بسم الله الرحمن الرحیم

خم های بیضوی

بر اساس کتاب:

ELLIPTIC CURVES

NUMBER THEORY

AND CRYPTOGRAPHY

(LAWRENCE C. WASHINGTON)

تهیه کننده: سِیّد مُحَمّد آذربرا

استاد: دکتر علی سرباز جانفدا

دانشگاه ارومیه

سال تحصیلی ۹۰-۸۹

فهرست مطالب

عنوان	صفحه
فصل اول:	
مقدمات	٤
فصل دوم: نظریه اساسی	
معادلات وایرشتراس	٨
قوانین گروهی	٩
فضاهای تصویری و نقطه در بینهایت	١٥
دستگاه های مختصات دیگر (تصویری، ژاکوبین، ادواردز)	١٧
Jـ پایا	٢٠
خم های بیضوی در مشخصه ٢	٢٣
درونریختی	٢٥
خم های منفرد	٣٤
تمرینات فصل دوم	٣٩

فصل سوم: نقاط تاب

نقاط تاب ٤٥

چندجمله ای های تقسیم ٥١

جفت سازی **Weil** ٥٣

جفت سازی **Tate – lichtenbaum** ٥٦

فصل چهارم: خم های بیضوی روی میدان های متناهی

خم های بیضوی روی میدان های متناهی ٥٧

درونریختی های فروبینوس ٦١

تعیین مرتبه خم های بیضوی ٦٧

گام کوچک، گام بزرگ **Baby step, Giant step** ٧٥

خانواده منحنی ها ٧٨

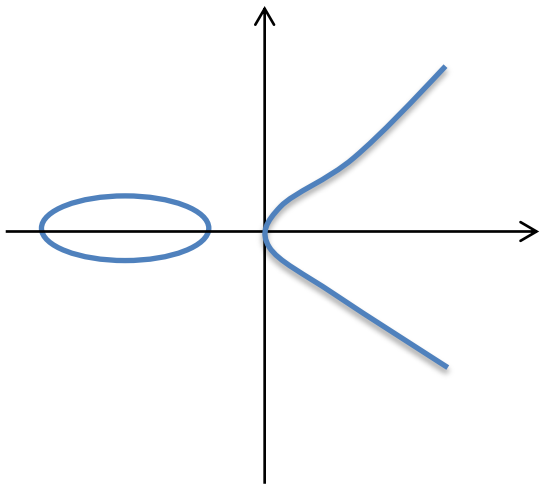
خم های فوق منفرد ٧٩

فصل هشتم: خم های بیضوی روی $\mathbb{Q}$ ٨٦

مقدمات

تعریف:

یک خم بیضوی در حالت کلی دارای معادله $y^۲ = \frac{x(x+۱)(۲x+۱)}{۶}$ می باشد که در آن x و y اعداد صحیح مثبت هستند و نموداری به شکل زیر دارد که نسبت به محور x متقارن است



روش حل این گونه مسائل:

برای حل این معادله از روش دیوفانت برای پیدا کردن یک عدد صحیح مثبت برای y استفاده می کنیم

برای این منظور از دو نقطه $(۰,۰)$ و $(۱,۱)$ که در معادله صدق می کنند شروع می کنیم. خط گذرا از این دو نقطه $y = x$ می باشد که با جایگذاری در معادله اصلی خواهیم داشت

$$y^۲ = \frac{x(x+۱)(۲x+۱)}{۶} \Longrightarrow x^۲ - \frac{۳}{۲}x^۲ + \frac{۱}{۲}x = ۰$$

بوضوح دو ریشه این معادله $x = ۰$ و $x = ۱$ می باشند ریشه سوم را با استفاده از نکته کلیدی زیر پیدا می کنیم.

*نکته: برای اعداد دلخواه a, b, c داریم

$$(x-a)(x-b)(x-c) = x^۳ - (a+b+c)x^۲ + (ab+ac+bc)x - abc$$

بنابراین زمانی که در یک معادله درجه ۳ ضریب $x^{۳}$ برابر ۱ باشد آنگاه مجموع سه ریشه برابر با منفی ضریب $x^{۲}$ است❋

لذا برای معادله بالا داریم $x = \frac{۳}{۲} + ۱ + ۰$ پس $x = \frac{۱}{۲}$ ریشه سوم چند جمله ای فوق است که با توجه به $y = x$ خواهیم داشت $y = \frac{۱}{۲}$ که مطلوب مسئله نیست زیرا ما به دنبال عدد صحیح بودیم

بنابر تقارن نمودار $(\frac{۱}{۲}, -\frac{۱}{۲})$ نیز روی نمودار قرار دارد حال دو نقطه $(\frac{۱}{۲}, -\frac{۱}{۲})$ و $(۱,۱)$ را در نظر می گیریم خط گذرا از این دو نقطه برابر $y = ۳x - ۲$ می باشد. (توجه داریم که اگر نقاط $(\frac{۱}{۲}, -\frac{۱}{۲})$ و $(۰,۰)$ را در نظر بگیریم خط گذرا از این دو نقطه برابر $y = -x$ می باشد که همان نتیجه قبلی را می دهد)

با جایگذاری خواهیم داشت $(۳x - ۲)^{۲} = \frac{x(x+۱)(۲x+۱)}{۶} \Longrightarrow x^{۲} - \frac{۵۱}{۲}x^{۲} + \cdots = ۰$ (طبق نکته فوق فقط تا توان دوم نیاز خواهیم داشت)

با در دست داشتن دو ریشه $\frac{۱}{۲}$ و ۱ خواهیم داشت $x = ۲۴ \xrightarrow{y=۳x-۲} y = ۷۰$ پس $\frac{۱}{۲} + ۱ + x = \frac{۵۱}{۲}$ توانستیم y را محاسبه کنیم لذا خواهیم داشت

$$۱^{۲} + ۲^{۲} + \cdots + ۲۴^{۲} = ۷۰^{۲}$$

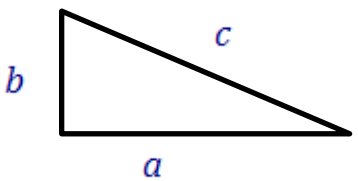
و یا به عبارت دیگر با ۴۹۰۰ توپ می توانیم هرمی با ۲۴ سطر طوری بسازیم که در سطر بالا یک توپ در سطر دوم ۴ توپ در سطر سوم ۹ توپ و به همین ترتیب در سطر ۲۴ ام $۲۴^{۲}$ توپ موجود باشد (یعنی در سطر i ام $i^{۲}$ توپ باشد.)

مثال

می خواهیم مثلثی قائم با اضلاع گویا طوری پیدا کنیم که مساحت آن یک عدد صحیح باشد مانند مثلثی با اضلاع $(۳,۴,۵)$ که دارای مساحت ۶ است و یا $(۸,۱۵,۱۷)$ که دارای مساحت ۶۰ است.

اگر اضلاع مثلث بالا را بر دو تقسیم کنیم مثلث $(۴, \frac{۱۵}{۲}, \frac{۱۷}{۲})$ را با مساحت ۱۵ خواهیم داشت پس ممکن است اضلاع مثلث صحیح نباشند ولی مساحت عددی صحیح باشد. لذا هدف ما یافتن نقاطی با این شرط است که مساحت مثلث عددی صحیح باشد.

