تعریف[chapter] قضیه[definition] لم[definition] نتیجه[definition] مثال[definition]

دانشگاه شهید مدنی آذربایجان

وزارت علوم، تحقیقات و فناوری
دانشگاه شهید مدنی آذربایجان
دانشکده علوم پایه
گروه ریاضی محض

پایان نامه
جهت اخذ درجه کارشناسی ارشد
رشته ریاضی محض

خم‌های بیضوی وابسته به میدان‌های ساده درجه چهار

استاد راهنما
دکتر فرضعلی ایزدی

پژوهشگر
فرزانه دیانتی

خرداد ۹۲
تبریز - ایران


بسم الله الرحمن الرحیم

تقدیم به مهربان فرشتگانی که:

لحظات ناب باور بودن، لذت و غرور دانستن، جسارت خواستن،
عظمت رسیدن و تمام تجربه های یکتا و زیبای زندگیم، مدیون حضور سبز
آنهاست

تقدیم به خانواده عزیزم. بخصوص برادر ارجمندم که در تمام عرصه های زندگی و تحصیل با تمام وجود یاریگر و مشوق
بنده بودند و پدر و مادر بزرگوار و همسر مهربانم.

خدایا...

دستر ابه ناپیدایی تو گشوده‌ام، چنان که در ذکری عالم گیر به سمت تو آمده اند!

آن قدر بزرگی، که هستی و همه ی اسبابش ملک کوچکی از املاک توست.

خدایا!

نمی دانم که کلمه را چگونه تقدیمت دارم، حال آن که کلمه آفریده توست، و چه موهبتی که تو نیز با کلمه با من سخن گفته ای...

بر انگشتانم که نگاه پر عطوفت خود را معطوف می داری توان نوشتن در آن ها جاری می شود!

خدایا!

اگر بخواهیم که مطلوب دیگران باشیم، تو اسبابش را به ما داده ای و ما را به سرعت به هدفان می رسانی، اما افسوس که این دلخوشی نه لذت بخش است و نه پایدار!

اما اگر بخواهیم مطلوب تو باشیم، سخت است و به دیده ای دست نیافتنی، اما آهسته آهسته شیرین است و پایدار...

خدایا!

مرا مطلوب خود گردان و از روی رحمت و فضل و بخشش ات با من مدارا کن!

خدایا!

در آستانه نیاز و فقر کامل خود به سویت رو کرده‌ام و می دانم که تو بی منتهای بی نیازی!

خدایا!

از نداشته هایم آن چه را که می دانم و نمی دانم و تو خوب به همه ی آن ها واقفی، نصیبم فرما...

به امید رحمتت...

سپاس گزاری...

سپاس خدایی را که اولین معلم است.
در آغاز وظیفه خود می‌دانم از زحمات بی‌شائبه استاد راهنمای خود، جناب آقای **دکتر فرضعلی ایزدی**، که شبانه‌روز وقت خود را با صبر و حوصله و متانت که نشانگر بار علمی سنگین ایشان می‌باشد در اختیار حقیر قرار داده‌اند تشکر و قدردانی کنم .
از اساتید گرامی جناب آقای **دکتر اسمعیل عابدی** و جناب آقای **دکتر مجتبی رنجبر** که زحمت داوری این پایان‌نامه را تقبل فرمودند کمال امتنان را دارم.

فرزانه دیانتی
خرداد ۱۳۹۲

فهرست مطالب

چکیده

در این پایان نامه، خانواده‌ای نا متناهی از خم‌های بیضوی پارامتری وابسته به میدان‌های ساده درجه ۳ را مورد مطالعه قرار می‌دهیم. اگر رتبه چنین خم‌هایی برابر ۱ باشد، ساختار گروهی و نقاط صحیح این خم‌ها را پیدا می‌کنیم. هم‌چنین نتایج مشابهی برای زیر خانواده‌ای نامتناهی از خم‌های با رتبه ۲ بدست می‌آوریم. این کار یعنی تعیین ساختار گروهی و یافتن نقاط صحیح برای اولین بار روی خانواده‌ای نامتناهی از خم‌های بیضوی از رتبه ۲ انجام شده است. ارتفاع کانونی ابزار اصلی ما برای این مطالعه است.

