Study of Rational Points of some Elliptic Curves

Dr. Hasan Sankari*
Mariam al-Shatoury**

(Received 23 / 1 / 2024. Accepted 23 / 4 /2024)

□ ABSTRACT □

This research focused on studying of a special type of curves given by non-singular weierstrass equation which called elliptic curves, the study of elliptic curves had answered many of purely theoretical questions asked by mathematicians , and it has great importance at the presenttime for its use inencryption,which depends on the algebraic structure of these curves ,so it has been the focus of attention of many recent studies.
One of the most important theorems is Nagell-lutz theorem which used in the studying of elliptic curves since it is a practical tool in finding all rational points of finite order on an elliptic curve over the rationals , the fundamental concepts were employed in the theory of projective geometry including the theorem of bezout to get the consequences of this study, this paper have focused on finding the rank of elliptic curves which has at least rational point of order two .
In addition to obtaining some important results related to these curves.

Keywords: Elliptic curve ,Torsion group , The rank of a curve , Quadratic Residues.

* **Associate Professor, Department of mathematics , Faculty of Science, Tishreen University, Lattakia, Syria .**
** **Postgraduate Student (Master), Mathematics Department ,Faculty of Science ,Tishreen University, Lattakia ,Syria .mariamalshatoury@gmail.com**

دراسة النقاط الكسرية لبعض المنحنيات الإهليلجية

د. حسن سنكري *

مريم الشاتوري **

(تاريخ الإيداع 23 / 1 / 2024. قُبِل للنشر في 23 / 4 /2024)

□ ملخّص □

اهتم هذا البحث بدراسة نوع خاص من المنحنيات المعطاة بمعادلة وايرستراش غير الشاذة والتي تسمى المنحنيات الإهليلجية ، وقد أجابت دراسة المنحنيات الاهليلجية عن العديد من القضايا النظرية البحتة المطروحة من قبل الرياضيين ،كما وتبرز أهميتها في وقتنا الحالي لاستخدامها في التشفير الذي يعتمد على البنية الجبرية لهذه المنحنيات لذلك كانت محط اهتمام في العديد من الدراسات الحديثة

وتعد نظرية Nagell–lutz من أهم النظريات المستخدمة في دراسة المنحنيات الإهليلجية حيث تعتبر أداة خاصة لإيجاد النقاط الكسرية ذات الرتبة المنتهية وتم توظيف المفاهيم الأساسية في نظرية الهندسة الإسقاطية ولاسيما نظرية Bezout للحصول على نتائج في هذه الدراسة، و تم التركيز في هذا البحث على إيجاد الرتبة لبعض المنحنيات الإهليلجيه والتي تملك على الأقل نقطة كسرية ذات رتبة 2 ،يضاف إلى ذلك الحصول على بعض النتائج المهمة المتعلقة بهذه المنحنيات

الكلمات المفتاحية: المنحني الإهليلجي ، زمرة الالتفاف، رتبة منحني، البواقي التربيعية .

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

** **طالبة دراسات عليا(ماجستير)– قسم الرياضيات– كلية العلوم – جامعة تشرين – اللاذقية –سورية.mariamalshatoury@gmail.com**

مقدمة:

المنحنيات الاهليلجية هي منحنيات ملساء من النوع 1 وهي تشكيلات إسقاطية ذات بعد 1 ،اهتم العديد من الباحثين في دراسة هذه المنحنيات منهم :William, fulton,Bezout,silverman Lucas ,Caushy,Poincare, , Tate,Bachet, Mazure,Siegel, وآخرون ، و نظرية موردیل (Mordell) التي دمجت الهندسة والجبر و نظرية الأعداد مع بعضها البعض في نظرية واحدة تعد من أعظم نظريات القرن العشرين والتي تنص على أن لزمرة النقاط الكسرية على منحني إهليلجي عدد منته من المولدات.

وعلى الرغم من تسمية هذه المنحنيات بالإهليلجية (الناقصية) إلا أنها ليست قطوع ناقصة إنما تعود هذه التسمية لكون هذه المنحنيات قد نشأت من دراسة مسألة كيفية حساب طول قوس قطع ناقص . إن أغلب المنحنيات التكعيبية هي منحنيات غير شاذة ويمكن كتابة كل منحني غير شاذ بصيغة وايرستراش التالية :

$y^2 = x^3 + \mathrm{a}x^2 + bx$ والتي تسمى معادلة وايرستراش .السؤال المهم هنا هل لهذا المنحني نقاط كسرية فوق حقل ما𝕜 ،و أي من هذه النقاط منتهي الرتبة ،إن إيجاد الحلول الصحيحة والكسرية لهذه المعادلات غير مدروس بشكل كامل إلا في حالات خاصة والتي تحتاج إلى مزيج من الهندسة والجبر ونظرية الأعداد، ولعل نظرية Siegel التي أثبت فيها أن هنالك فقط عدد منته من الحلول الصحيحة لمعادلة منحني إهليلجي غير شاذ من أهم النظريات في هذا المجال ،ولدراسة بعض المنحنيات الاهليلجية تم الاعتماد على تقنيات من الهندسة الجبرية وبشكل أدق هندسة المنحنيات الملساء [1] .

ليكن C المنحني الإهليلجي الذي معادلته: $y^2 = x^3 - Nx$ حيث N عدد صحيح موجب حر من التربيع . في عام *2007* بين *spearman* أنه إذا كان $N = u^4 + v^4$ عدد أولي وفردي حيث u, v أعداد صحيحة فإن $rank\left(C(Q)\right) = 2$ ، وبين أيضا *spearman* أنه إذا كانت $N = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4$ هو ضعفي عدد أولي فإن $rank\left(C(Q)\right) = 3$. وفي عام 2011 قام الباحثان Fujita و Terai بإثبات أنه إذا كان N من الشكل $N = a^2 + b^4$ عندئذ فإن $rank\left(C(Q)\right) = 2$. وفي 2012 أعطى fujita اشكالا للعدد الصحيح N تجعل رتبة المنحني $C: y^2 = x^3 - Nx$ تساوي *3*أو *4* .وفي عام 2016 أثبت Daghigh و Didari أنه إذا كان N عدد أولي فردي فإن رتبة المنحني الإهليلجي $C: y^2 = x^3 - 3Nx$ هي على الأكثر *2* .