مثلث قائم الزاویه زیر را با اضلاع a, b, c در نظر می گیریم



می خواهیم اضلاع مثلث را طوری بیابیم که مساحت آن ۵ شود

لذا با استفاده از فرمول مساحت و قضیه فیثاغورث دو رابطه زیر را خواهیم داشت

$ab = ۱۰$ و $a^۲ + b^۲ = c^۲$ طبق این روابط می توان نوشت

$$\left(\frac{a+b}{۲}\right)^۲ = \frac{a^۲ + ۲ab + b^۲}{۴} = \frac{c^۲ + ۲۰}{۴} = \left(\frac{c}{۲}\right)^۲ + ۵$$

$$\left(\frac{a-b}{۲}\right)^۲ = \frac{a^۲ - ۲ab + b^۲}{۴} = \frac{c^۲ - ۲۰}{۴} = \left(\frac{c}{۲}\right)^۲ - ۵$$

فرض کنید $x = \left(\frac{c}{۲}\right)^۲$ آنگاه خواهیم داشت

$$x + ۵ = \left(\frac{a+b}{۲}\right)^۲ \;\&\; x - ۵ = \left(\frac{a-b}{۲}\right)^۲$$

مسئله تبدیل شد به یافتن عدد گویای x که همزمان x و $x - ۵$ و $x + ۵$ مربع اعدادی گویا باشند و یا به عبارت دیگر دنبال یافتن سه مربع از اعداد گویا صادق در تصاعد حسابی بالا با قدر نسبت ۵ هستیم.

فرض کنیم x را داریم در این صورت حاصلضرب $x(x-۵)(x+۵) = x^۳ - ۲۵x$ باید مربع کامل باشد لذا بدنبال جواب گویایی برای معادله $y^۲ = x^۳ - ۲۵x$ هستیم

همانند بالا این معادله یک خم بیضوی است داریم: $x = \left(\frac{c}{۲}\right)^۲$ و

$$y = ((x+۵)(x)(x-۵))^{\frac{۱}{۲}} = \frac{(a-b)(c)(a+b)}{۸} = \frac{(a^۲ - b^۲)c}{۸}$$

سه نقطه $(۰,۰), (۵,۰), (-۵,۰)$ بوضوح روی خم قرار دارند که کمکی به ما نمی کنند زیرا هیچ مثلث یا خطی میان دو نقطه از منحنی و نقاط باقیمانده نمی دهد با کمی جایگذاری نقطه $(-۴,۶)$ بدست می آید، خطوط گذرا از این نقطه و سه نقطه فوق چیز خاصی به ما نمی دهد.

تنها احتمال باقیمانده خط گذرا از نقطه $(-۴,۶)$ و خودش است که خط مماس بر منحنی در نقطه $(-۴,۶)$ نامیده می شود.

با مشتق گیری ضمنی خواهیم داشت

$$۲yy' = ۳x^۲ - ۲۵ \implies y' = \frac{۳x^۲ - ۲۵}{۲y} = \frac{۲۳}{۱۲}$$

لذا خط مماس برابر $y = \frac{۲۳}{۱۲}x + \frac{۴۱}{۳}$ است که اگر با معادله خم قطع دهیم خواهیم داشت

$$(y = \frac{۲۳}{۱۲}x + \frac{۴۱}{۳})^۲ = x^۳ - ۲۵x \implies x^۳ - \left(\frac{۲۳}{۱۲}\right)^۲ x^۲ + \cdots = ۰$$

چون خط در $(-۴,۶)$ بر خم عمود است پس $x = -۴$ ریشه مضاعف است لذا

$$-۴ - ۴ + x = \left(\frac{۲۳}{۱۲}\right)^۲ \implies x = \frac{۱۶۸۱}{۱۴۴} = \left(\frac{۴۱}{۱۲}\right)^۲ \implies y = \frac{۶۲۲۷۹}{۱۷۲۸}$$

$$\xrightarrow{x=\left(\frac{c}{۲}\right)^۲} c = \frac{۴۱}{۶} \implies \frac{۶۲۲۷۹}{۱۷۲۸} = y = \frac{(a^۲ - b^۲)c}{۸} = \frac{۴۱(a^۲ - b^۲)}{۴۸}$$

$$a^۲ - b^۲ = \frac{۱۵۱۹}{۳۶} = c^۲ \implies a^۲ = \frac{۴۰۰}{۹} \ \& \ b^۲ = \frac{۹}{۴}$$

لذا $c = \frac{۴۱}{۶}\ , b = \frac{۳}{۲}\ , a = \frac{۲۰}{۳}$ و مثلث دارای مساحت ۵ است.

نکته:

حالت کلی مثال بالا پیدا کردن اضلاع گویای مثلث قائم الزاویه بطوریکه مساحت آن برابر عدد صحیح n شود، است که به مسئله اعداد همنهشت مشهور است.

یادآوری:

عدد صحیح n را آزاد از مربع می نامیم هرگاه n بصورت حاصلضرب اعداد مربع کامل غیر از ۱ نباشد مانند ۵ و ۱۵ (یعنی در تجزیه آن عدد مربع کامل دیده نشود)

فصل دوم: نظریه اساسی

معادلات وایرشتراس

معادله وایرشتراس:

خم بیضوی E نمودار معادله ای به فرم $y^2 = x^3 + Ax + B$ است که در آن A و B ثابت هستند این معادله را معادله وایرشتراس خم بیضوی می نامیم.

در این معادله A و B و x و y عناصر یک میدان هستند که این میدان برای مثال می تواند میدان اعداد حقیقی $\mathbb{R}$، میدان اعداد گویا $\mathbb{Q}$، میدان اعداد مختلط $\mathbb{C}$، یکی از میدان های متناهی $\mathbb{F}_p(=\mathbb{Z}_p)$ برای عدد اول p است و یا یکی از میدان های متناهی $\mathbb{F}_q$ است که در آن $q = p^k$ برای $k \geq 1$ می باشد.

تعریف:

اگر K یک میدان باشد و $A, B \in K$ و E یک خم بیضوی به فرم فوق باشد می گوییم E روی میدان K تعریف شده است.

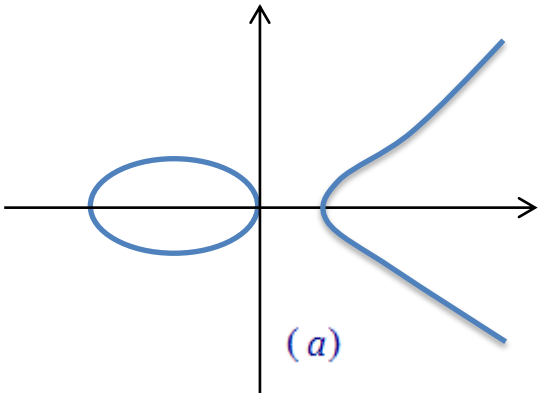
$E(L)$ را نقاطی با مختصات واقع در میدان $L \supseteq K$ در نظر می گیریم که L توسیع K می باشد طبق تعریف $E(L)$ همواره شامل نقطه ∞ است. لذا داریم

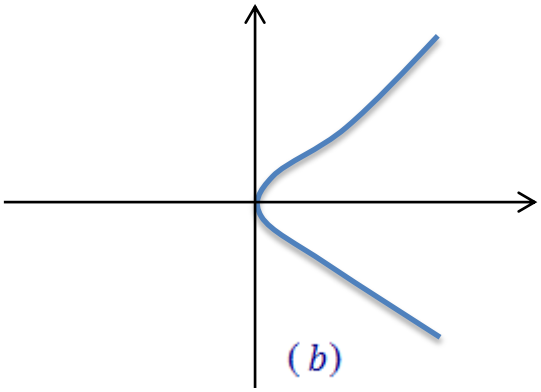
$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L | y^2 = x^3 + Ax + B\}$$

نکته:

امکان رسم نمودار با معنی در بسیاری از میدان ها وجود ندارد.

هرچند برای تصور می توان نمودار هایی رسم کرد برای مثال نمودار مکعب $y^2 = x^3 - x$ را در دو حالت رسم می کنیم: در حالت اول معادله دارای سه ریشه حقیقی مجزا و در حالت دوم معادله دارای یک ریشه حقیقی است.





تعریف:

گاهی معادله $y^2 = x^3 + Ax + B$ را به فرم $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ می نویسیم که $a_1, \dots, a_6$ اعداد ثابتی هستند.