.

کلمات کلیدی: خم بیضوی، رتبه خم بیضوی، میدان ساده درجه چهار، ارتفاع کانونی، گروه موردل-ویل، نقاط صحیح.

پیشگفتار

خم‌های بیضوی یکی از شاخه‌های بسیار مهم در هندسه حسابی است. در بسیاری از مسائل دیوفانتی، اساس کار استفاده از خم‌های بیضوی است. خم‌های بیضوی در تعیین اعداد اول و تجزیه اعداد صحیح به عوامل اول کاربرد دارند. در سال ۱۹۹۴، وایلز توانست [۱] از خاصیت‌های خم‌های بیضوی استفاده کرده و آخرین قضیه فرما [۲] را اثبات کند. هم‌چنین خم‌های بیضوی با رتبه بالا، به خاطر بالا بودن ضریب امنیت سیستم حاصل از آن‌ها در رمزنگاری مورد استفاده قرار می‌گیرند.

هدف ما در این پایان‌نامه حل دو مسئله دیوفانتی زیر است:

۱- تعیین ساختار گروه موردل-ویل $\mathrm{Q}_t(\mathbb{Q})$ (یا به طور معادل $\mathrm{C}_t(\mathbb{Q})$)، که در آن

$\mathrm{Q}_t(\mathbb{Q}) : Y^2 = X^4 - tX^3 - 6X^2 + tX + 1$ و $\mathrm{C}_t(\mathbb{Q}) : y^2 = x^3 - \left(16 + t^2\right)x$.

۲- تعیین همه نقاط صحیح روی Q_t و C_t.

در این خصوص ما به نتایج زیر می‌رسیم:

(۱) رتبه هرگز صفر نیست،

(۲) رتبه زوج تنها به کلاس هم‌نهشتی t به مدول ۱۶ بستگی دارد،

(۳) نقطه $[-4, 2t]$ همیشه جزء مولدهای $\mathrm{C}_t(\mathbb{Q})$ است،

(۴) در حالتی که رتبه برابر ۱ و t زوج باشد، تنها نقاط صحیح روی C_t عبارتند از $[0, 0], [-4, \pm 2t]$ و $\left[\frac{t^2}{4} + 4, \pm\left(\frac{t^3}{8} + 2t\right)\right]$،

(۵) در حالتی که رتبه برابر ۱ باشد، $[0, \pm 1]$ تنها نقاط صحیح روی Q_t هستند،

(۶) در رتبه‌های بالاتر نقاط صحیح معدودی روی Q_t وجود دارند که یک نقطه با مختص-x

[۱] Wiles

[۲] Fermat

مساوی ۳- جزء آن‌ها است.

این پایان‌نامه شامل سه فصل است. در فصل اول به ارائه تعاریف و مفاهیمی از خم‌های بیضوی که در فصل‌های بعدی مورد استفاده قرار می‌گیرند، می‌پردازیم. در فصل دوم به اختصار در مورد میدان‌های ساده بحث شده است. نهایتاً در فصل سوم ساختار گروهی و نقاط صحیح روی خم‌های بیضوی وابسته به میدان‌های ساده درجه چهار را تعیین می‌کنیم.

فصل ۱

تعاریف و مفاهیم اولیه

۱.۱ معادله خم بیضوی

فرض‌کنید K یک میدان جبری دلخواه باشد. صفحه آفین را روی این میدان با $A^{۲}_{\mathrm{K}}$ نشان می‌دهیم. فرض‌کنید $C \in \mathrm{K}[x,y]$ یک چندجمله‌ای تحویل‌ناپذیر باشد. مجموعه صفرهای C در این صفحه آفین یک خم آفین روی K است، این مجموعه را بصورت زیر نشان می‌دهیم:

$$\{(x,y) \in \mathrm{K} \times \mathrm{K} : C(x,y) = ۰\}.$$

با همگن کردن معادله $C(x,y) = ۰$ یعنی نوشتن معادله در صفحه تصویری $\mathbb{P}^{۲}_{\mathrm{K}}$ معادله $C([x:y:z]) = ۰$ را بدست می‌آوریم که همه جملات آن دارای درجه یکسانی هستند.