وفي عام 2023 أثبت *kim* أنه من أجل المنحني الإهليلجي الذي معادلته: $E_{-2p}: y^2 = x^3 - 2p$ حيث p عدد أولي فردي يحقق $p = 6t^4 - 8t^3u - 8tu^3 + 16t^2u^2 + 3u^4 w.i.t.u.1$ فإن:

$$rank\left(E_{(30u^4-10u^2v^2+9v^4)(304^4-10u^2v^2+11v^4}\right)(Q) = rank(E_{-2p})$$

أهمية البحث و أهدافه :

يهدف هذا البحث إلى دراسة النقاط الكسرية فوق المنحني الإهليلجي الذي معادلته من الشكل :

$$E: y^2 = x^3 \pm pqx$$

،وتكمن أهمية هذا البحث في دراسة نوع خاص من المنحنيات الاهليلجية المعطاة بمعادلة وايرستراش والتي تملك على الأقل نقطة ذات رتبة تساوي 2 .

طرائق البحث ومواده:

اعتمدنا في هذه الدراسة على تعاريف ومبرهنات أساسية ونتائج متعلقة بالمنحنيات الإهليلجية مستخلصة من مراجع علمية تخصصية وبحوث علمية منشورة في دوريات عالمية .

المفاهيم الأساسية والرموز المستخدمة :

• **تعريف 1 ، [2] (Elliptic curve over $\mathbb{k}$)**: ليكن $\mathbb{k}$حقل بحيث أن $\mathrm{char}(\mathbb{k}) \neq 2,3$ يعرَف المنحني الإهليلجي فوق$\mathbb{k}$ بأنه منحني أملس ذو فجوة واحدة بالإضافة لنقطة اللانهاية ويعرَف هذا المنحني بمعادلة وايرستراش التالية :

$C: y^2 = x^3 + Ax + B;\ \Delta = -(4a^3 - 27b^2) \neq 0$ ،حيث Δ يسمى مميز المنحني .

تعريف 2 ، [2] قانون التشكيل(The group law) : لتكن $P_1(x_1, y_1), P_2(x_2, y_2)$ نقطتان على المنحني الإهليلجي $C: y^2 = x^3 + ax^2 + bx + c$ فوق الحقل $\mathbb{k}$عندئذ :

$$P_1 + P_2 = P_3(x_3, y_3);\ x_3 = \lambda^2 - a - x_1 - x_2, y_3 = \lambda x_3 + v$$

حيث : $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}, v = y_1 - \lambda x_1 = y_2 - \lambda x_2$

تعريف 3 , [2] (رتبة نقطة) (Order of a point): نقول عن عنصر ما P من زمرة النقاط الكسرية $C(\mathbb{Q})$ أن له رتبة تساوي m إذا تحقق الشرط:

$$\forall\ m > m' \geq 1\ ;\ m'P \neq O$$ و $$mP = O$$

ونقول عندها أن ل P رتبة منتهية ،وإلا فنقول أن لها رتبة غير منتهية .

ونرمز لمجموعة النقاط ذات الرتبة المنتهية m بالشكل:

$$C(\mathbb{k})(m) = \{P \in C(\mathbb{k}); mP = O\} \cup \{O\}$$

تعريف 4 ، [2] (زمرة الالتفاف) (Torsion group): إن مجموعة كل النقاط الكسرية ذات الرتبة المنتهية مع قانون التشكيل المعرف سابقا تشكل زمرة ندعوها زمرة الالتفاف ونرمز لها $C(\mathbb{k})_{tors}$ ويكون :

$$C(\mathbb{k})_{tors} = \bigcup_{m=1}^{\infty} C(\mathbb{k})(m)$$

نظرية (mordell)[3]:(من أجل المنحنيات الاهليلجية التي تملك نقطة كسرية ذات رتبة 2) ليكن C منحني تكعيبي غير شاذ معطى بالمعادلة

$$C: y^2 = x^3 + ax^2 + bx$$

حيث a, b أعداد صحيحة عندئذ فإن زمرة النقاط الكسرية $C(\mathbb{Q})$ هي زمرة آبلية منتهية التوليد.

مبرهنة [4] : ليكن C منحني وايرستراش . عندئذ C يكون غير شاذ إذا وفقط إذا كانت $\Delta \neq 0$

مبرهنة [2]: ليكن C منحني وايرستراش شاذ عندئذ يكون ل C عقدة إذا وفقط إذا كانت $C_4 \neq 0$ و يكون ل C قرنة إذا وفقط إذا كان $C_4 = 0$

نظرية (Nagell-lutz) [5] : ليكن المنحني التكعيبي غير الشاذ C حيث :

$$C: y^2 = f(x) = x^3 + ax^2 + bx + c$$

حيث المعاملات a, b, c صحيحة وليكن Δ المميز لكثيرة الحدود التكعيبية $f(x)$:

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

ولتكن $P = (x, y)$ نقطة كسرية ذات رتبة منتهية عندئذ فإن x, y أعداد صحيحة بالاضافة لذلك فإما أن يكون $y = 0$ أو أن يكون y يقسم Δ.

نظرية (Mazur) [6] : ليكن المنحني التكعيبي الكسري غير الشاذ C بحيث أن $C(Q)$ تمتلك نقطة ذات رتبة منهية m عندئذ إما أن تكون $m = 12$ أو $1 \leq m \leq 10$

وبشكل أدق فإن مجموعة النقاط ذات الرتبة المنتهية في $C(Q)$ تشكل زمرة جزئية لها أحد الشكلين الآتيين :

(1) زمرة دورية من ذات رتبة N حيث $1 \leq N \leq 10$ أو $N = 12$

(2) جداء زمرة دورية ذات رتبة 2 مع زمرة دورية من المرتبة $2N$ حيث $1 \leq N \leq 4$.

نظرية (*Bezout's theorem*)[7] :
ليكن $\mathbb{k}$حقل مغلق جبريا ولتكن f و g كثيرتي حدود غير صفريتين في $\mathbb{k}[x,y,z]$ واللتان ليس لهما عوامل مشتركة عندئذ فإن :

$$\sum_{p\in P^2} I_p(f,g) = \deg(f)\,.\deg(g)\,.$$

تعريف 5، [3] : ليكن المنحني C المعطى بالمعادلة $C: y^2 = f(x) = x^3 + ax^2 + bx$ ولنعرف المنحني $\bar{C}$ المعطى بالمعادلة:

$$\bar{C}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x\ ;\ \bar{a} = -2a, \bar{b} = a^2 - 4b$$

ولنعرف التطبيقان $\emptyset, \Psi$ بالشكل :

$$\emptyset: C \to \bar{C};\quad \emptyset(x,y) = (\bar{x},\bar{y}):$$
$$\bar{x} = x + a + \frac{b}{x} = \frac{y^2}{x^2}\ , \bar{y} = \frac{y(x^2-b)}{x^2}$$
$$\Psi: \bar{C} \to C\ ;\ \Psi(\bar{x},\bar{y}) = (\frac{\bar{y}^2}{\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b}}{\bar{x}^2})$$