این فرم را معادله وایرشتراس تعمیم یافته می نامیم.

فرم وایرشتراس تعمیم یافته زمانی مفید خواهند بود که با میدان هایی با مشخصه ۲ یا ۳ کار می کنیم در صورتی که مشخصه میدان ۲ نباشد آنگاه با تقسیم معادله بر ۲ و مرفع کامل کردن خواهیم داشت

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

$$\Longrightarrow y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

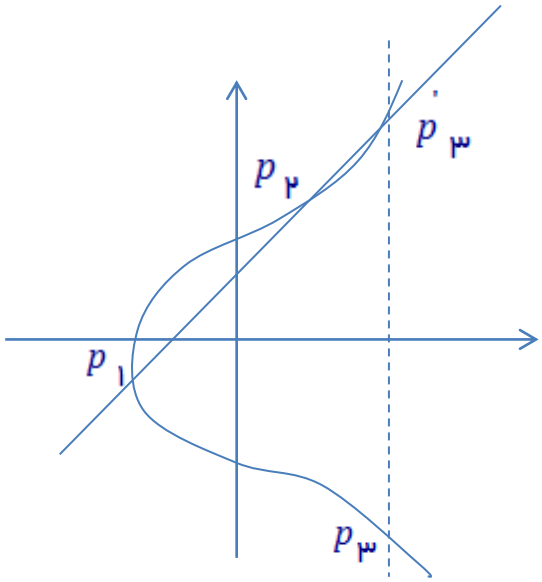
اگر مشخصه میدان ۳ باشد می توان فرض کرد $x_1 = x + \frac{a_2'}{3}$ و مشاهده کرد که برای ثابت های A و B

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

برای نتایج بعدی نقطه در بینهایت را به خم بیضوی اضافه می کنیم و برای راحتی (∞, ∞) را با ∞ نشان می دهیم همچنین ∞ در بالای محور y را با ∞ در پایین محور y یکسان می گیریم و با ∞ نشان می دهیم.

قوانین گروهی

در بخش یک با دو و یا حتی یک نقطه شروع کردیم و نقاط دیگر خم E را یافتیم در این بخش این روش را با جزئیات بیشتری بررسی می کنیم.



با دو نقطه $P_۱ = (x_۱, y_۱)$ و $P_۲ = (x_۲, y_۲)$ روی خم بیضوی E با معادله $y^۲ = x^۳ + Ax + B$ شروع می کنیم. نقطه جدید $P_۳$ را به صورت زیر تعریف می کنیم:

خط L را بین $P_۱$ و $P_۲$ رسم می کنیم که E را در نقطه سوم $P_۳'$ قطع می کند، وارون $P_۳'$ نسبت به محور x را $P_۳$ تعریف می کنیم.

تعریف می کنیم $P_۱ + P_۲ = P_۳$ مثال زیر نشان میدهد که این همان جمع مولفه به مولفه نیست در جایی که ابهام وجود دارد جمع فوق را بصورت زیر نشان می دهیم $P_۱ +_E P_۲ = P_۳$

خواص جمع این گروه

ابتدا فرض کنیم $P_۱ \neq P_۲$ و هیچکدام ∞ نباشند. خط L بین $P_۱$ و $P_۲$ دارای شیب $m = \frac{y_۲ - y_۱}{x_۲ - x_۱}$ می باشد اگر $x_۱ = x_۲$ آنگاه L عمود است که این مورد بعد از مورد زیر بحث خواهد شد.

پس فرض کنیم $x_۱ \neq x_۲$ که در این صورت معادله L بصورت $y = m(x - x_۱) + y_۱$ می باشد اگر نقاط تقاطع این خط را با خم بدست آوریم خواهیم داشت:

$$(m(x - x_۱) + y_۱)^۲ = x^۳ + Ax + B \implies ۰ = x^۳ - m^۲x^۲ + \cdots$$

سه ریشه این معادله نقاط تلاقی E و L است. در واقع پیدا کردن ریشه های یک مکعب راحت نیست ولی در این مسئله دو ریشه x_1, x_2 را می شناسیم زیرا P_1 و P_2 نقاطی هستند که به E و L تعلق دارند. پس طبق روالی که داریم می توان ریشه سوم را نیز بدست آورد. پس خواهیم داشت $y = m(x - x_1) + y_1$ و

$x = m^2 - x_1 - x_2$ قرینه نسبت به محور x ها نقطه P_3 را میدهد که $P_3 = (x_3, y_3)$ پس در این حالت خواهیم داشت:

$$\begin{cases} x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases}$$

اگر $x_1 = x_2$ و $y_1 \neq y_2$ آنگاه L عمود است لذا تقاطع آن با E نقطه ∞ است که قرینه اش نسبت به محور x ها برابر همان ∞ خواهد شد. پس در این حالت $P_1 + P_2 = \infty$

حالت $P_1 = P_2 = (x_1, y_1)$ را بررسی می کنیم چون در این حال هر دو نقطه در خط مماس واقعند شیب خط را با مشتق گیری ضمنی بدست می آوریم:

$$2y\frac{dy}{dx} = 3x^2 + A \implies m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

اگر $y_1 = 0$ خط عمود است و داریم $P_1 + P_2 = \infty$ که قبلا بررسی شد. (نکته اساسی طبق تمرین ۲.۵ این است که اگر $y_1 = 0$ آنگاه $3x^2 + A \neq 0$)

فرض کنیم $y_1 \neq 0$ معادله L بصورت $y = m(x - x_1) + y_1$ همانند قبل داریم $x^3 - \cdots + m^2x^2 = 0$ در این حالت ما فقط یک ریشه مضاعف x_1 را می شناسیم زیرا خط L بر خم بیضوی E در نقطه P_1 مماس است.

پس مثل قبل خواهیم داشت

$$\begin{cases} y_3 = m(x_1 - x_3) - y_1 \\ x_3 = m^2 - 2x_1 \end{cases}$$

در نهایت فرض کنید $P_۲ = \infty$ خط بین $P_۱$ و ∞ یک خط عمودی است که با E در نقطه $P_۱'$ تلاقی دارد که قرینه $P_۱$ نسبت به محور x هاست پس $P_۱ + \infty = P_۱$ برای تمام نقاط $P_۱$ روی E . پس بوضوح $\infty + \infty = \infty$

جمع بندی خواص گروه

فرض کنید E یک خم بیضوی باشد که توسط $y^۲ = x^۳ + Ax + B$ داده شده باشد. فرض کنید $P_۱ = (x_۱, y_۱)$ و $P_۲ = (x_۲, y_۲)$ نقاطی روی E باشند که مخالف ∞ باشند.

تعریف می کنیم $P_۱ + P_۲ = P_۳ = (x_۳, y_۳)$ بطوریکه

۱-اگر $x_۱ \neq x_۲$ آنگاه

$$x_۳ = m^۲ - x_۱ - x_۲$$

$$y_۳ = m(x_۱ - x_۳) - y_۱$$

$$m = \frac{y_۲ - y_۱}{x_۲ - x_۱}$$

۲-اگر $x_۱ = x_۲$ ولی $y_۱ \neq y_۲$ آنگاه $P_۱ + P_۲ = \infty$

۳-اگر $P_۱ = P_۲ = (x_۱, y_۱)$ و $y_۱ \neq ۰$ آنگاه

$$y_۳ = m(x_۱ - x_۳) - y_۱$$

$$x_۳ = m^۲ - ۲x_۱$$

$$m = \frac{۳x_۱^۲ + A}{۲y_۱}$$

۴-اگر $P_۱ = P_۲$ و $y_۱ = ۰$ آنگاه $P_۱ + P_۲ = \infty$

همچنین برای تمام نقاط تعریف می کنیم $P + \infty = P$

توجه داریم که وقتی P_1 و P_2 دارای مختصات متعلق به میدان L باشند که A, B نیز عناصر این میدان هستند آنگاه $P_1 + P_2$ نیز داری مختصات در L هستند. بنابراین $E(L)$ تحت عمل جمع معرفی شده در بالا بسته است.