تعریف ۱.۱.۱. خم بیضوی E به فرم وایراشتراس کلی روی میدان K به‌صورت زیر تعریف می‌شود:

$$C : y^{۲} + a_{۱}xy + a_{۳}y = x^{۳} + a_{۲}x^{۲} + a_{۴}x + a_{۶}$$

که در آن $a_{۶}, ..., a_{۱}$ ثابت‌هایی در میدان K هستند.

معادله C به فرم

$$C : y^{۲} + a_{۱}xy + a_{۳}y = x^{۳} + a_{۲}x^{۲} + a_{۴}x + a_{۶}$$

را در صفحه آفین $A^{۲}_{\mathrm{K}}$ در نظر می‌گیریم. با همگن‌سازی معادله C معادله همگن

$$y^{۲}z + a_{۱}xyz + a_{۳}yz^{۲} = x^{۳} + a_{۲}x^{۲}z + a_{۴}xz^{۲} + a_{۶}z^{۳}$$

را بدست می‌آوریم. با جاگذاری $z = ۰$ داریم $x = ۰$، تنها کلاس هم‌ارزی با شرط $x = z = ۰$ عبارت است از $[۰ : ۱ : ۰]$. نقطه اشتراک محور y ها با خط در بی‌نهایت $([۰ : ۱ : ۰])$ را نقطه در بی‌نهایت نامیده و آنرا با $\mathfrak{O}$ نشان می‌دهیم. که این نقطه عضو همانی گروه خم بیضوی است. می‌توان مجموعه نقاط معادله همگن C را در صفحه تصویری به صورت زیر تعریف کرد.

تعریف ۱.۱.۲. مجموعه نقاط معادله همگن C را در صفحه تصویری $\mathbb{P}^{۲}_{\mathrm{K}}$ به صورت

$$E(\mathrm{K}) = \{(x, y) \in \mathrm{K} \times \mathrm{K} | y^{۲} + a_{۱}xy + a_{۳}y = x^{۳} + a_{۲}x^{۲} + a_{۴}x + a_{۶}\} \cup \{\infty\}$$

تعریف می‌کنند.

اگر میدان F توسیع میدان K باشد، آنگاه

$$E(\mathrm{F}) = \{(x, y) \in \mathrm{F} \times \mathrm{F} | y^{۲} + a_{۱}xy + a_{۳}y = x^{۳} + a_{۲}x^{۲} + a_{۴}x + a_{۶}\} \cup \{\infty\}.$$

تعریف ۱.۱.۳. مبین خم بیضوی E را با $\triangle$ نشان داده و تعریف می‌کنیم:

$$\triangle = b^{۲}_{۲}b_{۸} - ۸b^{۳}_{۴} - ۲۷b^{۲}_{۶} + ۹b_{۲}b_{۴}b_{۶}$$

که در آن

$$b_{۲} = a^{۲}_{۱} + ۴a_{۲},$$

$$b_{۴} = ۲a_{۴} + a_{۱}a_{۳},$$

$$b_{۶} = a^{۲}_{۳} + ۴a_{۶},$$

$$b_{۸} = a_{۱}a_{۲}a_{۶} + ۴a_{۲}a_{۴} - a_{۱}a_{۳}a_{۶} + a_{۲}a^{۲}_{۳} - a^{۲}_{۴}.$$

تعریف ۴.۱.۱. فرض کنید مشخصه میدان دو و سه نباشد. در این صورت خواهیم داشت:

$$(y+\frac{a_1x}{2}+\frac{a_3}{2})^2=x^3+(a_2+\frac{a_1^2}{4})x^2+(a_4+\frac{a_1a_3}{2})x+(\frac{a_3^2}{4}+a_6)$$

