تعمیمی از مسألهٔ اعداد همنهشت

وحیده رسولی

دانشکدهٔ علوم

گروه ریاضی

مهر ۱۳۹۱

پایان‌نامهٔ کارشناسی ارشد

استاد راهنما:

دکتر علی سرباز جانفدا

تقدیم به

آنان که آفتاب مهرشان در آستان قلبم هیچ‌گاه غروب نخواهد کرد.

استاد عشق، پدرم

آوای خوش زندگی‌ام، همسرم

برادران و خواهران همراهم

به پاس تعبیر عظیم و لطیف از کلمه‌ی "ایثار" و به پاس عاطفه‌ی سرشار و گرمای امیدبخش وجودش که در سردترین روزگار بهترین پشتیبان بود، تقدیم به "روح مادرم".

تقدیر و تشکر

همواره سر بر آستان کبریایی حق می‌ساییم و برکات و یاوری‌هایش را در هر زمینه سپاس می‌گوییم.

اینک که در سایه‌ی الطاف بی‌پایان الهی این دوره از تحصیلاتم با نگارش این رساله به پایان می‌رسد لازم می‌دانم از کلیه‌ی اساتید و بزرگوارانی که چه در طول تحصیل و چه در طول تهیه و تدوین این پایان‌نامه قبول زحمت فرموده و مرا یاری و راهنمایی نموده‌اند سپاسگزاری نمایم.

از استاد راهنمای ارجمند جناب آقای دکتر علی سرباز جانفدا که همواره با رهنمودهای ارزشمند خویش روشنگر مسیر پایان‌نامه بودند، کمال تشکر و قدردانی را دارم.

از اساتید فرهیخته جناب آقای دکتر هوشنگ بهروش و جناب آقای دکتر رضا سزیده که زحمت داوری این پایان‌نامه را بر عهده داشتند، سپاسگزاری می‌نمایم.

از خانواده‌ی عزیزم که در تمام مراحل زندگی همراه من بودند و همیشه از دعای خیرشان بهره‌مند بودم تشکر و قدردانی می‌نمایم.

در پایان از کلیه‌ی دوستان به پاس تمام خوبیها کمال تشکر را دارم.

چکیده

در این پایان‌نامه، یک تعمیم معین از مسأله‌ی اعداد همنهشت کلاسیک را مطالعه می‌کنیم. مخصوصاً، مساحت‌های صحیح از مثلث‌های قائم‌الزاویه، با یک زاویه‌ی دلخواه θ $(\frac{\pi}{3} \leq \theta < \pi)$ را مورد بررسی قرار می‌دهیم. این اعداد θ—همنهشت نامیده می‌شوند. یک آزمون خم بیضوی برای تعیین این‌که عدد صحیح داده شده‌ی n عددی θ—همنهشت است یا نه، ارائه می‌دهیم. سپس "چگالی" اعداد صحیح n را که θ—همنهشت می‌باشند بررسی می‌کنیم.

پیش‌گفتار

مطالعه‌ی مثلث‌های قائم‌الزاویه با اضلاع صحیح به کاری از فیثاغورس [۱] و اقلیدس [۲] بر می‌گردد. ریاضیدانان یونان به‌طور کامل چنین مثلث‌هایی را طبقه‌بندی کرده‌اند. یکی از این طبقه‌بندی‌ها مربوط به مثلثی با اضلاع خوب [۳] است که برای اولین بار توسط ریاضیدانان عرب در قرن ده مورد مطالعه قرار گرفت. در این طبقه‌بندی از همه‌ی مساحت‌های صحیح ممکن از مثلث‌های قائم‌الزاویه با اضلاع گویا سؤال می‌شود. این طبقه‌بندی به مسأله‌ی اعداد همنهشت معروف است.