قضیه ۲.۱

جمع نقاط در خم بیضوی E در شرایط زیر صدق می کند

۱-(جابجایی) $P_1 + P_2 = P_2 + P_1$ برای تمام نقاط P_1 و P_2 در E

۲-(عنصر همانی) برای تمام نقاط P در E داریم $P + \infty = P$

۳-(وجود وارون) نقطه ی P در E را در نظر می گیریم آنگاه P' در E وجود دارد بطوریکه $P + P' = \infty$
معمولا این نقطه را با $-P$ نمایش می دهیم

۴-(شرکت پذیری) برای تمام نقاط P_1 و P_2 و P_3 در E داریم $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$

یعنی نقاط E همراه با عمل جمع یک گروه آبلی با عنصر همانی ∞ تشکیل میدهند.

تذکر:

برای معادلات وایرشتراس اگر $P = (x, y)$ آنگاه $-P = (x, -y)$

برای معادلات وایشتراس تعمیم یافته اگر $P = (x, y)$ آنگاه $-P = (x, -a_1 x - a_3 - y)$

مثال ۲.۱

برای خم $y^2 = \frac{x(x+1)(2x+1)}{6}$ داریم

$$(0,0) + (1,1) = \left(\frac{1}{2}, -\frac{1}{2}\right) \quad , \quad (1,1) + \left(\frac{1}{2}, -\frac{1}{2}\right) = (24, -70)$$

در خم $y^2 = x^3 - 25x$ داریم

$$2(-4,6) = (-4,6) + (-4,6) = \left(\frac{1681}{144}, -\frac{62279}{1728}\right)$$

همچنین داریم $2(5,0) = 2(-5,0) = \infty$ و همچنین $2(0,0) = (0,0) + (-5,0) = (5,0)$

نکته:

۱-یک خم بیضوی روی یک میدان متناهی دارای تعداد متناهی نقطه با مختصات واقع در این میدان متناهی است. لذا در این حالت یک گروه آبلی متناهی داریم. خصوصیات این گونه گروه ها و کاربردهایش در رمزنگاری مشخص می شود.

۲-اگر E یک خم بیضوی روی میدان $\mathbb{Q}$ باشد آنگاه $E(\mathbb{Q})$ یک گروه آبلی متناهیا تولید شده است. این مطلب به قضیه موردل-ویل مشهور است.

این گونه گروه ها با $\mathbb{Z}^r \oplus F$ برای برخی گروه های متناهی F و برخی $r \geq 0$ یکریخت هستند. عدد صحیح r را مرتبه $E(\mathbb{Q})$ می نامیم.

۳-یک خم بیضوی روی میدان اعداد مختلط $\mathbb{C}$ با یک Tor یکریخت است

۴-اگر E روی $\mathbb{R}$ تعریف شود آنگاه $E(\mathbb{R})$ با دایره واحد s^1 و یا $s^1 \oplus \mathbb{Z}_2$ یکریخت است. مورد اول متناظر وقتی است که چند جمله ای درجه سوم $x^3 + Ax + B$ فقط دارای یک ریشه حقیقی باشد. حالت دوم متناظر زمانی است که $x^3 + Ax + B$ دارای سه ریشه حقیقی متمایز باشد.

تعریف:

نقطه ی P در E و عدد صحیح k را در نظر می گیریم آنگاه kP را با $P + \cdots + P$ (k مرتبه) نشان میدهیم اگر k منفی باشد آنگاه $kP = (-P) + \cdots + (-P)$ ($|k|$بار)

برای محاسبه kP برای k بزرگ P را مکررا با خود جمع می کنیم

مثال:

در این مثال $۱۹P$ را محاسبه می کنیم برای این منظور محاسبات زیر را باید انجام دهیم

$$۲P \;\&\; ۴P = ۲P + ۲P \;\&\; ۸P = ۴P + ۴P \;\&\; ۱۶P = ۸P + ۸P \;\&\; ۱۹P = ۱۶P + ۲P + P$$

این روش برای محاسبه kP برای k بسیار بزرگ استفاده می شود فقط تنها مشکل موجود افزایش سریع مختصات نقاط در میدان $\mathbb{Q}$ است ولی وقتی با میدان های متناهی مثل $\mathbb{F}_p$ کار می کنیم دیگر چنین مشکلی موجود نیست زیرا می توانیم پیوسته پیمانه p را کاهش دهیم (این کار را با توجه به قانون شرکت پذیری بدون هیچ مشکلی می توان انجام داد)

فضاهای تصویری و نقطه در بینهایت

می دانیم که دو خط موازی در بینهایت همدیگر را قطع می کنند. فضاهای تصویری این امکان را فراهم می سازد که نقطه در بینهایت را روی خم بیضوی مطالعه کنیم.

تعریف:

فرض کنیم K یک میدان باشد. فضای تصویری دو بعدی P_k^2 روی K توسط کلاس هم ارزی سه تایی (x,y,z) داده می شود دکه $x,y,z \in K$ بطوریکه حداقل یکی از آنها مخالف صفر است.

تعریف:

دو سه تایی (x_1,y_1,z_1) و (x_2,y_2,z_2) هم ارزند هرگاه عنصر ناصفر $\lambda \in K$ موجود باشد بطوریکه $(x_1,y_1,z_1)=(\lambda x_2,\lambda y_2,\lambda z_2)$ در این صورت می نویسیم $(x_1,y_1,z_1)\sim(x_2,y_2,z_2)$

تذکر:

کلاس هم ارزی یک سه تایی (x,y,z) فقط به قسمت گویای x,y,z بستگی دارد لذا ما کلاس هم ارزی (x,y,z) را با $(x:y:z)$ نمایش می دهیم.

اگر $(x:y:z)$ نقطه ای باشد که $z \neq 0$ آنگاه $(x:y:z)=(\frac{x}{z}:\frac{y}{z}:1)$.

نکته:

تعداد نقاط در P_k^2 متناهی است (در حالت $z=0$)

تعریف:

اگر $z=0$ آنگاه مختصات y یا x برابر ∞ خواهد شد پس نقطه (x,y,∞) نقطه در بینهایت در P_k^2 نامیده می شود.

تعریف:

یک چند جمله ای از درجه n را همگن نامیم هرگاه بصورت حاصلجمع قسمت هایی به فرم $ax^iy^jz^k$ باشد که $a \in K$ و $i+j+k=n$.

برای مثال $F(x,y,z)=2x^2-5xyz+7yz^2$ همگن از درجه ۳ است.

اگر چند جمله ای F همگن از درجه n باشد آنگاه برای هر $\lambda \in K$ داریم $F(\lambda x, \lambda y, \lambda z) = \lambda^n (x, y, z)$ در نتیجه اگر F همگن با درجه ای مشخص باشد و $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ آنگاه $F(x_1, y_1, z_1) = 0$ اگر و تنها اگر $F(x_2, y_2, z_2) = 0$

بنابراین ریشه F در P_k^2 بستگی به انتخاب نماینده برای کلاس های هم ارزی ندارد پس مجموعه ریشه های F در P_k^2 خوش تعریف است.

نکته:

اگر $f(x, y)$ یک چند جمله ای باشد می توان آن را با وارد کردن توان مناسب z همگن کرد. برای مثال اگر $f(x, y) = y^2 - x^3 - Ax - B$ آنگاه می توانیم چند جمله ای

$F(x, y, z) = y^2 z - x^3 - Axz^2 - Bz^3$ را به عنوان همگن شده چند جمله ای بالا در نظر می گیریم.