مبرهنة [3] : ليكن C و $\bar{C}$ منحنيين إهليلجيين معرفين بالمعادلتين :

$$C: y^2 = x^3 + ax^2 + bx$$
$$\bar{C}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x\ ;\ \bar{a} = -2a\ , \bar{b} = a^2 - 4b$$

ولتكن $T = (0,0) \in C$ عندئذ :

(a) يوجد هومومورفيزم $\emptyset : C \to \bar{C}$ معرف بالشكل :

$$\emptyset(\mathrm{p}) = \begin{cases} (\dfrac{y^2}{x^2}, \dfrac{y(x^2-b)}{x^2} & ; if\ p = (x,y) \neq O,T \\ \bar{O}\ ; if\ p = O\ or\ p = T \end{cases}$$

نواة $\emptyset$ هي $\{O,T\}$

(b) بتطبيق نفس الإجراء ل $\bar{C}$ يعطي تطبيق $\bar{\emptyset}: \bar{C} \to \bar{\bar{C}}$ المنحني $\bar{\bar{C}}$ إيزومورفي ل$\bar{C}$ وفق التطبيق $(x,y) \to (\frac{1}{4}x, \frac{1}{8}y)$ يوجد بالتالي هوموموفيزم $\Psi: \bar{C} \to C$ معرف بالشكل:

$$\Psi(\bar{p}) = \begin{cases} (\dfrac{\bar{y}^2}{\bar{x}^2}, \dfrac{\bar{y}(\bar{x}^2-\bar{b})}{\bar{x}^2}\ ; if\ \bar{p} = (\bar{x},\bar{y}) \neq O,T \\ O\ if\ \bar{p} = \bar{O}\ or\ \bar{p} = \bar{T} \end{cases}$$

(c) التركيب $\Psi \square \emptyset$ هو تطبيق الضرب ب 2 أي : $\Psi \square \emptyset(\mathrm{p}) = 2\mathrm{p}$.

تعريف 6، [3] : لتكن Γ مجموعة النقاط الكسرية على المنحني الاهليلجي C أي $\Gamma = C(Q)$
ولنعرف التطبيق α :

$$\alpha : \Gamma \to Q^*/Q^{*^2}$$
$$\propto (O) = 1\ (mod\ Q^{*^2})$$
$$\propto (T) = b\ (mod\ Q^{*^2})$$
$$\propto (x,y) = x\ \left(mod\ Q^{*^2}\right)\ ;\ x \neq 0$$

ويرمز ب $\bar{\Gamma}$ لمجموعة النقاط الكسرية على المنحني الاهليلجي $\bar{C}$.

مبرهنة [3] : ليكن $\propto$ التطبيق المعرف سابقا عندئذ :

(1) التطبيق $\propto$ هوموموفيزم .

(2) نواة $\propto$ هي الصورة $\Psi(\bar{\Gamma})$ ، وبالتالي ينتج عن $\propto$ هوموموفيزم تقابل واحد_لواحد

$$\Gamma/\Psi(\bar{\Gamma}) \to Q^*/Q^{*^2}$$

(3) لتكن $\rho_1, \rho_2, \ldots \rho_t$ الاعداد الاولية المختلفة التي تقسم b عندئذ فإن صورة $\propto$ هي الزمرة الجزئية من Q^*/Q^{*^2}المكونة من العناصر :

$$\{\pm{\rho_1}^{e_1}{\rho_2}^{e_2}{\rho_3}^{e_3}\ldots.{\rho_t}^{e_t}\,;e_i=0\ or\ 1\}$$

(4) الدليل $(\Gamma:\Psi(\overline{\Gamma}))$ يساوي على الاكثر 2^{t+1} .

مبرهنة[8] : ليكن E المنحني الإهليلجي الذي معادلته :

$$y^2=x^3-37px$$

حيث p عدد أولي يكتب بالشكل :

$$p=125u^4+36u^2v^2+2v^2.w.i.u.v.1\,;p\equiv 3(mod\ 16)$$

عندئذ فإن : $rank\ (E)(Q)=1$.

مبرهنة [8]: ليكن E المنحني الإهليلجي الذي معادلته :

$$y^2=x^3-37px$$

حيث: $p=48841u^4+442u^2v^2+948v^2.w.i.u.v.1\ \ ;p\equiv 7(mod\ 16)$

عندئذ فإن : $rank\ (E)(Q)=1$.

مبرهنة[9]: ليكن E المنحني الإهليلجي الذي معادلته :

$$y^2=x^3+2pqx$$

حيث p و q عددان أوليان يحققان: $p\equiv 5(mod\ 16), q\equiv 5(mod\ 16)$

عندئذ فإن : $rank\ (E)(Q)=0$.

مبرهنة [9]: ليكنE_{-2p} المنحني الإهليلجي الذي معادلته:$E_{-2p}: y^2=x^3-2p$ حيث p عدد أولي فردي يحقق $p=6t^4-8t^3u-8tu^3+16t^2u^2+3u^4w.i.t.u.1$ فإن:

$$rank\left(E_{(30u^4-10u^2v^2+9v^4)(304^4-10u^2v^2+11v^4}\right)(Q)=rank(E_{-2p})$$

مثال [10]:يأخذ المنحنيين :

$$E: y^2=x^3-17x\ ,\overline{E}:\ y^2=x^3+68x$$

عندئذ: $\#\alpha\ (\Gamma)=4$ ، $\alpha\ (\overline{\Gamma})=4$ ومنه فإن : $rank\ (E)(Q)=2$

مبرهنة [11] : ليكن E_{4p} المنحني الإهليلجي المعطى بالمعادلة $y^2=x^3+4px$ حيث p عدد أولي يحقق $p\equiv 1(mod\ 8)$: ويكتب بالشكل $p=t^2+16$ حيث t عدد صحيح فردي ، وليكن E_{-4p} المنحني الإهليلجي : $y^2=x^3-4px$ حيث p عدد أولي يحقق $p\equiv 5(mod\ 16)$ ويكتب بالشكل : $p=324+t^2$ عندئذ فإن رتبتي E_{4p} و E_{-4p} هما على الترتيب 2 و 1 .