می‌توانیم بنویسیم

$$y_1^2=x^3+\bar{a}_2x^2+\bar{a}_4x+\bar{a}_6$$

که در آن $y_1=y+\frac{a_1x}{2}+\frac{a_3}{2}$ و $\bar{a}_6,\bar{a}_4,\bar{a}_2$ ثابت‌هایی در میدان میباشند و هم‌چنین با قرار دادن $x_1=x+\frac{\bar{a}_2}{3}$ خواهیم داشت:

$$y_1^2=x_1^3+Ax_1+B$$

که در آن A و B ثابت‌هایی در میدان $\mathbb{K}$ هستند. این معادله را معادله وایر اشتراس می‌نامند.

بنا به تعریف ۴.۴.۱، مبین خم یعنی $\triangle$ بصورت $\triangle=-(4A^3+27B^2)$ در می‌آید.

اگر r_3,r_2,r_1 ریشه‌های مجزای معادله درجه سه باشند. می‌توان نشان داد که مبین این معادله درجه سه به صورت زیر است

$$((r_1-r_2)(r_1-r_3)(r_2-r_3))^2=-\left(4A^3+27B^2\right).$$

تعریف ۵.۱.۱. نقطه $P_0=(x_0,y_0)$ را روی خم

$$y^2-x^3-Ax-B=F(x,y)$$

نقطه تکین می‌نامند هرگاه

$$F(P_0)=0,\qquad \frac{\partial F}{\partial x}\mid_{P_0}=0,\qquad \frac{\partial F}{\partial y}\mid_{P_0}=0.$$

به عبارت دیگر، نتوان در نقطه P_0 بر منحنی خط مماس منحصربفرد رسم کرد.

تعریف ۶.۱.۱. خم بیضوی E را هموار نامیم هرگاه نقطه تکین نداشته باشد.

گزاره ۷.۱.۱. *فرض‌کنید* $F(x,y,z)=y^2z-x^3-Axz^2-Bz^3=0$ *خم بیضوی روی میدان* $\mathbb{K}$ $(char(\mathbb{K})\neq 2,3)$ *با* $\triangle\neq 0$ *باشد، دراین‌صورت خم هموار است.*

برهان. فرض‌کنید $P=(x:y:z)$ نقطه تکین منحنی $F(x,y,z)=y^۲z-x^۳-Axz^۲-Bz^۳=۰$ باشد(ف خ)، دراین‌صورت

$$F_x=-۳x^۲-Az^۲,\quad F_y=۲yz,\quad F_z=y^۲-۲Axz-۳Bz^۲.$$

دو حالت $z=۰$ و $z\neq ۰$ را در نظر می‌گیریم. حالت $z=۰$ نقطه در بی‌نهایت خم بیضوی را می‌دهد. در این حالت داریم، $F_x=۰$ و $F_y=۰$ لذا $x=۰$ و $y=۰$ بنابراین، $P=(۰:۰:۰)$ که غیرممکن است زیرا نقاط در $\mathbb{P}^۲_K$ هستند. اگر $z\neq ۰$ لذا $z=۱$. در این حالت داریم، $F_y=۰$ لذا $y=۰$ بنابراین، $P=(x:۰:۱)$ بایستی در $x^۳+Ax+B=۰$ و $F_x=-۳x^۲-A$ صدق کند و این به این معنی است که $(x:۰:۱)$ ریشه مضاعف منحنی است که تناقض است. لذا خم بیضوی نقطه تکین ندارد و هموار است. □

گزاره ۸.۱.۱. *فرض‌کنید $F(x,y)=y^۲-f(x)=۰$ خم بیضوی باشد. اگر $(x_۰,y_۰)$ نقطه‌ای روی خم باشد. خم در این نقطه هموار است اگر و فقط اگر حداقل یکی از $\frac{\partial F}{\partial x}$ و $\frac{\partial F}{\partial y}$ در این نقطه نا صفر باشند.*

برهان. رجوع شود به [۵]. □

خم‌های بیضوی که ما با آنها سروکار داریم، هموار فرض می‌شوند. بنابراین مشتقات جزئی آنها نباید همزمان صفر شود یعنی

$$۲y+a_۱x+a_۳=۰\quad,\quad a_۱y=۳x^۲+۲ax+a_۴.$$

در هیچ نقطه (x,y) روی خم توأماً صفر نباشند.