عدد صحیح مثبت n را یک عدد همنهشت می‌نامیم هرگاه برابر با مساحت مثلث قائم‌الزاویه با اضلاع گویا باشد. در قرن سیزدهم میلادی، فیبوناتچی [۴] در یکی از کتاب‌های خود، بدون ارائه‌ی هیچ اثباتی، ادعا کرده بود که عدد ۱، عددی همنهشت نیست. در اوایل قرن شانزدهم میلادی، فرما [۵] این ادعا را ثابت کرد. وی همچنین نشان داد که ۲ و ۳ نیز اعداد همنهشت نیستند. اویلر [۶] برای اولین بار، مثلثی را پیدا کرد که نشان می‌داد عدد ۷، عددی همنهشت می‌باشد. برای مطالعه‌ی بیشتر درباره‌ی تاریخچه‌ی این مسأله به [۳] مراجعه کنید.

مسأله‌ی اعداد همنهشت قابل تعمیم به مسأله‌ی اعداد θ−همنهشت می‌باشد. فرض می‌کنیم $\frac{\pi}{3} \leq \theta < \pi$ یک زاویه باشد. عدد صحیح مثبت n را یک عدد θ−همنهشت می‌گوییم هرگاه برابر با مساحت مثلثی با اضلاع گویا باشد که بزرگترین زاویه‌ی آن θ است. برای دیدن تعمیم‌های دیگر از مسأله‌ی اعداد همنهشت به [۱۴] مراجعه کنید.

---

[۱] Pythagoras
[۲] Euclidos
[۳] nice
[۴] Fibonacci
[۵] Fermat
[۶] Euler

این پایان‌نامه بر اساس مرجع [۱۲]، در سه فصل تنظیم گردیده است. فصل اول آن در سه بخش، شامل تعاریف و قضایای مورد نیاز از خم‌های بیضوی می‌باشد که مطالب این فصل مختصر بوده و برای درک بهتر مطالب فصل‌های بعدی مورد نیاز می‌باشد.

در فصل دوم به مطالعه‌ی اعداد همنهشت می‌پردازیم و ارتباط بین خم‌های بیضوی و مسأله‌ی اعداد همنهشت را بیان می‌کنیم.

در فصل سوم که بحث اصلی این پایان‌نامه است، مسأله‌ی اعداد همنهشت را تعمیم می‌دهیم و برای اولین بار از مفهوم چگالی اعداد صحیح، در تعمیم اعداد همنهشت استفاده می‌کنیم.

فهرست مندرجات

فصل ۱

مفاهیم مقدماتی خم‌های بیضوی

در این فصل، مقدماتی از مباحث جبری و نظریه‌ی خم‌های بیضوی را ارائه می‌کنیم. این مطالب در فصل‌های بعدی مورد نیاز خواهند بود.

۱.۱ روابط وایرشتراس و خم‌های بیضوی

در این بخش مقدمه‌ای از نظریه‌ی خم‌های بیضوی را بیان می‌کنیم. K را میدانی دلخواه با بستار جبری $\bar{K}$ و مشخصه‌ی $\mathrm{char}(K)$ در نظر می‌گیریم.

تعریف ۱.۱.۱ مجموعه‌ی تمامی n−تایی‌های واقع در $\bar{K}$، یعنی مجموعه‌ی

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{(x_1, \cdots, x_n) : x_i \in \bar{K}\}$$

را n−فضای آفین[1] روی K می‌گوییم. همچنین مجموعه‌ی

$$\mathbb{A}^n(K) = \{(x_1, \cdots, x_n) : x_i \in K\}$$

را نقاط K−گویای[2] $\mathbb{A}^n$ می‌گوییم.

[1] affine n-space
[2] K-rational points

تعریف ۲.۱.۱ رابطه‌ی هم‌ارزی $\sim$ را روی $\mathbb{A}^{n+1}$ به صورت زیر تعریف می‌کنیم:

$(x_0,\cdots,x_n) \sim (y_0,\cdots,y_n)$ اگر و تنها اگر یک $\lambda \in \bar{K}^*$ وجود داشته باشد که برای هر $0 \leq i \leq n$، $y_i = \lambda x_i$. مجموعه‌ی $\{(\lambda x_0,\cdots,\lambda x_n) : \lambda \in \bar{K}^*\}$ را کلاس هم‌ارزی $(x_0,\cdots,x_n)$ گفته و با $[x_0 : \cdots : x_n]$ نمایش می‌دهیم. حال n—فضای تصویری[۳] (روی K) را به صورت زیر تعریف می‌کنیم:

$$\mathbb{P}^n = \mathbb{P}^n(\bar{K}) = \{[x_0 : \cdots : x_n] \mid x_i \in \bar{K},\ \exists\, i\ :\ x_i \neq 0\}.$$