تعريف 7، [12] :اذا كان p عدد أولي و a عدد صحيح نعرف رمز ليجندر ل a بالقياس ل p بالشكل :

$$\left(\frac{a}{p}\right)=\begin{cases}1\ ; & \text{إذا كان } a \text{ باقي تربيعي بالمقاس ل } p\\ -1\ ; & \text{إذا كان } a \text{ باقي غير تربيعي بالمقاس ل } p\end{cases}$$

مبرهنة (قاعدة ضرب البواقي التربيعية)[12]: ليكن p عدد أولي فردي و a, b أعداد صحيحة عندئذ فإن :

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$$

مبرهنة [12]: ليكن p عدد أولي فردي عندئذ :

$$\left(\frac{-1}{p}\right)=\begin{cases}1; & \text{إذا كان } p\equiv 1\ (mod\ 4)\\ -1\ ; & \text{إذا كان } p\equiv 3\ (mod\ 4)\end{cases}$$

نظرية (تمهيدية غاوس) [13] : ليكن p عدد أولي فردي عندئذ :

$$\left(\frac{2}{p}\right)=\begin{cases}1; & \text{إذا كان } p\equiv 1\ (mod\ 8) \text{ أو } p\equiv 7\ (mod\ 8)\\ -1\ ; & \text{إذا كان } p\equiv 3\ (mod\ 8) \text{ أو } p\equiv 5\ (mod\ 8)\end{cases}$$

ملاحظة 1:

بالرغم من أننا عملنا في هذا البحث على إيجاد الرتبة لأشكال خاصة من المنحنيات الإهليلجية من أجل تحديد جميع النقاط الكسرية عليها إلا أن تحديد الرتبة قد يكون غاية في الصعوبة في بعض الأحيان لذلك يجدر بنا الإشارة إلى أنه تم اتباع العديد من الطرق المبتكرة لإيجاد نقاط كسرية فوق المنحنيات الإهليلجية دون الاستعانة بالرتبة وكذلك لإيجاد أسر من المنحنيات الاهليلجية والتي تملك نقاط كسرية غير مبتذلة ونذكر منها الطريقة التي اتبعها [14] sultanowو آخرون حيث عملو على إيجاد بعض الشروط على العددين الاوليين p ,q لكي يكون للمنحني الاهليلجي $y^2 = x^3 - pqx$ نقاط كسرية غير مبتذلة من خلال دراسة تقاطع هذا المنحني مع المستقيم الذي معادلته $y = \frac{a}{b}x$.

النتائج و المناقشة:

مبرهنة 1:ليكن لدينا المنحني الإهليلجي C الذي معادلته :

$C: y^2 = x^3 - pqx$; p≡3(mod 8),q≡3(mod 8) حيث p,q عددان أوليان يحققان $p = 8t^2 + 3$ و $q = 7t^2 + 3$ ليكن التطبيق ∝ حيث :

$$\alpha : \Gamma \rightarrow Q^*/Q^{*^2}$$

حيثΓ مجموعة النقاط الكسرية فوق المنحني C عندئذ فإن :

$\alpha(\Gamma)=\{1, -pq, p, -q\}$ أي تكون : $\#\alpha(\Gamma) = 4$.

الاثبات: لدينا $b=b_1b_2$:$\alpha(\Gamma)\in\{1, -pq, -1, pq, p, -q, q, -p\}$

ندرس قابلية حل كل من المعادلات التالية:

$$N^2 = M^4 - pqe^4 \quad ①$$
$$N^2 = -M^4 + pqe^4 \quad ②$$
$$N^2 = pM^4 - qe^4 \quad ③$$
$$N^2 = qM^4 - pe^4 \quad ④$$

لكن لدينا : $-pq, 1 \in \alpha(\Gamma)$ والمعادلة ① لها حل دوما حيث لها الحل الخاص$(N, e, M) = (1,0,1)$.

دراسة المعادلة ② $N^2 = -M^4 + pqe^4$:

وبأخذ التطابق بالقياس ل p لهذه المعادلة نجد : $N^2 \equiv -M^4 (mod\ p)$

لكن بما أن $p \equiv 3(mod\ 4)$ (حيث$p \equiv 3(mod\ 8)$) فإن 1- باقي غير تربيعي بالنسبة للمقاس p وهذا يناقض كون N^2 باقي تربيعي بالنسبة للمقاس p، إذا ليس للتطابق حلول وبالتالي المعادلة ② مستحيلة الحل وبالتالي $p,-1 \notin \propto (\Gamma)$

دراسة المعادلتين ④ و ③

بما أن $p \equiv q \equiv 3(mod\ 4)$ (حيث$p \equiv q \equiv 3(mod\ 8)$) فإن أحد التطابقين $q \equiv x^2 (mod\ p), p \equiv x^2 (mod\ q)$ له حل والآخر ليس له حل (حيث$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$) لكن لدينا:

$$p = 8t^2 + 3 = t^2 + 7t^2 + 3 \equiv t^2 + q \equiv t^2 (mod\ q)$$

وبالتالي p باقي تربيعي بالنسبة للمقاس q وبالتالي فإن q باقي غير تربيعي للمقاس p،

بأخذ $e = 1, M = 1$ في المعادلة ③ $N^2 = pM^4 - qe^4$ فنجد :

$N^2 = q - p = 8t^2 + 3 - (7t^2 + 3) = t^2$ وبالتالي $(M, e, N) = (1,1,t)$ حل للمعادلة ③ فالمعادلة ③ قابلة للحل وبالتالي $p, -q \in \propto (\Gamma)$.

و بأخذ التطابق للمعادلة ④ $N^2 = qM^4 - pe^4$ بالنسبة للمقاس p ينتج

$N^2 \equiv qM^4 (mod\ p)$ لكن q باقي غير تربيعي بالنسبة للمقاس p وبالتالي ليس لهذا التطابق حل ومنه المعادلة ④ مستحيلة الحل وبالتالي. $q, -p \notin \propto (\Gamma)$.

ينتج أن $\alpha(\Gamma)=\{1,-pq,p,-q\}$ ومنه : $\#\alpha(\Gamma)=4$.

◧

مبرهنة 2 : لنأخذ المنحني $\bar{C}$ الذي معادلته :

$\bar{C}: y^2 = x^3 + 4pqx = 0$; p≡3(mod 8),q≡3(mod 8) وليكن التطبيق $\bar{\propto}$ حيث :

$$\bar{\alpha}:\bar{\Gamma} \rightarrow Q^*/Q^{*^2}$$

عندئذ فإن :$\bar{\propto}(\bar{\Gamma})=\{1,4pq\}$ أي تكون : $\#\bar{\propto}(\bar{\Gamma})=2$.