قضیه ۹.۱.۱. *خم بیضوی به فرم وایراشتراس منفرد است اگر و فقط اگر مبین آن صفر باشد. بطور معادل خم بیضوی منفرد است اگر و فقط اگر دارای ریشه مضاعف باشد.*

برهان. قضیه را در حالتی که خم به شکل $y_۱^۲=x_۱^۳+Ax_۱+B$ باشد ثابت می‌کنیم. اثبات در حالت کلی نیز به همین صورت است.

فرض‌کنید که خم $y_1^2 = x_1^3 + Ax_1 + B$ در نقطه $\mathrm{P} = (x_0, y_0)$ منفرد باشد. تعریف می‌کنیم $F(x,y) = y^2 - f(x)$. بنا به منفرد بودن خم در $\mathrm{P} = (x_0, y_0)$ خواهیم داشت $\frac{\partial F}{\partial y} = 2y = 0$ و بنابراین $y = 0$. همچنین $\frac{\partial F}{\partial y} = -f(x) = -3x^2 - a = 0$ اما $y = 0$ اگر و فقط اگر $f(x) = 0$. بنابراین منفرد بودن در x_0 زمانی رخ می‌دهد که $f(x_0) = f'(x_0) = 0$. یعنی x_0 ریشه مشترک f, f' است. در نتیجه f در x_0 دارای ریشه مضاعف است. □

تبصره ۱.۱.۱۰. *اگر معادله به شکل $cy^2 = dx^3 + ax + b$ باشد، آن‌گاه با ضرب طرفین معادله در c^3d^2 ، معادله زیر*

$$(c^2dy)^2 = (cdx)^3 + (ac^2d)(cdx) + (bc^3d^2)$$

حاصل می‌شود. با تغییر متغییرهای $y_1 = c^2dy$ و $x = cdx$ ، معادله به فرم وایر اشتراس تبدیل می‌شود.

۲.۱ ساختار گروه روی خم بیضوی

برای ایجاد گروه باید یک عمل تعریف شود. فرض‌کنید E خم بیضوی روی میدان $\mathbb{K}$ به معادله $y^2 = x^3 + Ax + B$ و نقاط P_1 و P_2 دو نقطه متعلق به خم باشند.

۱.۲.۱ قانون جمع روی خم بیضوی

تعریف ۱.۲.۱. ابتدا خط گذرا از P_1 و P_2 را رسم می‌کنیم و آنرا L می‌نامیم. خط L منحنی E را در یک نقطه سوم، $\bar{\mathrm{P}_3}$ قطع می‌کند. ممکن است این نقطه یکی از نقاط P_1 و P_2 باشد. بازتاب $\bar{\mathrm{P}_3}$ نسبت به محور x ها نقطه P_3 را بدست می‌دهد و تعریف می‌کنیم:

$$P_۱ + P_۲ = P_۳.$$

تبصره ۲.۲.۱. *اگر $P_۱ = P_۲$، آنگاه خط گذرنده از $P_۱$ و $P_۲$، مماس بر خم در این نقطه می‌باشد.*

حال به ارائه فرمول‌هایی برای محاسبه $P_۱ + P_۲$ می‌پردازیم.

$$P_۱ = (x_۱, y_۱) \quad , \quad P_۲ = (x_۲, y_۲) \quad , \quad \bar{P_۳} = (x_۳, y_۳) \quad , \quad P_۳ = (x_۳, -y_۳).$$

• فرض کنید $P_۱ \neq P_۲$ و هیچکدام برابر ∞ نباشند. آن‌گاه شیب خط گذرا از نقطه‌های $P_۱$ و $P_۲$ برابر است با:

$$m = \frac{y_۲ - y_۱}{x_۲ - x_۱}$$

◦ اگر $x_۱ \neq x_۲$. آن‌گاه معادله خط L به‌صورت زیر می‌باشد.