هرگاه $[x_0 : \cdots : x_n] \in \mathbb{P}^n$، آنگاه x_0، $\cdots$، x_n را مختصات همگن[۴] متناظر با $[x_0 : \cdots : x_n]$ می‌گوییم. همچنین مجموعه‌ی $\mathbb{P}^n(K) = \{[x_0 : \cdots : x_n] \mid \forall\, i\ :\ x_i \in K\}$ را مجموعه‌ی نقاط K—گویای $\mathbb{P}^n$ می‌گوییم.

اگر $x_n = 0$ باشد، آنگاه نقاط $[x_0 : x_1 : x_2 : \cdots : 0]$ را نقاط در بی‌نهایت $\mathbb{P}^n(\bar{K})$ تعریف می‌کنیم. اگر $x_n \neq 0$ باشد، آنگاه نقاط $[x_0 : x_1 : x_2 : \cdots : x_n] = [\frac{x_0}{x_n} : \frac{x_1}{x_n} : \frac{x_2}{x_n} : \cdots : 1]$ را نقاط متناهی $\mathbb{P}^n(\bar{K})$ تعریف می‌کنیم.

تبصره ۳.۱.۱ می‌توانیم n—فضای آفین را به n—فضای تصویری بنشانیم:

$$\mathbb{A}^n(\bar{K}) \mapsto \mathbb{P}^n(\bar{K})$$
$$(x_1, x_2, \cdots, x_n) \mapsto [x_1 : x_2 : \cdots : x_n : 1]$$

در واقع نقاط متناهی n—فضای تصویری، متناظر با تمام نقاط n—فضای آفین خواهند بود.

تعریف ۴.۱.۱ یک چندجمله‌ای $f \in \bar{K}[X] = \bar{K}[X_0,\cdots,X_n]$ را همگن از درجه d می‌گوییم هرگاه به ازای هر $\lambda \in \bar{K}$، داشته باشیم:

$$f(\lambda X_0,\cdots,\lambda X_n) = \lambda^d f(X_0,\cdots,X_n).$$

[۳] projective n-spase

[۴] homogeneous coordinates

مثال ۵.۱.۱ چندجمله‌ای‌های $X^۲+۴XY+Y^۲,\ \ X^۲+۲XY,\ \ X^۲+Y^۲\in\bar{\mathbb{Q}}[X,Y]$ همگن از درجه دو هستند.

تبصره ۶.۱.۱ اگر F یک چندجمله‌ای همگن باشد و $(X_۱,Y_۱,Z_۱)\sim(X_۲,Y_۲,Z_۲)$، آنگاه

$F(X_۱,Y_۱,Z_۱)=\circ$ اگر و تنها اگر $F(X_۲,Y_۲,Z_۲)=\circ$.

اگر $F(X,Y,Z)$ یک چندجمله‌ای دلخواه باشد، آنگاه ممکن است $F(X,Y,Z)=\circ$، ولی $F(\lambda X,\lambda Y,\lambda Z)\neq\circ$. به‌عنوان مثال، $F(X,Y,Z)=X^۲+۲X-۳Z$ یک چندجمله‌ای دلخواه می‌باشد که $F(۱,۱,۱)=\circ$، ولی $F(۲,۲,۲)\neq\circ$. بنابراین نتیجه می‌گیریم که در فضاهای تصویری باید با چندجمله‌ای‌های همگن کار کنیم. در غیر این صورت در ریشه‌های آن دچار سردرگمی می‌شویم.