الإثبات:

وجدنا من المبرهنة السابقة $\left(\frac{q}{p}\right)=-1$ و $\left(\frac{p}{q}\right)=1$

ولدينا: $\bar{\propto}(\bar{\Gamma}) \in \{\pm 1, \pm 4pq, \pm 2pq, \pm 2, \pm 4p, \pm q, \pm p, \pm 4q, \pm 4, pq, \pm 2p, \pm 2q, \}$

ويكون لدينا المعادلات المتعلقة ب $\bar{\Gamma}$ التالية لدراستها :

$$N^2 = M^4 + 4pqe^4 \quad ①$$
$$N^2 = 2pqM^4 + 2e^4 \quad ②$$
$$N^2 = 4pM^4 + qe^4 \quad ③$$
$$N^2 = pM^4 + 4qe^4 \quad ④$$
$$N^2 = 4M^4 + pqe^4 \quad ⑤$$
$$N^2 = 2pM^4 + 2qe^4 \quad ⑥$$

بما أن $\bar{\propto}(\bar{o}) = 1$ و $\bar{\propto}(\bar{T}) = 4pq$ فإن $1,4pq \in \bar{\propto}(\bar{\Gamma})$ فالمعادلة ① لها حل دوما . ونلاحظ أن $pq \equiv 4pq \pmod{Q^{*^2}}$ و $4 \equiv 1 \pmod{Q^{*^2}}$ وبالتالي المعادلة ⑤ لا داعي لدراستها لأننا لا نحصل على عناصر جديدة في $\bar{\propto}(\bar{\Gamma})$.

•دراسة المعادلة ② $N^2 = 2pqM^4 + 2e^4$:

بأخذ التطابق بالقياس ل p نجد:

$N^2 \equiv 2e^4 (mod\ p)$ هذا التطابق مستحيل الحل لأن 2 باقي غير تربيعي بالنسبة للمقاس p وبالتالي المعادلة ② مستحيلة الحل .

لدراسة قابلية حل المعادلات ③و ④ و ⑥ نميز حالتين :

(1)_ في حالة $p \equiv x^2 (mod\ q)$ ليس له حل و $q \equiv x^2 (mod\ p)$ له حل عندئذ:

بأخذ التطابق للمعادلة ③ $N^2 = 4pM^4 + qe^4$ بالنسبة للمقاس q:

$N^2 \equiv 4pM^4 (mod\ q)$ وبما أن p باقي غير تربيعي بالنسبة للمقاس q هنا فإن هذا التطابق ليس له حلول وبالتالي المعادلة ③ مستحيلة الحل .

وبأخذ التطابق للمعادلة ④ $N^2 = pM^4 + 4qe^4$ بالنسبة للمقاس q :

$N^2 \equiv pM^4 \pmod{q}$ هذا التطابق ليس له حلول وبالتالي المعادلة ④ ليس لها حلول.

و بأخذ التطابق للمعادلة ⑥ $N^2 = 2pM^4 + 2qe^4$ بالنسبة للمقاس p نجد :

$N^2 \equiv 2qe^4 (mod\ p)$ بما أن 2 باقي غير تربيعي للمقاس p بينما q باقي تربيعي للمقاس p فإن $2q$ باقي غير تربيعي للمقاس p وبالتالي التطابق الأخير ليس له حلول وبالتالي المعادلة ⑥ مستحيلة الحل .

(2)_ في حالة $p \equiv x^2 (mod\ q)$ له حل و $q \equiv x^2 (mod\ p)$ ليس له حل عندئذ :

بأخذ التطابق للمعادلة ③ $N^2 = 4pM^4 + qe^4$ بالنسبة للمقاس p:

$N^2 \equiv qe^4 (mod\ p)$ هذا التطابق ليس له حلول وبالتالي المعادلة ③ مستحيلة الحل .

و بأخذ التطابق للمعادلة ④ $N^2 = pM^4 + 4qe^4$ بالنسبة للمقاس p :

$N^2 \equiv 4qe^4 \pmod{p}$ هذا التطابق ليس له حلول وبالتالي المعادلة ④ ليس لها حلول .

و بأخذ التطابق للمعادلة ⑥ $N^2 = 2pM^4 + 2qe^4$ بالنسبة للمقاس q نجد :

$N^2 \equiv 2pM^4 (mod\ q)$ بما أن 2 باقي غير تربيعي للمقاس q بينما p باقي تربيعي للمقاس q فإن $2p$ باقي غير تربيعي بالنسبة للمقاس q وبالتالي التطابق الأخير ليس له حلول وبالتالي المعادلة ⑥ مستحيلة الحل من كلا

الحالتين (1) و (2) نستنتج أن المعادلات ③ و ④ و ⑥ ليس لها حلول وبالتالي: $p, q, 2p, 2q, 4p, 4q \notin \bar{\propto}(\bar{\Gamma})$.ومنه نجد أن :
$\bar{\propto}(\bar{\Gamma})=\{1,4pq\}$ أي تكون : $\#\bar{\propto}(\bar{\Gamma})=2$.

◧

نتيجة 1: رتبة المنحني الاهليلجي الذي معادلته :

C:$y^2=x^3-pqx$; p≡3(mod 8),q≡3(mod 8)

حيث p,q عددان أوليان يحققان $p=8t^2+3, q=7t^2+3$
فوق الحقل $\mathbb{Q}$ هي $rank\ (C)(\mathbb{Q})=1$.
الإثبات :
وجدنا سابقا أن $\#\propto(\Gamma)=4, \#\bar{\propto}(\bar{\Gamma})=2$
وبالتالي نجد : $2^r=\frac{\propto(\Gamma).\bar{\propto}(\bar{\Gamma})}{4}$ ومنه $2^r=\frac{2^2\cdot 2^1}{4}=1$ وبالتالي $rank\ (C)(Q)=1$.

◧

مبرهنة 3: ليكن لدينا المنحني الإهليلجي E_{pq} الذي معادلته :

$E_{pq}: y^2=x^3+pqx$; p≡3(mod 8),q≡3(mod 8)

حيث p,q عددان أوليان يحققان $p=t^2-2t+8, q=3t^2+16$ عندئذ فإن :

$$rank(E_{(t^2-2t+8)(3t^2+16)}(\mathbb{Q}))=1\ or\ 2$$

برهان :
لدينا المعادلات المتعلقة ب Γ التالية :

$$N^2=M^4+pqe^4 \quad ①$$
$$N^2=pM^4+qe^4 \quad ②$$

أولا نلاحظ أن :$4p-q=(t-4)^2$ ومنه فإن : $4\mathrm{P}\equiv(t-4)^2\ (mod\ q)$ أي أن p باقي تربيعي بالقياس ل q وبما أن $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=-1$ فإن $\left(\frac{q}{p}\right)=-1$.
و بما أن $1, pq\in\propto(\Gamma)$ لا داعي لدراسة المعادلة ① , حيث يكون لها الحل الخاص $(M,e,N)=(1,0,1)$
نأخذ المعادلة ② بالقياس ل p نجد :

$$N^2\equiv qe^4(mod\ p) \quad \text{وبالتالي نجد:} \quad 1=\left(\frac{N^2}{p}\right)=\left(\frac{qe^4}{p}\right)=\left(\frac{q}{p}\right)=-1$$