$$y = m(x - x_۱) + y_۱$$

برای پیدا کردن تقاطع این خط و خم، معادله خط را در معادله خم جای‌گذاری می‌کنیم.

$$(m(x - x_۱) + y_۱)^۲ = x^۳ + Ax + B.$$

با مرتب کردن آن خواهیم داشت:

$$۰ = x^۳ - m^۲x^۲ + \cdots.$$

مجموع سه ریشه معادله درجه سوم برابر منفی ضریب جمله $x^۲$ از آن معادله می‌باشد. برای نشان دادن علت آن به روش ذیل عمل می‌کنیم:
فرض کنید ریشه‌های معادله درجه سوم $x^۳ + ax^۲ + bx + c$ برابر با $tgsr$ باشند. آن‌گاه:

$$x^۳ + ax^۲ + bx + c = (x - r)(x - s)(x - t) = x^۳ - (r + s + t)x^۲ + \cdots.$$

پس

$$r+s+t=-a.$$

بنابراین اگر ما دو ریشه r و s از معادله را داشته باشیم می‌توانیم ریشه سوم را از عبارت $t=-a-r-s$ به‌دست آوریم. پس با توجه به گفته‌های بالا خواهیم داشت:

$$x_۳=m^۲-x_۱-x_۲.$$

و هم‌چنین با جای‌گذاری در معادله خط داریم:

$$y_۳=m\,(x_۳-x_۱)+y_۱.$$

در نتیجه داریم

$$\bar{\mathrm{P}_۳}=(x_۳,-y_۳)=\left(m^۲-x_۱-x_۲,m\,(x_۱-x_۳)-y_۱\right)$$

◦ اگر $x_۱=x_۲$ آن‌گاه خط L خط عمودی است بنابراین خم را در نقطه ∞ قطع می‌کند که قرینه نقطه ∞ نسبت به محور x ها همان ∞ را به‌دست می‌دهد. بنابراین:

$$\mathrm{P}_۱+\mathrm{P}_۲=\infty.$$

• فرض کنید $\mathrm{P}_۱=\mathrm{P}_۲$ و مخالف ∞ در این‌صورت خط گذرا از این دو نقطه مماس بر خم در این نقطه می‌باشد. بنابراین شیب خط برابر است با:

$$۲Y\frac{\partial y}{\partial x}=۳x^۲+A\Longrightarrow m=\frac{\partial y}{\partial x}=\frac{۳x_۱^۲+A}{۲y_۱}.$$

◦ اگر $y_۱=۰$. آن‌گاه خط مماس، خط عمودی است. بنابراین

$$\bar{\mathrm{P}_۳}=\infty\Longrightarrow\mathrm{P}_۱+\mathrm{P}_۲=\infty.$$

◦ و اگر $y_۱\neq۰$. آن‌گاه همانند قسمت قبل و با در نظر گرفتن $x_۱=x_۲$ داریم

$$\bar{\mathrm{P}_۳}=(x_۳,-y_۳)=\left(m^۲-۲x_۱,m\,(x_۱-x_۳)-y_۱\right)$$

هم‌چنین تعریف می‌کنیم $\mathrm{P}_۱+\infty=\mathrm{P}_۱$، پس با تعمیم این تعریف داریم $\infty+\infty=\infty$.

۲.۲.۱ وارون

اگر $P_۱ = (x_۱, y_۱)$ آن‌گاه $-P_۱ = (x_۱, -y_۱)$. برای توجیه این تعریف به روش ذیل عمل می‌کنیم: فرض کنید که نقطه $P_۱$ را با نقطه مورد ادعای $-P_۱$ جمع کنیم. در این صورت خط عبوری از $P_۱$ و $-P_۱$ عمود خواهد بود، بنابراین سومین نقطه مشترک در روی خم ∞ خواهد بود. حال ∞ به ∞ وصل کرده و سومین نقطه تقاطع را می‌یابیم. از وصل کردن ∞ به ∞ خطی در بی‌نهایت حاصل می‌شود که سومین نقطه نیز ∞ است، چرا که خط در بی‌نهایت، خم را در $\infty * \infty * \infty$ قطع می‌کند. این نشان می‌دهد که $P_۱ + (-P_۱) = \infty$. بنابراین $-P_۱$ همان قرینه $P_۱$ است. واضح است که $-\infty = \infty$.