یک چندجمله‌ای غیرهمگن را می‌توان به یک چندجمله‌ای همگن تبدیل کرد. این عمل را همگن‌سازی[۵] می‌نامیم. بنابراین اگر $f(X_۱,X_۲,\cdots,X_{n-۱})$ یک چندجمله‌ای غیرهمگن از درجه‌ی m در $\mathbb{A}^n(\bar{K})$ باشد و بخواهیم در $\mathbb{P}^n(\bar{K})$ همگن‌سازی کنیم به صورت زیر عمل می‌کنیم:

$$F(X_۱,X_۲,\cdots,X_n)=X_n^m f(\frac{X_۱}{X_n},\frac{X_۲}{X_n},\cdots,\frac{X_{n-۱}}{X_n})\in\mathbb{P}^n(\bar{K})$$

مثال ۷.۱.۱ چندجمله‌ای غیرهمگن $f(X,Y)=Y^۲-X^۳-aX-b$ را با عمل همگن‌سازی به چندجمله‌ای همگن $F(X,Y,Z)=Y^۲Z-X^۳-aZ^۲X-bZ^۳$ تبدیل می‌شود.

تعریف ۸.۱.۱ یک خم مسطح جبری تصویری[۶] روی K، مجموعه‌ی ریشه‌های چندجمله‌ای همگن غیرثابت $F(X,Y,Z)\in K[X,Y,Z]$ در $\bar{K}$ است:

$$C=C(F)=\left\{[x:y:z]\in\mathbb{P}^۲\mid F(x,y,z)=\circ\right\}.$$

[۵] homogenizing
[۶] plane projective algebraic curve

مجموعه نقاط K−گویای C را به صورت زیر تعریف می‌کنیم:

$$C(K) = C(F)(K) = \left\{[x:y:z] \in \mathbb{P}^{۲}(K) \mid F(x,y,z) = ۰\right\}.$$

نقطه در بی‌نهایت این خم، $P = [x:y:z] \in C$ است که در آن $z = ۰$، زیرا اگر $P = [x:y:z] \in C$ نقطه‌ای با $z \neq ۰$ باشد، آنگاه $[x:y:z] = [\frac{x}{z}:\frac{y}{z}:۱]$. اگر $z = ۰$، آنگاه هر دو مختص x و y برابر ∞ می‌شوند.

تعریف ۹.۱.۱ یک خم مسطح جبری آفین [۷] روی K، مجموعه‌ی ریشه‌های چندجمله‌ای همگن غیرثابت $f(X,Y) \in K[X,Y]$ در $\bar{K}$ است:

$$C = C(f) = \left\{(x,y) \in \mathbb{A}^{۲} \mid f(x,y) = ۰\right\}.$$

مجموعه نقاط K−گویای C را به صورت زیر تعریف می‌کنیم:

$$C(K) = C(f)(K) = \left\{(x,y) \in \mathbb{A}^{۲}(K) \mid f(x,y) = ۰\right\}.$$

نقطه در بی‌نهایت این خم، $\mathcal{O} = (\infty,\infty)$ می‌باشد.

تعریف ۱۰.۱.۱ گونه‌ی[۸] یک خم مسطح هموار از درجه‌ی d (به بیان دقیق‌تر یک خم هموار که با یک معادله‌ی چندجمله‌ای همگن از درجه‌ی d، $F(X,Y,Z) \in \bar{K}[X,Y,Z]$ داده شده باشد.) به صورت زیر تعریف می‌شود:

$$g = \frac{۱}{۲}(d-۲)(d-۱).$$

[۷] plane affine algebraic curve

[۸] genuse

تعریف ۱۱.۱.۱ یک خم بیضوی[۹] زوج مرتب $(E, \mathcal{O})$ است که E یک منحنی هموار $(\Delta \neq 0)$ با گونه‌ی ۱ است و $\mathcal{O} \in E$.(اغلب فقط E را می‌نویسیم و از نوشتن $\mathcal{O}$ صرف‌نظر می‌کنیم.) $\mathcal{O}$ را نقطه در بی‌نهایت خم می‌گیریم به‌طوری که خطوط موازی با محور y ها همدیگر را در $\mathcal{O}$ قطع می‌کنند. به عبارت دیگر، هر خط گذرا از $\mathcal{O}$ موازی محور y ها است.

