \subseteq H^1\left(Gal(\bar{k},k),E[3]:S_1\right)$ حيث أن $Sel^{(3)}(E,k)$ هي زمرة سلمر(Selmer group) **[9]** و S_1 مجموعة الأعداد في k التي تحوي ∞ و $\{v; v|3D\}$، إذا كان $v|3$ فإن

$E \cong E_v(mod\ v)$ ولكنه لدينا حسب الفرض $E(\mathbb{Q})[3] = E(k)[3]$ فإن E له تمثيل جيد عند النقطة v ومنه $\xi \in Sel^{(3)}(E,k)$ غير متشعب عند النقطة v وهذا يناقض كون $v \in S_1$ وبالتالي $v \not\equiv 3(mod\ 4)$ ومنه

حيث أن S_2 مجموعة الأعداد في k التي تحوي ∞ و $\{v; v|D\}$ وبالتالي $v = D$ ومنه $D \equiv 1(mod\ 4)$.
وبالتالي تصبح السلسلة (6) بالشكل:

حيث أن:

$$H^1(Gal(\overline{k},k),\mu_3 : S_2) \overset{[15]}{\cong} \left\{ b \in {k^*}/{k^{*3}} ; ord_v(b) \equiv 0(mod\ 3)\ \forall v \notin S_2 \right\}$$

$\cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}$

مبرهنة مساعدة [8] **[16، 17]**: إذا كان $k = \mathbb{Q}(\sqrt{D})$ حقلاً مميزه d بحيث $(3,d) = 1$ ويحقق:

i. $3 \nmid CL(k)$.

ii. v تنشطر في k حيث أن $v \in S_2$.

iii. $E(\mathbb{Q})[3] = E(k)[3]$.

عندئذٍ نقطة هيغنر (Heegner point) $(d,1,1)$ لها رتبة تساوي اللانهاية ورتبة المنحني الاهليلجي تساوي 1.

مبرهنة (7): إذا كان $\mathfrak{E} \subseteq \mathfrak{D}$ حيث D عدد أولي و $D \equiv 5(mod\ 8)$ فإن رتبة المنحني الاهليلجي تساوي 1 بالإضافة إلى أن زمرة شافاريتش (Shafarevich group) **[9]** $Ш(E(k),k)[3] = 0$.

البرهان: لدينا من المبرهنة (6) أنه إذا كان $\mathfrak{E}(\mathbb{Q})[3] = \mathfrak{E}(k)[3]$ و $3 \nmid CL(k)$ فإنّ
$D \equiv 1(mod\ 4)$ ومنه $d = D$ وتكون v تنشطر في k إذا كان $d = D \not\equiv 1(mod\ 8)$ وبالتالي
$D \equiv 5(mod\ 8)$ ومن المبرهنة المساعدة (8) ينتج أن رتبة المنحني الاهليلجي $E \in \mathfrak{D}$ تساوي 1.
ومنه يكون:

$\Rightarrow E$

$\cong \mathbb{Z}/3\mathbb{Z} \oplus 0$

ولدينا $0 \to {E(k)}/{3E(m)} \to Sel^{(3)}(E,k) \to Ш^{(3)}(E,k) \to 0$

ومنه $Ш^{(3)}(E,k) = 0$.

مبرهنة مساعدة (9) **[1]**: ليكن $E: y^2 = x^3 + ax + b; a,b \in \mathbb{Z}$ منحنياً إهليلجياً فوق الحقل k عندئذٍ النقطة $p = (x,y)$ لها رتبة منتهية إذا كان $x,y \in \mathbb{Z}$ أو $y = 0$ أو $y^2 | 4a^3 + 27b^2$.

نتيجة (4): إن حل المعادلات الديوفانتية $y^2 = x^3 + Dx$ حيث $D \equiv 5(mod\ 8)$ هو

حيث أن $E(k)_{tors}$ تحسب من المبرهنة المساعدة (9) إضافة إلى نقطة هيغنر $(d,1,1)$ حيث أن المعادلات الديوفانتية $y^2 = x^3 + Dx$ في الفضاء الاسقاطي $\mathbb{P}_k^1$ هي من الشكل $y^2z = x^3 + Dxz^2$.

الاستنتاجات والتوصيات:

توصلنا في هذه المقالة إلى تحديد عدد النقاط ذات الرتب المنتهية للمعادلات الديوفانتية من الشكل $y^2 = x^3 + Dx$ وتحديد رتبة المنحني الاهليلجي عندما $D \equiv 5(mod\ 8)$ ، ونوصي بإيجاد رتبة المنحني الاهليلجي من الشكل $y^2 = x^3 + ax + b$ حيث $a, b \neq 0$.

المراجع:

[1] SILVERMAN, J. H. *The Arithmetic of Elliptic Curves*, Springer New York, 2013,513.

[2] HARTSHORNE, R. *Algebraic geometry* ,vol. 52, Springer Science & Business Media, 2013,496.

[3] MOLLIN, R.A. *Advanced Number Theory with Applications*, CRC Press, 2009,466.

[4] HULEK, K. *Elementary Algebraic Geometry*, American Mathematical Society, 2003,213.

[5] Fu, L. *Etale Cohomology Theory*, World Scientific, 2011,611.

[6] LIU, Q. *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, 2002,577.

[7] HOLME, A. *A Royal Road to Algebraic Geometry*, Springer Berlin Heidelberg, 2011,364.

[8] COHEN, H. *Number Theory: Volume I: Tools and Diophantine Equations*, Springer New York, 2007,560.

[9] JETCHEV, D. P. University of California, *Selmer Groups, Component Groups and Heegner Points*, University of California, Berkeley, 2008,112.

[10] SAFAREVIC, I. R. *Basic Algebraic Geometry 2*, Springer-Verlag, 2013,262.

[11] MACLEAN, C., PERRIN, D. *Algebraic Geometry: An Introduction*, Springer London, 2007,257.

[12] KNAPP, A. W. *Advanced Algebra*, Birkhäuser Boston, 2007,730.

[13] GOLDFELD, D., JORGENSOM, J., JONES, P. *Number Theory, Analysis and Geometry: In Memory of Serge Lang*, Springer, 2011,704.

[14] MILEN, J.S. Abelian Varieties, www.jmilne.org/math/, 2008,166.

[15] LIEDTKE, C. The p-torsion subgroup scheme of an elliptic curve, *Journal of Number Theory*, vol. 131, pp. 2064-2077, 2011.

[16] BYEON, D., JEON, D., KIM, C.H. *Rank-one quadratic twists of an infinite family of elliptic curves*, Journal für die reine und angewandte Mathematik (Crelles Journal), vol. 2009, pp. 67-76, 2009.

[17] BYEON, D. *Heegner points on elliptic curves with a rational torsion point*, Journal of Number Theory, vol. 132, pp. 3029-3036, 2012.