وهذا تناقض وبالتالي المعادلة ② لايمكن أن يكون لها حلول صحيحة غير مبتذلة .
وبالتالي يكون $\#\alpha(\Gamma)=2$.
الآن لنأخذ المنحني $\bar{E}: y^2=x^3-4pqx$
فيكون لدينا المعادلات المتعلقة ب $\bar{\Gamma}$ التالية :

① $N^2=M^4-4pqe^4$	⑦ $N^2=-4qM^4+pe^4$
② $N^2=-4M^4+qpe^4$	⑧ $N^2=-M^4+4pqe^4$
③ $N^2=4M^4-pqe^4$	⑨ $N^2=2M^4-2pqe^4$
④ $N^2=-4pM^4+qe^4$	⑩ $N^2=-2M^4+2pqe^4$
⑤ $N^2=4pM^4-qe^4$	⑪ $N^2=2pM^4-2qe^4$
⑥ $N^2=4\mathrm{q}M^4-pe^4$	⑫ $N^2=-2pM^4+2qe^4$

نلاحظ $1,-4pq\epsilon\bar{\propto}(\bar{\Gamma})$ لذلك لا داعي لدراسة المعادلة ① .
كما نلاحظ أن :$1\equiv 4\ (\mathrm{mod}\ Q^{*2})$ كذلك $-4\mathrm{pq}\equiv-\mathrm{pq}\ (\mathrm{mod}\ Q^{*2})$ لذلك فإن دراسة المعادلة ③ لا تعطينا عناصر جديدة في $\bar{\propto}(\bar{\Gamma})$ لذلك لا داعي لدراستها .
نأخذ المعادلة ② بالقياس ل p فنجد :

$$N^2 \equiv -4M^4(mod\ p) \Rightarrow 1 = \left(\frac{N^2}{p}\right) = \left(\frac{-4M^4}{p}\right) = \left(\frac{-4}{p}\right) = (\frac{-1}{p}) = -1$$

وهذا تناقض وبالتالي المعادلة② ليس لها حلول صحيحة غير مبتذلة .

كذلك بأخذ المعادلة ④ بالقياس ل p فنجد :

$$N^2 \equiv \mathrm{q}e^4(mod\ p) \Rightarrow 1 = \left(\frac{N^2}{p}\right) = \left(\frac{qe^4}{p}\right) = \left(\frac{q}{p}\right) = -1$$

وهذا تناقض وبالتالي المعادلة④ لا يمكن أن يكون لها حلول صحيحة غير مبتذلة .

الآن : نكتب المعادلة ⑤ بالشكل :

$$N^2 = 4(t^2 - 2t + 8)M^4 - (3t^2 + 16)e^4 \quad ⑤$$

وبأخذ $e = M = 1$ نحصل على :

$$N^2 = 4(t^2 - 2t + 8) - (3t^2 + 16) = 4t^2 - 8t + 32 - 3t^2 - 16 = t^2 - 8t + 16 = (t-4)^2$$

وبالتالي $(M, e, N) = (1,1, t-4)$ حل للمعادلة ⑤، وبالتالي $4p, -q \in \bar{\alpha}(\bar{\Gamma})$.

ونلاحظ $4\mathrm{p} \equiv \mathrm{p}\ (\mathrm{mod}\ Q^{*2})$ كذلك $-\mathrm{q} \equiv -4\mathrm{q}\ (\mathrm{mod}\ Q^{*2})$ وبالتالي لا حاجة لدراسة المعادلة ⑦ لأنها لا تعطينا عناصر جديدة في $\bar{\alpha}(\bar{\Gamma})$.

نأخذ المعادلة ⑥ بالقياس ل p نجد:

$$N^2 \equiv 4\mathrm{q}M^4(mod\ p) \Rightarrow 1 = \left(\frac{N^2}{p}\right) = \left(\frac{4qM^4}{p}\right) = \left(\frac{q}{p}\right) = -1$$

وهذا تناقض وبالتالي المعادلة⑥ ليس لها حلول صحيحة غير مبتذلة .

نأخذ المعادلة ⑧ بالقياس ل p نجد :

$$N^2 \equiv -M^4(mod\ p) \Rightarrow 1 = \left(\frac{N^2}{p}\right) = \left(\frac{-M^4}{p}\right) = \left(\frac{-1}{p}\right) = -1$$

تناقض وبالتالي المعادلة ⑧ مستحيلة الحل .

نأخذ المعادلة ⑨ بالقياس ل p نجد :

$$N^2 \equiv 2M^4(mod\ p) \Rightarrow 1 = \left(\frac{N^2}{p}\right) = \left(\frac{2M^4}{p}\right) = \left(\frac{2}{p}\right) = -1$$

تناقض وبالتالي المعادلة ⑨ مستحيلة الحل .

نأخذ المعادلة ⑪ بالقياس ل q نجد :

$$N^2 \equiv 2pM^4(mod\ p) \Rightarrow 1 = \left(\frac{N^2}{q}\right) = \left(\frac{2pM^4}{q}\right) = \left(\frac{2p}{q}\right) = -1$$

تناقض وبالتالي المعادلة ⑪ مستحيلة الحل .

الآن بقي لدينا المعادلتان :

$$N^2 = -2M^4 + 2pqe^4 \quad ⑩ \qquad \text{و} \qquad N^2 = -2pM^4 + 2qe^4 ⑫$$

ولدينا حتى الآن أربعة عناصر في $\bar{\Gamma}$) $\overline{\propto}$ هي $\{1, -4pq, 4p, -q\} \subseteq \overline{\propto}(\bar{\Gamma})$ وبقيت لدينا أربعة قيم إضافية محتملة في هذه الزمرة هي $-2, 2pq, -2p, 2q$ وبما أن $\# \overline{\propto}(\bar{\Gamma}) = 2^t$ من الشكل : $\# \overline{\propto}(\bar{\Gamma})$ حيث t عدد طبيعي، نستنتج أنه إما أن تكون كل من المعادلتين قابلة للحل أو كلاهما غير قابلة للحل وبالتالي ينتج أنه إما $\# \overline{\propto}(\bar{\Gamma}) = 2^2$ أو $\# \overline{\propto}(\bar{\Gamma}) = 2^3$.