تعریف ۱۲.۱.۱ فرض می‌کنیم K یک میدان و E یک خم بیضوی باشد. در این صورت مجموعه‌ی $E(K)$ را به صورت زیر تعریف می‌کنیم:

$$E(K) = \{(x.y) \in E \mid x, y \in K\} \cup \{\mathcal{O}\}.$$

هرگاه E به عنوان یک منحنی روی میدان K تعریف شده باشد گوییم خم بیضوی E روی میدان K تعریف شده است و می‌نویسیم E/K.

تعریف ۱۳.۱.۱ فرض می‌کنیم K یک میدان بوده، $a_1, a_2, a_3, a_4, a_6 \in \bar{K}$ و خم E توسط معادله‌ی درجه سوم

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

تعریف شده باشد. خم E را به همراه نقطه در بی‌نهایت $\mathcal{O} = (\infty, \infty)$ در نظر می‌گیریم. تغییر متغیرهای $x = X/Z$ و $y = Y/Z$، خم E را به فرم تصویری و همگن

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

تبدیل می‌کند. نقطه‌ی $\mathcal{O} = (\infty, \infty)$ روی E با نقطه‌ی $[X : Y : 0]$ روی رابطه‌ی همگن بدست آمده متناظر است. بنابراین با قرار دادن $Z = 0$ در رابطه‌ی همگن نتیجه می‌شود $X^3 = 0$، پس

[۹] elliptic curve

$X = 0$. چون $[0 : 0 : 0] \notin \mathbb{P}^2(\bar{K})$، در نتیجه $\mathcal{O} = [0 : 1 : 0]$ تنها نقطه‌ی متناظر با نقطه‌ی $\mathcal{O} = (\infty, \infty)$ است. یعنی تنها نقطه در بی‌نهایت روی C نقطه‌ی $\mathcal{O} = [0 : 1 : 0]$ می‌باشد. معمولاً به خم جبری (تصویری) C و یا به‌طور معادل به خم جبری (آفینی) E، معادله‌ی تعمیم یافته‌ی وایرشتراس[10] گفته می‌شود.

فرض می‌کنیم خم جبری E، توسط رابطه‌ی (۱.۱) تعریف شده باشد. پروفسور جان. تیت[11] کمیت‌های b_2، b_4، b_6، b_8، c_4، c_6، Δ، j و ω را برای این خم به صورت زیر معرفی کرده است:

$$b_2 = a_1^2 + 4a_2 \qquad c_4 = b_2^2 - 24b_4$$

$$b_4 = a_1a_3 + 2a_4 \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

$$b_6 = a_3^2 + 4a_6 \qquad \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

$$b_8 = b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \qquad j = \frac{c_4^3}{\Delta}$$

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$

که در آن به Δ، j و ω به ترتیب مبین[12]، j–پایا[13] و دیفرانسیل نرون[14] خم جبری E گفته می‌شود. به‌راحتی می‌توان دید که این کمیت‌ها در روابط زیر صدق می‌کنند:

$$4b_8 = b_2b_6 - b_4^2, \; 1728\Delta = c_4^3 - c_6^2.$$

تغییر متغیرهای $x = u^2x' + r$ و $y = u^3y' + u^2sx' + t$، به‌طوری که $u, r, s, t \in \bar{K}$ و $u \neq 0$، خم بیضوی

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

[10] generalized Weierstrass equation

[11] John T.Tate

[12] discriminant

[13] j-invariant

[14] Neron differentioal

را به خم بیضوی

$$E' : (y')^{2} + a'_{1}(x')(y') + a'_{3}(y') = (x')^{3} + a'_{2}(x')^{2} + a'_{4}(x') + a'_{6},$$

تبدیل می‌کنند. تغییر متغیرها در جهت عکس برای تبدیل خم E' به E به صورت زیر هستند:

$$x' = \frac{1}{u^{2}}(x - r),\ y' = \frac{1}{u^{3}}(y - sx + sr - t).$$

چنین تغییر متغیرهایی را دوگویا[15] می‌نامیم. بنابراین داریم:

$$ua'_{1} = a_{1} + 2s,$$

$$u^{2}a'_{2} = a_{2} - sa_{1} + 3r - s^{2},$$

$$u^{3}a'_{3} = a_{3} + ra_{1} + 2t,$$

$$u^{4}a'_{4} = a_{4} - sa_{3} + 2ra_{2} - (t + rs)a_{1} + 3r^{2} - 2st,$$

$$u^{6}a'_{6} = a_{6} + ra_{4} + r^{2}a_{2} + r^{3} - ta_{3} - rta_{1} - t^{2},$$