اگر چند جمله ای F همگن باشد از درجه n باشد آنگاه:

$$F(x, y, z) = z^n f\left(\frac{x}{z}, \frac{y}{z}\right)$$

$$f(x, y) = F(x, y, 1)$$

حال می توانیم معنی این که دو خط در بینهایت به هم می رسند را ببینیم فرض کنیم $y = mx + b_1$ و

$y = mx + b_2$ دو خطو موازی باشند که $b_1 \neq b_2$.

اگر دو خط فوق را بصورت همگن بنویسیم داریم $y = mx + b_1 z$ و $y = mx + b_2 z$

با حل معادلات و یافتن نقاط تلاقی خواهیم داشت $y = mx$, $z = 0$ چون هر سه x, y, z نمی تواند صفر باشد پس فرض کنیم $x \neq 0$ لذا با تقسیم بر x و یافتن نقاط تلاقی دو خط داریم $(x : mx : 0) = (1 : m : 0)$

بطور مشابه اگر $x = c_1$ و $x = c_2$ دو خط عمودی باشند در نقطه $(0 : 1 : 0)$ تلاقی دارند. این نقطه یکی از نقاط در بینهایت P_k^2 است.

حال فرض کنیم خم بیضوی E با معادله $y^2 = x^3 + Ax + B$ داده شده باشد. فرم همگن آن بصورت

$y^2z = x^3 + Axz^2 + Bz^3$ است نقطه (x, y) در معادله اصلی متناظر نقطه $(x : y : 1)$ در معادله تصویری است.

برای این که ببینیم کدام نقاط E در بینهایت هستند قرار می دهیم $z = 0$ و نتیجه می گیریم $x^3 = 0$ پس $x = 0$ و y می تواند هر عدد ناصفر باشد (توجه داریم که $(0,0,0)$ نمی تواند رخ دهد) لذا $(0,1,0) = (0, y, 0)$ و این تنها نقطه در بینهایت E است. چنانچه در بالا دیده شد $(0,1,0)$ در تمام خط های عمودی قرار گرفته است. پس هر خط عمود، E را در نقطه در بینهایت قطع می کند. بعلاوه $(0 : -1 : 0) = (0 : 1 : 0)$ که یکی در بالا و دیگری پایین محور x هاست نیز وضعیتی مشابه فوق دارند.

بررسی معادله فرما:

نشان می دهیم معادله فرما در حالت $n = 3$ یعنی $x^3 + y^3 + z^3 = 0$ وقتی $xyz \neq 0$ جواب ندارد.

چون $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ لذا بایستی $(x + y) \neq 0$.

فرض کنیم $\frac{y}{z} = u - v$ و $\frac{x}{z} = u + v$

آنگاه $(u + v)^3 + (u - v)^3 + 1 = 0$ لذا $2u^3 + 6uv^2 + 1 = 0$ چون $x + y \neq 0$ پس می توان طرفین را بر u^3 تقسیم کرده و با مرتب سازی عبارت زیر بدست می آید $6(\frac{u}{v})^2 = -\left(\frac{1}{u}\right)^3 - 2$ فرض کنید $y_1 = \frac{36v}{u} = \frac{36(x-y)}{x+y}$ پس خواهیم داشت $y_1^2 = x_1^3 - 432$ می توان نشان داد تنها جواب گویای این معادله $(x_1, y_1) = (12, \pm 36)$ و ∞ است حالت $y_1 = 36$ نتیجه می دهد $x + y = x - y$ یعنی $y = 0$ و حالت $y_1 = -36$ نتیجه می دهد $x = 0$ و نقطه $(x, y) = \infty$ متناظر است با $x = -y$ یعنی $z=0$

پس $x^3 + y^3 + z^3 = 0$ وقتی $xyz \neq 0$ دارای جواب نیست.

دستگاه‌های مختصات دیگر

فرمول اضافه کردن دو نقطه به یک خم بیضوی در فرم وایرشتراس نیازمند دو عمل ضرب یک عمل مربع کردن و دو انعکاس در میدان مربوطه است. هر چند که یافتن معکوس سریع است با این حال خیلی کندتر از ضرب است.

مختصات تصویری:

به طور معمول در مختصات تصویری نقاط را به صورت $(x:y:z)$ نمایش می دهیم با مشخص کردن مقسوم علیه ها در فرمول های استاندارد برای جمع، مطالب زیر را خواهیم داشت:

فرض کنید $P_i = (x_i:y_i:z_i)$ برای $i = ۱,۲$ نقاط روی خم بیضوی $y^۲z = x^۳ + Axz^۲ + Bz^۳$ باشد. آنگاه $(x_۱:y_۱:z_۱) + (x_۲:y_۲:z_۲) = (x_۳:y_۳:z_۳)$ که در آن $x_۳$ و $y_۳$ و $z_۳$ بصورت زیر محاسبه می شوند.

وقتی $P_۱ \neq \pm P_۲$

$$u = y_۲z_۱ - y_۱z_۲ \ , \ v = x_۲z_۱ - x_۱z_۲ \ , \ w = u^۲z_۱z_۲ - v^۳ - ۲v^۲x_۱z_۲$$

$$x_۳ = vw \ , \ y_۳ = u(v^۲x_۱z_۲ - w) - v^۳y_۱z_۲ \ , \ z_۳ = v^۳z_۱z_۲$$

وقتی $P_۱ = P_۲$

$$t = Az_۱^۲ + ۳x_۱^۲ \ , \ u = y_۱z_۱ \ , \ v = ux_۱y_۱ \ , \ w = t^۲ - ۸v$$

$$x_۳ = ۲uw \ , \ y_۳ = t(۴v - w) - ۸y_۱^۲u^۲ \ , \ z_۳ = ۸u^۳$$

وقتی $P_۱ = -P_۲$ داریم $P_۱ + P_۲ = \infty$

در این روش جمع نقاط نیازمند ۱۲ ضرب و ۲ مربع کردن است در حالیکه مضاعف سازی به ۷ ضرب و ۵ مربع کردن نیاز دارد.

در این روش، وارون کردن لازم نیست چرا که جمع و تفرق کردن بسیار سریعتر از ضرب کردن است.

مختصات ژاکوبین:

تغییر در مختصات تصویری به یک دوگانه سازی سریعتر منجر می شود.

فرض کنید $(x:y:z)$ نشان دهنده نقاط آفین $(x/z^{۲}, y/z^{۳})$ یاشد. این مطلب معقول است زیرا در بخش ۱۱ نشان داده خواهد شد که تابع x دارای دو قطب در بینهایت و تابع y دارای سه قطب در بینهایت است.

در مختصات ژاکوبین خم بیضوی $y^{۲} = x^{۳} + Ax + B$ به خم بیضوی $y^{۲} = x^{۳} + Axz^{۴} + Bz^{۶}$ تبدیل می شود و نقطه در بینهایت دارای مختصات $(۰:۱:۰) = \infty$ می باشد.

فرض کنید $P_i = (x_i:y_i:z_i)$ برای $i = ۱,۲$ نقاط روی خم بیضوی $y^{۲} = x^{۳} + Axz^{۴} + Bz^{۶}$ باشند. آنگاه $(x_۱:y_۱:z_۱) + (x_۲:y_۲:z_۲) = (x_۳:y_۳:z_۳)$ که در آن $x_۳$ و $y_۳$ و $z_۳$ بصورت زیر محاسبه می شوند.