لدينا $2^r = \frac{\propto(\Gamma).\overline{\propto}(\bar{\Gamma})}{4}$

ومنه إما أن تكون $2^r = \frac{2^2 \cdot 2^1}{4} = 2^1$ أو $2^r = \frac{2^3 \cdot 2^1}{4} = 2^2$ وبالتالي ينتج :

$$rank(E_{(t^2-2t+8)(3t^2+16)}(Q)) = 1\ or\ 2$$

◧

نتيجة 2 : ليكن المنحني الإهليلجي C الذي معادلته :

$$E_{pq}: y^2 = x^3 + pqx \quad ; p = 8k+3, q = 8l+3 \quad ; k,l \in N$$

حيث p,q عددان أوليان يحققان $p = t^2 - 2t + 8, q = 3t^2 + 16$ عندئذ فإنه إذا كان $l - k$ مربعا كاملا فإن :

$$rank(E_{(t^2-2t+8)(3t^2+16)}(Q)) = 2$$

برهان :

أولا بما أن $p = t^2 - 2t + 8, q = 3t^2 + 16$ نلاحظ أن q > p أيا يكن العدد الحقيقي t وبالتالي فإن $l > k$

بما أن معطيات هذه النتيجة تتطابق مع معطيات المبرهنة 3 بالاضافة للشرط الاخير لدينا من المبرهنة 3 $\#\alpha(\Gamma) = 2$.

كذلك وجدنا أن $\{1, -4pq, 4p, -q\} \subseteq \overline{\propto}(\bar{\Gamma})$ وأن كل من المعادلات ⑪,⑨,⑧,⑦,⑥,④,② مستحيلة الحل لذلك $\#\overline{\propto}(\bar{\Gamma}) = 4 \text{ or } 8$ أي أنه إما كل من المعادلتين

⑩ $N^2 = -2M^4 + 2pqe^4$ و ⑫ $N^2 = -2pM^4 + 2qe^4$

لها حل أو كلاهما ليس له حل لكن لدينا بوضع $e = m = 1$ في المعادلة ⑫ نجد:

$$N^2 = -2(8k+3) + 2(8k+3) = -16k - 6 + 16l + 6 = 16(l-k)$$

وبالتالي نجد أن $(M, e, N) = (1,1,4\sqrt{l-k})$ هو حل للمعادلة ⑫ .

وبالتالي $\#\overline{\propto}(\bar{\Gamma}) = 2^4$ وبالتالي $-2p, 2q, -2, 2pq \in \overline{\propto}(\bar{\Gamma})$

وبالتالي $2^r = \frac{2^3 \cdot 2^1}{4} = 2^2$ ومنه $rank(E_{(t^2-2t+8)(3t^2+16)}(Q)) = 2$.

◧

مبرهنة 4 : ليكن لدينا المنحني الإهليلجي E_{4pq} الذي معادلته :

$$E_{pq}: y^2 = x^3 - 4pqx \text{ ; p≡3(mod 8),q≡3(mod 8)}$$

حيث p,q عددان أوليان يحققان $p = t^2 - 2t + 8, q = 3t^2 + 16$ عندئذ فإن :

$$rank(E_{(t^2-2t+8)(3t^2+16)}(Q)) = 1 \text{ or } 2$$

و إذا كان $l - k$ مربعا كاملا فإن :

$$rank(E_{(t^2-2t+8)(3t^2+16)}(Q)) = 2$$

البرهان : لدينا المعادلات المتعلقة ب Γ التالية :

① $N^2 = M^4 - 4pqe^4$	⑦ $N^2 = -4qM^4 + pe^4$
② $N^2 = -4M^4 + qpe^4$	⑧ $N^2 = -M^4 + 4pqe^4$
③ $N^2 = 4M^4 - pqe^4$	⑨ $N^2 = 2M^4 - 2pqe^4$
④ $N^2 = -4pM^4 + qe^4$	⑩ $N^2 = -2M^4 + 2pqe^4$
⑤ $N^2 = 4pM^4 - qe^4$	⑪ $N^2 = 2pM^4 - 2qe^4$
⑥ $N^2 = 4qM^4 - pe^4$	⑫ $N^2 = -2pM^4 + 2qe^4$

وبما أن الشروط على p, q تتطابق مع الشروط الواردة في المبرهنة 3 وبالتالي فإن

$1, -4pq, 4p, q \in \alpha(\Gamma)$ وفي الحالة التي يكون فيها $l - k$ مربعا كاملا فإن

$1, -4pq, 4p, q - 2p, 2q, -2, 2pq \in \alpha(\Gamma)$

وبالتالي $\alpha(\Gamma) = 2^2 \text{ or } 2^3$

الآن نأخذ المنحني $\bar{E}_{4pq}: y^2 = x^3 + 16pqx$ و يكون لدينا المعادلات المتعلقة ب $\bar{\Gamma}$ التالية:

① $N^2 = M^4 + 16pqe^4$	② $N^2 = 4pqM^4 + 4e^4$
③ $N^2 = 16pM^4 + qe^4$	④ $N^2 = pM^4 + 16qe^4$
⑤ $N^2 = 2M^4 + 8pqe^4$	⑥ $N^2 = 2pM^4 + 8qe^4$

$N^2 = 8pM^4 + 2qe^4$ ⑦ $N^2 = 4pM^4 + 4qe^4$ ⑧

$N^2 = 16M^4 + pqe^4$ ⑨ $N^2 = 8M^4 + 2pqe^4$ ⑩

بما أن $1,16pq \in \overline{\propto}\ \bar{\Gamma}$ فلا حاجة لدراسة المعادلة ① كما أن $1 \equiv 4 \equiv 16(mod\ Q^{*2})$ و $16pq \equiv 4pq \equiv pq(mod\ Q^{*2})$ وبالتالي لا داعي لدراسة المعادلتين ② و ⑨ لأنها لا تعطينا عناصر جديدة في $\overline{\propto}\ \bar{\Gamma}$

نأخذ المعادلة ③ بالقياس ل p فنجد :

$$N^2 \equiv qe^4 (\text{mod p})$$

$$1 = \left(\frac{N^2}{p}\right) = \left(\frac{qe^4}{p}\right) = \left(\frac{q}{p}\right) = -1$$

تناقض وبالتالي المعادلة ③ مستحيلة الحل .

نأخذ المعادلة ④ بالقياس ل p كذلك نجد

$$N^2 \equiv 16qe^4 (mod\ p)$$

ومنه : $1 = \left(\frac{N^2}{p}\right) = \left(\frac{16qe^4}{p}\right) = \left(\frac{q}{p}\right) = -1$ تناقض وبالتالي المعادلة ④ مستحيلة الحل .