$$u^{2}b'_{2} = b_{2} + 12r,$$

$$u^{4}b'_{4} = b_{4} + rb_{2} + 6r^{2},$$

$$u^{6}b'_{6} = b_{6} + 2rb_{4} + r^{2}b_{2} + 4r^{3},$$

$$u^{8}b'_{8} = b_{8} + 3rb_{6} + 3r^{2}b_{4} + r^{3}b_{2} + 3r^{4},$$

$$u^{4}c'_{4} = c_{4},$$

$$u^{6}c'_{6} = c_{6},$$

[15] birational

$u^{12}\Delta' = \Delta,$

$j' = j,$

$u^{-1}\omega' = \omega.$

تعریف ۱۴.۱.۱ دو معادله به فرم رابطه‌ی تعمیم یافته‌ی وایرشتراس را یکریخت می‌گوییم هرگاه چنین تغییر متغیرهای دوگویایی بین آن‌ها وجود داشته باشد.

قضیه ۱۵.۱.۱ فرض می‌کنیم E/K یک خم جبری به صورت رابطه‌ی تعمیم یافته‌ی وایرشتراس باشد. تحت فرض‌های ذکر شده در هر قسمت، عناصر $r, s, t \in \bar{K}$ و $u \in \bar{K}^*$ وجود دارند به‌طوری که تغییر متغیرهای

$$x = u^2x' + r,\ y = u^3y' + u^2sx' + t,$$

نقطه‌ی $\mathcal{O} = (\infty, \infty)$ را ثابت نگه داشته و خم E را به خم E' ذکر شده تبدیل می‌کنند که کمیت‌های موجود مطابق بحث بالا می‌باشند.

(۱) هرگاه $\mathrm{char}(K) \neq 2, 3$، آنگاه

$$E' : y'^2 = x'^3 + a'_4x' + a'_6,\ \Delta' = -16(4a'^3_4 + 27a'^2_6),\ j' = 1728\frac{4a'^3_4}{4a'^3_4 + 27a'^2_6};$$

(۲) هرگاه $\mathrm{char}(K) = 3$ و $j \neq 0$، آنگاه

$$E' : y'^2 = x'^3 + a'_2x'^2 + a'_6,\ \Delta' = -a'^3_2a'_6,\ j' = -\frac{a'^3_2}{a'_6};$$

(۳) هرگاه $\mathrm{char}(K) = 3$ و $j = 0$، آنگاه

$$E' : y'^2 = x'^3 + a'_4x' + a'_6,\ \Delta' = -a'^3_4,\ j' = 0;$$

(۴) هرگاه $\mathrm{char}(K)=2$ و $j\neq 0$، آنگاه

$$E' : y'^2 + a'_1x'y' = x'^3 + a'_2x'^2 + a'_6,\ \Delta' = a'_6,\ j' = \frac{1}{a'_6};$$

(۵) هرگاه $\mathrm{char}(K)=2$ و $j=0$، آنگاه

$$E' : y'^2 + a'_3y' = x'^3 + a'_4x' + a'_6,\ \Delta' = a'^3_4,\ j' = 0.$$

همچنین هرگاه E روی K تعریف شده باشد، آنگاه $r,s,t\in K$ و $u\in K^*$.

اثبات: به [[۱۳]، ضمیمه‌ی A، گزاره‌ی ۱.۱] مراجعه شود. □

تعریف **۱۶.۱.۱** فرض می‌کنیم خم بیضوی E روی میدان K تعریف شده باشد. تاب[۱۶] خم بیضوی E، خم بیضوی E' است که با خم E روی $\bar{K}$ یکریخت است. به عبارت دیگر دو خم بیضوی که دارای j–پایاهای یکسان باشند را تاب یکدیگر گویند.