وقتی $P_۱ \neq \pm P_۲$

$$r = x_۱z_۲^{۲} \ , \ s = x_۲z_۱^{۲} \ , \ t = y_۱z_۲^{۳} \ , \ u = y_۲z_۱^{۳} \ , \ v = s - r \ , \ w = u - t$$

$$x_۳ = -r^{۳} - ۲rv^{۲} + w^{۲} \ , \ y_۳ = -tv^{۳} + (rv^{۲} - x_۳)w \ , \ z_۳ = vz_۱z_۲$$

وقتی $P_۱ = P_۲$

$$v = ۴x_۱y_۱^{۲} \ , \ w = ۳x_۱^{۲} + Az_۱^{۴}$$

$$x_۳ = -۲v + w^{۲} \ , \ y_۳ = -۸y_۱^{۴} + (v - x_۳)w \ , \ z_۳ = ۲y_۱z_۱$$

وقتی $P_۱ = -P_۲$ داریم $P_۱ + P_۲ = \infty$

برای جمع نقاط به ۱۲ ضرب و ۴ مربع کردن لازم داریم و دوگانه سازی به ۳ ضرب و ۶ مربع کردن نیاز دارد و وارون کردن هم لازم نیست.

مختصات ادواردز:

قضیه ۲.۱۸

فرض کنید K میدانی باشد که مشخصه اش دو نیست. خم $C: u^{۲} + v^{۲} = c^{۲}(۱ + du^{۲}v^{۲})$ با خم بیضوی $E: y^{۲} = (x - c^{۴}d - ۱)(x^{۲} - ۴c^{۴}d)$ یکریخت است

با تغییر متغییر $x = \frac{-۲c(w-c)}{u^۲}$ و $y = \frac{۴c^۲(w-c)+۲c(c^۴d+۱)u^۲}{u^۳}$ که در آن $w = (c^۲du^۲ - ۱)v$ نقطه $(۰,۱)$ عضو همانی گروه خواهد بود و عمل جمع برای تمام نقاط $(u_i, v_i) \in C(K)$ بصورت زیر خواهد بود.

$$(u_۱, v_۱) + (u_۲, v_۲) = (\frac{u_۱v_۲+u_۲v_۱}{c(۱+du_۱u_۲v_۱v_۲)}, \frac{v_۱v_۲-u_۱u_۲}{c(۱-du_۱u_۲v_۱v_۲)})$$

و وارون نقطه (u, v) برابر $(-u, v)$ است (یعنی $-(u, v) = (-u, v)$)

نکته:

در مختصات ادوارد فرمول مجزایی برای $P_۱ + P_۲ ,۲P$ وقتی $P_۱ \neq P_۲$ وجود ندارد

Jـ پایا

فرض کنید E یک خم بیضوی باشد که توسط $y^۲ = x^۳ + Ax + B$ داده شده است که A و B عناصر میدانی هستند که مشخصه اش ۲ و ۳ نیست. اگر فرض کنیم

$$x_۱ = \mu^۲x \quad , \quad y_۱ = \mu^۳y \quad s.t. \quad \mu \in \bar{K}^\times$$

آنگاه $y_۱^۲ = x_۱^۳ + A_۱x_۱ + B_۱$ که در آن $A_۱ = \mu^۴A \quad , \quad B_۱ = \mu^۶B$

(درمعادله وایرشتراس تعمیم یافته $y^۲ + a_۱xy + a_۳y = x^۳ + a_۲x^۲ + a_۴x + a_۶$ تغییر متغیر باعث بوجود آمدن ضریب جدید $\mu^i a_i$ می شود.)

یک $j-$ پایا از E را بصورت زیر تعریف می کنیم

$$j = j(E) = ۱۷۲۸\frac{۴A^۳}{۴A^۳ + ۲۷B^۲}$$

توجه داریم که با توجه به مبین مکعب، مخرج منفی است پس $j-$ پایا ناصفر است. تغییر متغیر ها j را بدون تغییر می گذارند.

قضیه:

فرض کنید $y_1^2 = x_1^3 + A_1x_1 + B_1$ و $y_2^2 = x_2^3 + A_2x_2 + B_2$ دو خم بیضوی با j – پایاهای به ترتیب j_1 و j_2 باشند. اگر $j_1 = j_2$ آنگاه $\mu \neq 0$ در $\overline{K}$ (= بستار جبری K) هست که $A_2 = \mu^4 A_1$ و $B_2 = \mu^6 B_1$

تغییر متغیر $y_2 = \mu^3 y_1$ و $x_2 = \mu^2 x_1$ معادلات مربوط به خم های بیضوی را به هم تبدیل می کنند.

اثبات:

ابتدا فرض می کنیم $A_1 \neq 0$ چون این هم ارز است با اینکه $j_1 \neq 0$ لذا خواهیم داشت $A_2 \neq 0$.

μ را طوری انتخاب می کنیم که $A_2 = \mu^4 A_1$ لذا

$$\frac{4A_2^3}{4A_2^3 + 27B_2^2} = \frac{4A_1^3}{4A_1^3 + 27B_1^2} = \frac{4\mu^{-12}A_2^3}{4\mu^{-12}A_2^3 + 27B_1^2} = \frac{4A_2^3}{4A_2^3 + 27\mu^{12}B_1^2}$$

که نتیجه می دهد $B_2^2 = (\mu^6 B_1)^2$ بنابراین $B_2 = \pm\mu^6 B_1$

اگر $B_2 = \mu^6 B_1$ قضیه اثبات شده است

اگر $B_2 = -\mu^6 B_1$ آنگاه با تبدیل μ به $i\mu$ ($i^2 = -1$) روابط $A_2 = \mu^4 A_1$ و $B_2 = \mu^6 B_1$ باقی خواهد ماند.

اگر $A_1 = 0$ آنگاه $A_2 = 0$. چون $4A_i^3 + 27B_i^2 \neq 0$ داریم $B_2 \neq 0$ و B_1 و μ را طوری بر می گزینیم که $B_2 = \mu^6 B_1$.

توجه:

j دارای دو مقدار است که اغلب اتفاق می افتد

۱۷۲۸-۰ $j =$ در این حالت خم بیضوی E دارای معادله $y^2 = x^3 + B$ خواهد بود.

۱۷۲۸-۲ $j =$ در این حالت خم بیضوی E دارای معادله $y^2 = x^3 + Ax$ خواهد بود.

مورد اول یک بار با $B = -432$ در بخش ۲.۵.۲ توسط معادلات فرما $x^3 + y^3 + z^3 = 0$ دیده شده و مورد دوم یک بار با $A = -25$ و یک بار با $A = -4$ در بخش اول دیده شد.

حالت های یک و دو که در بالا اشاره شده دارای خود ریختی هایی به فرم زیر هستند

حالت اول، یعنی خم $y^2 = x^3 + B$ دارای خود ریختی $(x, y) \longmapsto (\xi x, -y)$ است که در آن ξ ریشه سوم واحد نابدیهی است

حالت دوم، یعنی خم $y^2 = x^3 + Ax$ دارای خود ریختی $(x, y) \longmapsto (-x, iy)$ است که در آن $i^2 = -1$.

توجه:

توجه می کنیم که $j-$ پایا بیان می کند که چه زمانی دو خم در بستار جبری یک میدان یکریخت هستند. اما اگر با میدان K (بدون بستار جبری) کار کنیم ممکن است ۲ خم را با $j-$ پایاهای یکسان بیابیم که نمی توانیم آن ها را با توابع با ضرایب در K به یکدیگر تبدیل کنیم.

برای مثال هر دوی $y^2 = x^3 - 25x$ و $y^2 = x^3 - 4x$ دارای $j = 1728$ هستند. خم اول دارای تعداد نامتناهی نقطه با مختصات در $\mathbb{Q}$ برای مثال تمام ضرایب $(-4,6)$ است و برای خم دوم تنها نقاط زیر را داریم $\infty, (2,0), (-2,0), (0,0)$

پس ما نمی توانیم یکی از خم ها را با توابع با مختصات در $\mathbb{Q}$ به دیگری تبدیل کنیم. البته می توانیم از $\mathbb{Q}(\sqrt{10})$ برای تبدیل خم ها به یکدیگر استفاده کرد که $(x, y) \longmapsto (\mu^2 x, \mu^2 y)$ که $\mu = \frac{\sqrt{10}}{2}$.