نأخذ المعادلة ⑤ بالقياس ل p نجد:

$1 = \left(\frac{N^2}{p}\right) = \left(\frac{2M^4}{p}\right) = \left(\frac{2}{p}\right) = -1$ تناقض فالمعادلة ⑤ مستحيلة الحل .

نأخذ المعادلة ⑥بالقياس ل q نجد:

$1 = \left(\frac{N^2}{q}\right) = \left(\frac{2pM^4}{q}\right) = \left(\frac{2p}{q}\right)\left(\frac{p}{q}\right) = -1$ تناقض فالمعادلة ⑥مستحيلة الحل .

نأخذ المعادلة ⑦بالقياس ل q نجد:

$$1 = \left(\frac{N^2}{q}\right) = \left(\frac{8pM^4}{q}\right) = \left(\frac{8}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{p}{q}\right) = -1$$

تناقض فالمعادلة ⑦مستحيلة الحل . نأخذ المعادلة ⑧بالقياس ل p نجد:

$$1 = \left(\frac{N^2}{p}\right) = \left(\frac{4qe^4}{p}\right) = \left(\frac{q}{p}\right) = -1$$

تناقض فالمعادلة ⑧مستحيلة الحل

بأخذ المعادلة ⑩ بالقياس ل p نجد :

$$1 = \left(\frac{N^2}{p}\right) = \left(\frac{8M^4}{p}\right) = \left(\frac{2}{p}\right) = -1$$

فالمعادلة ⑩ مستحيلة الحل .

ينتج أن : $\overline{\propto}\ (\bar{\Gamma}) = 2$ وبالتالي $2^r = \frac{2^3 \cdot 2^1}{4} = 2^2$ أو $2^r = \frac{2^2 \cdot 2^1}{4} = 2^1$ و منه :

$$rank(E_{4(t^2-2t+8)(3t^2+16)}(Q)) = 1\ or\ 2$$

◧

مثال 1 :

ليكن لدينا المنحني $C: y^2 = x^3 - pqx$ حيث p,q عددان أوليان يحققان $p = 8t^2 + 3, q = 7t^2 + 3$ من أجل $t = 2o$ نجد $p = 3203\ , q = 2803$ كل من pو q أولي و يطابق 3 بالمقاس ل 8 وبالتالي بحسب النتيجة 1 فإن زمرة النقاط الكسرية لها :

$$C(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$.

مع النقطة المولدة *(120812,2416240)= (x,y)*.

مثال عن المبرهنتين 1 و 2 مع النتيجة 1:

t	*p*	*q*	*r*	*generator*
20	*30203*	*20803*	*1*	*(120812,2416240)*

أمثلة عن المبرهنة 3:

t	p	q	rank
3	11	43	2
7	43	163	1 or 2
11	107	379	1 or 2
27	683	2203	1 or 2
35	1163	3691	1 or 2
59	3371	10459	1 or 2

أمثلة عن المبرهنة 4:

t	p	q	rank	generator
3	11	43	2	(44,-44)
7	43	163	1 or 2	(172,516)
11	107	379	1 or 2	(428,2996)
27	683	2203	1 or 2	(2732,62836)
35	1163	3691	1 or 2	(4652,144212)
59	3371	10459	1 or 2	(13484,741620)

الاستنتاجات والتوصيات:

في هذا البحث تمت دراسة بعض المنحنيات الإهليلجية ذات الشكل $y^2 = x^3 \pm Nx$ التي تملك على الأقل نقطة كسرية ذات رتبة 2 ، حيث تم إيجاد زمرة النقاط الكسرية لهذه المنحنيات فوق الحقل $\mathbb{Q}$ بالإضافة لدراسة البنية الجبرية لهذه النقاط والحصول على بعض النتائج المتعلقة بها

إن دراسة المنحنيات الاهليلجية من الشكل $y^2 = x^3 \pm Nx$ والنتائج التي توصلنا إليها تعتبر من المسائل المهمة في الدراسات الحديثة للمنحنيات الإهليلجية واستخداماتها المختلفة ، نوصي بدراسة هذا النوع من المنحنيات من أجل قيم أخرى للعدد N ثم الاستفادة من هذه الدراسة للتعميم على هذ النوع من المنحنيات .

References:

[1SANKARI,H, BOJAKLI,M.*Torsion Point on Modular Curves.*Tishreen university journal S.A. vol .43, No.23,2021,49-60.

[2] SILVERMAN,J,H,Tate,J, The Arithmetic of Elliptic Curves .springer-verlag, New York,2009,45-103.

[3] MILNE,J,S, Elliptic curves, University of Michigan, V1.01, Aug.21.1996, 41-55.

[4] SILVERMAN,J,H,Tate,J. Rational points on Elliptic curves . Springer,New York,2015, 56-105.

[5] ADAMSSON,A,Points of Finite Order of an Elliptic Curve over the Rational Numbers, Stockholms University,2018,14-23

[6] BONNEVIER.E, An Introduction to Algebraic Geometry and Bezout's Theorem,Stockholms University,2018 35-47.

[7] FULTON,W, Algebraic curves ,An Introduction to Algebraic Geometry,Princeton University,2008, 57-59.

[8] KIM,S,W. *Ranks in Elliptic Curves* $y^2 = x^3 - 37px$ *and* $y^2 = x^3 - 61px$ *and* $y^2 = x^3 - 67px$ *and* $y^2 = x^3 - 83px$ *and* $y^2 = x^3 - 947px$,International Journal of algebra , vol.17, May. 23,2023 ,121-142.

[9] KIM,S,W.*Ranks in Elliptic curves* $y^2 = x^3 \pm Ax$. International Jornal of Contemporary Mathematical science ,vol.18,no.1,2023, 22.
[10] KIM,S,W. *Ranks of Elliptic Curves* $y^2 = x^3 \pm 4px$. International Journal of Algebra Nov.5,2015 205-211.
[11] KHALAFALLAH,H, Mordell-Well Theorem and the Rank of Elliptic Curves,California State University ,2007, 33 .
[12] NIVEN,N,M,ZUCKERMAN,H,S,MONTGOMERY,H,L,An introduction to the theory of numbers , first Eddition ,Wiley,J,Inc ,S,1991, 131-150.
[13] KOPAL,J. Diophantine equations,National Institute of Science Education ,Pune ,2015, 8-62.
[14]SULTANOW,E,AMIR,M,HATZIILIOU,A,TFAIHA,A,TEHRANI,M,BUCHANNAN ,B.ON Families Of Elliptic Curves $E_{pq}: y^2 = x^3 - pqx$ That Intersects The same line $L_{a,b}: y = \frac{a}{b}x$ Of Rational Slope ,2023 1-13.