توجه می‌کنیم که یکریختی خم‌های بیضوی را روی میدان‌های به‌طور جبری بسته‌ی K بررسی می‌کنیم. چون اگر K به‌طور جبری بسته نباشد ممکن است j–پایاهای دو خم برابر بوده ولی دو خم یکریخت نباشند. به‌عنوان مثال، دو خم بیضوی $E_1 : y^2 = x^3 - 25x$ و $E_2 : y^2 = x^3 - 4x$ را روی $\mathbb{Q}$ در نظر می‌گیریم. j–پایای هر دو خم برابر ۱۷۲۸ می‌باشد در حالی که خم $E_1 : y^2 = x^3 - 25x$ دارای بی‌نهایت مختصات در $\mathbb{Q}$ می‌باشد ولی خم E_2 دارای تعداد نقاط محدود $(0,0)$، $(-2,0)$، $(2,0)$ و $\mathcal{O}$ می‌باشد. بنابراین $E_1(\mathbb{Q})\ncong E_2(\mathbb{Q})$.

تعریف **۱۷.۱.۱** فرض می‌کنیم خم بیضوی

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

[۱۶] twist

روی میدان K تعریف شده باشد. در این صورت تاب مربعی[۱۷] روی خم بیضوی E توسط d ($d \in K/K^{۲}$ و $d \neq ۰$) را به صورت زیر تعریف می‌کنیم:

$$E_d \ : \ dy^{۲} = x^{۳} + a_{۲}x^{۲} + a_{۴}x + a_{۶}.$$

تبصره ۱۸.۱.۱ دو خم بیضوی

$$E_d : dy^{۲} = x^{۳} + a_{۲}x^{۲} + a_{۴}x + a_{۶} \ , \ E'_d : y^{۲} = x^{۳} + a_{۲}x^{۲}d + a_{۴}xd^{۲} + a_{۶}d^{۳}$$

تحت نگاشت $(x, y) \to (\frac{x}{d}, \frac{y}{d^{۲}})$ یکریخت هستند. بنابراین تاب مربعی خم بیضوی E توسط d را می‌توان به صورت $E_d : y^{۲} = x^{۳} + a_{۲}x^{۲}d + a_{۴}xd^{۲} + a_{۶}d^{۳}$ نیز تعریف کرد.

تبصره ۱۹.۱.۱ فرض می‌کنیم E/K یک خم جبری باشد و $\mathrm{char}(K) \neq ۲, ۳$. طبق قضیه‌ی ۱۵.۱.۱ خم E را توسط رابطه‌ی

$$E : y^{۲} = x^{۳} + ax + b \ \ (a, b \in K), \tag{۲.۱}$$

به همراه نقطه در بی‌نهایت $\mathcal{O} = (\infty, \infty)$ در نظر می‌گیریم. در این حالت می‌گوییم خم نمایشی به فرم وایرشتراس کوتاه[۱۸] دارد، که در حالت اخیر مقدارهای Δ و j مربوطه به صورت زیر هستند:

$$\Delta = -۱۶(۴a^{۳} + ۲۷b^{۲}), \ j = -۱۷۲۸\frac{(۴a)^{۳}}{\Delta}.$$

تعریف ۲۰.۱.۱ فرض می‌کنیم خم جبری E با معادله‌ی $f(x, y) = ۰$ تعریف شده باشد. نقطه‌ی $P = (x_{۰}, y_{۰}) \in E$ یک نقطه‌ی منفرد[۱۹] است اگر و تنها اگر

$$\frac{\partial f}{\partial x}(x_{۰}, y_{۰}) = ۰, \ \frac{\partial f}{\partial y}(x_{۰}, y_{۰}) = ۰.$$

[۱۷] quadratic twist
[۱۸] short weierstrass form
[۱۹] singular point

یک خم را منفرد گوییم هرگاه در تمام نقاط خودش منفرد باشد.