تعریف:

اگر دو خم بیضوی متفاوت که روی یک میدان K تعریف شده اند دارای $j-$ پایاهای یکسان باشند آنگاه می گوییم این دو خم به هم تابیده شده (پیچ خورده) اند.

در نهایت توجه می کنیم که $j-$ پایای $y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}$ وقتی که $j \neq 0,1728$ است برابر j است.

چون $y^2 = x^3 + x$ و $y^2 = x^3 + 1$ دارای $j-$ پایاهای ۰ و ۱۷۲۸ هستند ما $j-$ پایاها بین دوسویی های $K \longrightarrow \overline{K}$ از خم بیضوی تعریف شده روی K را می یابیم (یعنی، هر $j \in K$ متناظر با یک خم بیضوی تعریف شده روی K است. و هر دو خم بیضوی تعریف شده روی K با $j-$ پایاهای یکسان می توانند با تغییر متغیرها به یکدیگر تبدیل شوند که روی $\overline{K}$ تعریف می شوند.)

در میدان هایی با مشخصه ۲ و ۳، $j-$ پایا می تواند تعریف شود و نتایج مشابه بالا نیز برقرار است.

خم های بیضوی در مشخصه ۲

ما در بخش گذشته از معادلات وایرشتراس به جای معادلات وایرشتراس تعمیم یافته استفاده کردیم به همین دلیل نتایج بدست آمده در میدان های با مشخصه ۲ کارایی ندارند.

توجه کنید که معادلات وایرشتراس یکتا هستند

فرض کنیم $f(x,y)=y^{۲}-x^{۳}-Ax-B$ آنگاه $f_y=۲y=۰$ زیرا در مشخصه دو داریم $۲=۰$

فرض کنید $x_.$ ریشه (ممکن است در توسیع های K باشد) $f_x=-۳x^{۲}-A=۰$ و $y_.$ ریشه دوم (ریشه توان دوم) $x_.^{۳}+Ax_.+B$ باشد آنگاه $(x_.,y_.)$ در منحنی قرار دارند و

$$f_x(x_.,y_.)=f_y(x_.,y_.)=۰$$

بنابراین با معادلات وایرشتراس تعمیم یافته برای خم بیضوی E کار می کنیم

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

اگر $a_۱\neq ۰$ با تغییر متغیر خواهیم داشت

$$x=a_۱^{۲}x_۱+\left(\frac{a_۳}{a_۱}\right)\quad,\quad y=a_۱^{۳}y_۱+a_۱^{-۳}(a_۱^{۲}a_۴+a_۳^{۲})$$

که معادله را به فرم زیر در می آورند

$$y_۱^{۲}+x_۱y_۱=x_۱^{۳}+a_۲'x_۱^{۲}+a_۶'$$

این معادله یکتا نیست اگر و تنها اگر $a_۶'\neq ۰$

$j-$ پایا در این حالت $\frac{۱}{a_۶'}$ تعریف می شود.

اگر $a_۱=۰$ فرض می کنیم $x=x_۱+a_۲$ و $y=y_۱$ معادله زیر را خواهیم داشت

$$y_۱^{۲}+a_۳'y_۱=x_۱^{۳}+a_۴'x_۱+a_۶'$$

این معادله یکتا نیست اگر و تنها اگر $a_۳'\neq ۰$ و $j-$ پایا در این حالت صفر تعریف می شود.

حال به معادله وایرشتراس تعمیم یافته بر می گردیم و نقاط در بینهایت را بررسی می کنیم. معادله همگن زیر را داریم

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

حال اگر $z = 0$ خواهیم داشت $x^3 = 0$ پس $(0:1:0) = \infty$ تنها نقطه در بینهایت E است که درست مثل معادله وایرشتراس استاندارد است.

خط L بین نقاط $(x_.,y_.)$ و ∞، خط عمودی $x = x_.$ است. پس اگر $(x_.,y_.)$ در E قرار داشته باشد نقطه تلاقی دیگر E و L نقطه $(x_.,-a_1x_. - a_3 - y_.)$ می باشد.

حال می توانیم جمع نقاط را توصیف کنیم. البته برای تمام نقاط P داریم $P + \infty = P$. جمع سه نقطه P,Q,R برابر بینهایت است اگر و تنها اگر هم خط باشند. معکوس نقاط بصورت زیر است

$$-(x,y) = (x,-ax - a_3 - y)$$

برای جمع دو نقطه P_1 و P_2 روال زیر را طی می کنیم

خط L گذرا از P_1 و P_2 را رسم می کنیم (وقتی $P_2 = P_1$ این خط مماس است) این خط E را درنقطه سومی مثل P_3' قطع می کند. حال $P_3 = -P_3'$ را محاسبه می کنیم (تنها با فرمول داده شده این کار را انجام می دهیم و توجه می کنیم که این وارون نسبت به محور x ها نیست.) و سپس $P_1 + P_2 = P_3$

این جمع شرکت پذیر است. نقاط E شامل ∞ نیز هستند پس به فرم یک گروه آبلی هستند.

دوگانه سازی نقاط در مشخصه ۲

دو حالت زیر را بررسی می کنیم

۱- $y^2 + xy = x^3 + a_2x^2 + a_6$ لذا $y^2 + xy + x^3 + a_2x^2 + a_6 = 0$ (چون در مشخصه ۲ هستیم) با مشتق گیری ضمنی خواهیم داشت $xy' + (y + x^2) = 0$ (زیرا $2 = 0$ و $1 = 3$)

بنابراین شیب خط گذرا از نقطه $P = (x_.,y_.)$ برابر $m = \frac{y_.+x_.^2}{x_.}$ است لذا معادله خط بصورت زیر در می آید $y = m(x - x_.) + y_. = mx + b$ برای برخی b است. با جایگذاری نقاط قطع L و E مثل (x_1,y_1) را می یابیم.

$$0 = (mx+b)^2 + x(mx+b) + x^3 + a_2x^2 + a_6 = x^3 + (m^2+m+a_2)x^2 + \cdots$$

حاصل جمع ریشه ها ی $x_1 + x_0 + x_0$ برابر (m^2+m+a_2) است لذا داریم

$$x_1 = m^2 + m + a_2 = \frac{y_0^2 + x_0^4 + x_0y_0 + x_0^3 + a_2x_0^2}{x_0^2} = \frac{x_0^4 + a_6}{x_0^2}$$

(چون $y_0^2 = x_0y_0 + x_0^3 + a_2x_0^2 + a_6$)

مختصات y این اشتراک (قطع دادن) $y_1 = m(x_1 - x_0) + y_0$ است. نقطه (x_1, y_1) مساوی $-2P$ می باشد پس $2P = (x_2, y_2)$ که $y_2 = -x_1 - y_1 = x_1 + y_1$ و $x_1 = \frac{x_0^4+a_6}{x_0^2}$

۲- $y^2 + a_3y + x^3 + a_4x + a_6 = 0$ این معادله را بصورت $y^2 + a_3y = x^3 + a_4x + a_6$ می نویسیم (چون مشخصه میدان ۲ است) سپس با مشتق گیری ضمنی خواهیم داشت

$a_3y' + (x^2 + a_4) = 0$ پس خط مماس $y = m(x - x_0) + y_0$ است که $m = \frac{x_0^2+a_4}{a_3}$ با جایگذاری و حل همانند مورد قبل نقاط قطع L و E مثل (x_1, y_1) را می یابیم که

$$x_1 = m^2 = \frac{a_0^4 + a_4^2}{a_3^2} \quad , \quad y_1 = m(x_1 - x_0) + y_0$$

بنابراین $2P = (x_2, y_2)$ که $y_2 = a_3 + y_1$ و $x_1 = \frac{x_0^4+a_4^2}{a_3^2}$.