مثال ۳.۲.۱. *فرض کنید*

$$E(\mathbb{Q}) : y^۲ = x^۳ - ۴۳X + ۱۶۶.$$

ثابت می‌کنیم که $P = (۳, ۸) \in E(\mathbb{Q})$. $۲P, ۳P, ۴P$ *و* $۸P$ *را محاسبه می‌کنیم و* P *را با* $۸P$ *مقایسه می‌کنیم.*

حل: $P \in E(\mathbb{Q})$ *زیرا*

$$۸^۲ = ۳^۳ - ۴۳ \cdot ۳ + ۱۶۶ \quad \longrightarrow \quad ۶۴ = ۲۷ - ۱۲۹ = ۱۶۶.$$

برای پیدا کردن $۲P$ *داریم:*

$$m = \frac{۳ \cdot ۹ - ۴۳}{۱۶} = -۱ \quad , \quad y_۱ - mx_۱ = ۸ - (-۱)۳ = ۱۱.$$

پس

$$x(۲P) = (-۱)^۲ - ۲ - ۳ = -۵ \quad , \quad y(۲P) = -(m.x(۲P) + ۱۱) = -۱۶.$$

برای محاسبه $۴P$ *داریم:*

$$m = \frac{۳(-۵)^۲ - ۴۳}{-۳۲} = -۱ \quad , \quad y_۱ - mx_۱ = (-۱۶) - (-۱)(-۵) = -۲۱,$$

$$x(۴P) = (-۱)^۲ - ۲(-۵) = ۱۱ \quad , \quad y(۴P) = -((-۱) \cdot ۱۱ - ۲۱) = ۳۲.$$

برای $۸P$ داریم:

$$m = \frac{۳۰ \cdot ۱۱^۲ - ۴۳}{۶۴} = ۵ \quad , \quad y_۱ - mx_۱ = ۳۲ - ۵ - ۱۱ = -۲۳.$$

$$x(۸P) = ۵^۲ - ۲ \cdot ۱۱ = ۳ \quad , \quad y(۸P) = -(۵ \cdot ۳ - ۲۳) = ۸.$$

توجه داریم که $۸P = P$ پس $۷P = \infty$ پس $۳P = -۴P$. بنابراین

$$x(۳P) = x(-۴P) = x(۴p) = ۱۱,$$

$$y(۳P) = y(-۴P) = -y(۴P) = -۳۲.$$

قضیه ۴.۲.۱. *جمع نقاط روی خم بیضوی E در شرایط زیر صدق می‌کند:*

۱. *برای هر $P_۱, P_۲$ روی E، $P_۱ + P_۲ = P_۲ + P_۱$.* (*جابه‌جایی*)

۲. *برای هر P روی E، $P + \infty = P$.* (*عضو همانی*)

۳. *برای هر P روی E نقطه‌ای مانند $\bar{P}$ موجود است به‌طوری که $P + \bar{P} = \infty$ که این نقطه $\bar{P}$ را $-P$ تعریف می‌کنیم.*(*عضو قرینه*)

۴. *برای هر $P_۱$، $P_۲$، $P_۳$ روی E، $(P_۱ + P_۲) + P_۳ = P_۱ + (P_۲ + P_۳)$.* (*شرکت‌پذیری*)

برهان. رجوع شود به [۱۴] □

بنابراین نقاط روی خم تحت عمل جمع گروه آبلی با عضو همانی ∞ را تشکیل می‌دهند.

۳.۱ پارامتر پایای j

معادله

$$y^۲ + a_۱xy + a_۳y = x^۳ + a_۲x^۲ + a_۴x + a_۶$$

را با روابط زیر