فرض می‌کنیم $P=(x_0,y_0)$ یک نقطه‌ی منفرد روی خم جبری E باشد که توسط رابطه‌ی (۱.۱) تعریف شده است. تابع $f(x,y)$ را به صورت زیر در نظر می‌گیریم:

$$f(x,y)=y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6,$$

در این صورت از تعریف ۲۰.۱.۱ نتیجه می‌شود:

$$\frac{\partial f}{\partial x}(P)=a_1y_0-3x_0^2-2a_2x_0-a_4=0,$$

$$\frac{\partial f}{\partial y}(P)=2y_0+a_1x_0+a_3=0.$$

مشتقات جزئی دیگر تابع $f(x,y)$ به صورت زیر قابل محاسبه هستند:

$$\frac{\partial^2 f}{\partial y^2}(P)=2,\ \frac{\partial^2 f}{\partial x^2}(P)=-2(3x_0+a_2),$$

$$\frac{\partial^2 f}{\partial x\partial y}(P)=a_1=\frac{\partial^2 f}{\partial y\partial x}(P),$$

$$\frac{\partial^3 f}{\partial x^3}(P)=-6,\ \frac{\partial^3 f}{\partial y^3}(P)=0.$$

حال سری تیلور تابع $f(x,y)$ در نقطه‌ی P را می‌توان به صورت زیر نوشت:

$$\begin{aligned}f(x,y)=&f(x_0,y_0)+\left\{(x-x_0)\frac{\partial f}{\partial x}(P)+(y-y_0)\frac{\partial f}{\partial y}(P)\right\}\\&+\frac{1}{2!}\left\{(x-x_0)^2\frac{\partial^2 f}{\partial x^2}(P)+2(x-x_0)(y-y_0)\frac{\partial^2 f}{\partial y\partial x}(P)+(y-y_0)^2\frac{\partial^2 f}{\partial y^2}(P)\right\}\end{aligned}$$

$$+\frac{1}{3!}\Big\{(x-x_0)^3\frac{\partial^3 f}{\partial x^3}(P)+3(x-x_0)^2(y-y_0)\frac{\partial^3 f}{\partial x^2\partial y}(P)$$
$$+3(x-x_0)(y-y_0)^2\frac{\partial^3 f}{\partial x\partial y^2}(P)+(y-y_0)^3\frac{\partial^3 f}{\partial y^3}(P)\Big\}+\cdots$$

حال با جایگذاری مقادیر مشتقات جزئی و ساده کردن جملات نتیجه می‌شود:

$$f(x,y)-f(x_0,y_0)=[(y-y_0)-\alpha(x-x_0)][(y-y_0)-\beta(x-x_0)]-(x-x_0)^3, \quad (3.1)$$

که در آن α و β در $\bar{K}$ قرار داشته و به صورت زیر می‌باشند:

$$\alpha=\frac{-a_1+\sqrt{a_1^2-4(3x_0+a_2)}}{2},\ \beta=\frac{-a_1-\sqrt{a_1^2-4(3x_0+a_2)}}{2}.$$

تعریف ۲۱.۱.۱ با در نظر گرفتن نمادهای بالا، نقطه‌ی منفرد P را یک گره[20] برای خم جبری E می‌گوییم هرگاه $\alpha\neq\beta$، که در این صورت خطوط مماس بر خم به صورت زیر هستند:

$$y-y_0=\alpha(x-x_0),\ y-y_0=\beta(x-x_0).$$

به‌طور مشابه، نقطه‌ی منفرد P را یک نقطه‌ی بازگشت [21] برای خم E می‌گوییم هرگاه $\alpha=\beta$، که در این صورت تنها خط مماس بر خم به صورت $y-y_0=\alpha(x-x_0)$ است.

گزاره ۲۲.۱.۱ هر خم جبری تعریف شده توسط رابطه‌ی تعمیم یافته‌ی وایرشتراس را می‌توان به صورت زیر دسته‌بندی کرد:

(۱) E نامنفرد است اگر و تنها اگر $\Delta\neq 0$؛

(۲) E دارای گره است اگر و تنها اگر $\Delta=0$، $c_4\neq 0$؛

(۳) E دارای نقطه‌ی بازگشت است اگر و تنها اگر $\Delta=c_4=0$.

در حالت‌های (۲) و (۳) تنها یک نقطه‌ی منفرد وجود دارد.

اثبات: به [[۱۳]، فصل III، گزاره‌ی ۴.۱] مراجعه شود. □

[20] node
[21] cusp