درونریختی

منظور از یک درون ریختی از E یک همریختی $\alpha: E(\bar{K}) \longrightarrow E(\bar{K})$ است که توسط یک تابع گویا داده می شود. بعبارت دیگر $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ و توابع گویا (چند جمله ای های خارج قسمتی) $R_1(x,y)$ و $R_2(x,y)$ با ضرایب در $\bar{K}$ موجود باشند بطوریکه برای تمام $(x,y) \in E(\bar{K})$ داشته باشیم $\alpha(x,y) = R_1(x,y) + R_2(x,y)$

چون α همریختی است داریم $\alpha(\infty) = \infty$ و همچنین فرض می کنیم α نابدیهی باشد یعنی برخی نقاط (x,y) موجود باشند بطوریکه $\alpha(x,y) \neq \infty$.

درون ریختی بدیهی که تمام نقاط را به ∞ می نگارد را با 0 نشان می دهیم.

مثال

فرض کنید E با $y^2 = x^3 + Ax + B$ داده شده باشد و فرض کنید $\alpha(P) = 2P$ آنگاه α همریختی است و $\alpha(x,y) = (R_1(x,y), R_2(x,y))$ که در آن $R_1(x,y) = (\frac{3x^2+A}{2y})^2 - 2x$ و

$$R_2(x,y) = \left(\frac{3x^2+A}{2y}\right)\left(3x - \left(\frac{3x^2+A}{2y}\right)^2\right) - y$$

چون α همریختی است که توسط توابع کسری داده شده لذا α یک درونریختی روی E است.

توجه:

برای توضیح درون ریختی ها توسط توابع گویا بهتر است یک شکل استاندارد در نظر داشته باشیم. برای سادگی فرض کنیم خم بیضوی ما به فرم وایرشتراس داده شده باشد. فرض کنیم $R(x,y)$ تابع گویای دلخواهی باشد چون برای تمام $(x,y) \in E(\overline{K})$ داریم $y^2 = x^3 + Ax + B$ پس می توانیم توان های زوج y را با یک چند جمله ای از x و توانهای فرد y را با ضرب y در یک چند جمله ای از x بیان کنیم و ملاحظه کنیم که کسرهای گویای مشابهی مثل $R(x,y)$ با نقاط در $E(\overline{K})$ می دهند.

بنابراین می توانیم فرض کنیم $R(x,y) = \frac{P_1(x)+P_2(x)y}{P_3(x)+P_4(x)y}$ بعلاوه با گویا کردن کسر و جایگذاری y^2 با $x^3 + Ax + B$ خواهیم داشت $R(x,y) = \frac{q_1(x)+q_2(x)y}{q_3(x)}$

درون ریختی $\alpha(x,y) = (R_1(x,y), R_2(x,y))$ را در نظر می گیریم.

چون α همریختی است داریم $\alpha(x,-y) = \alpha\big(-(x,y)\big) = -\alpha(x,y)$ یعنی

$$R_1(x,-y) = -R_1(x,y) \text{ و } R_2(x,-y) = -R_2(x,y)$$

لذا اگر R_1 را به فرم $R_1(x,y) = \frac{q_1(x)+q_2(x)y}{q_3(x)}$ بنویسم آنگاه $q_2(x) = 0$ و اگر R_2 را به فرم فوق بنویسیم آنگاه خواهیم داشت $q_1(x) = 0$

پس می توانیم فرض کنیم $\alpha(x,y) = (r_1(x), r_2(x)y)$ که در آن $r_1(x)$ و $r_2(x)$ توابع گویا هستند.

حال می توانیم به این پرسش که اگر یکی از توابع گویا در نقطه ای تعریف نشود چه اتفاقی می افتد پاسخ بدهیم.

فرض کنیم $r_1(x) = {p(x)}/{q(x)}$ که در آن p و q چند جمله ای هایی هستند که عامل مشترک ندارند.

اگر برای برخی نقاط (x,y) داشته باشیم $q(x) = 0$ آنگاه می توان فرض کرد $\alpha(x,y) = \infty$. اگر $q(x) \neq 0$ آنگاه طبق تمرین ۲.۱۹ ، $r_2(x)$ تعریف می شود. لذا تابع گویا است و در نتیجه α تعریف می شود.

تعریف:

درجه α را (در حالتی که α نابدیهی است) بصورت $deg\alpha = \max\{\deg p(x), \deg q(x)\}$ تعریف می کنیم

اگر $\alpha = 0$ درجه α را برابر صفر در نظر می گیریم.

تعریف:

$\alpha \neq 0$ را یک درون ریختی جداشدنی نامیم هرگاه مشتق $r_1'(x)$ متحد با صفر نباشد یا بطور معادل حداقل یکی از $p'(x)$ یا $q'(x)$ متحد با صفر نباشد.

مثال

در ادامه مثال قبلی وقتی $\alpha(P) = 2P$ خواهیم داشت $R_1(x,y) = (\frac{3x^2+A}{2y})^2 - 2x$ و با توجه به این که $y^2 = x^3 + Ax + B$ با اندکی محاسبات خواهیم داشت

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

لذا $deg\alpha = 4$

چند جمله ای $q'(x) = 4(3x^2 + A)$ مخالف صفر است (حتی در مشخصه ۳ نیز چنین است زیرا اگر $A = 0$ آنگاه $x^3 + B$ دارای ریشه چند گانه است که متناقض با فرض است)

لذا α جداشدنی است.

مثال

مثال قبل را در مشخصه ۲ بررسی می کنیم از فرمول های دوگانه سازی که در بخش قبلی بدست آمد استفاده می کنیم. در مورد $y^2 + xy = x^3 + a_2x^2 + a_6$ داریم $\alpha(x,y) = (r_1(x), R_2(x,y))$ که $r_1(x) = {x^4 + a_6}/{x^2}$ بنابراین $deg\alpha = 4$.

چون $p'(x) = 4x^3 = 0$ و $q'(x) = 2x = 0$ پس درون ریختی مورد بحث جدا شدنی نیست.

بطور مشابه اگر $y^2 + a_3y = x^3 + a_4x + a_6$ آنگاه $r_1(x) = {x^4 + a_4^2}/{a_3^2}$ بنابراین $deg\alpha =$

۴ ولی α جداشدنی نیست.

نکته

در مشخصه p نگاشت $\alpha(Q) = Q$ دارای درجه p^2 است و جداشدنی نیست.

مثال

یک مثال مهم برای درون ریختی نگاشت فروبینوس می باشد. که بصورت زیر تعریف می شود

فرض کنیم E روی میدان متناهی $\mathbb{F}_q$ تعریف شود. آنگاه نگاشت $\varphi_q(x,y) = (x^q, y^q)$ را نگاشت فروبینوس می نامیم که نقش بسیار مهمی در نظریه خم های بیضوی روی میدان متناهی $\mathbb{F}_q$ دارد.

لم ۲.۲۰

فرض کنیم E روی میدان متناهی $\mathbb{F}_q$ تعریف شود. آنگاه φ_qیک درون ریختی از E با درجه q است که جداشدنی نیست

اثبات:

فرض کنیم $\varphi_q(x,y) = (x^q, y^q)$ نگاشتی با توابع گویا (چند جمله ای ها) باشد که دارای درجه q است.

نکته اصلی این است که $\varphi_q : E(\overline{\mathbb{F}_q}) \longrightarrow E(\overline{\mathbb{F}_q})$ یک همریختی است. فرض کنیم (x_1, y_1) و (x_2, y_2) نقاطی در $E(\overline{\mathbb{F}_q})$ باشند بطوریکه $x_1 \neq x_2$ و جمع این دو نقطه برابر نقطه (x_3, y_3) باشد که $x_3 = m^2 - x_1 - x_2$ و $y_3 = m(x_1 - x_3) - y_1$ بطوریکه $m = \frac{y_2 - y_1}{x_2 - x_1}$

(ما در اینجا با فرم وایرشتراس کار می کنیم و اثبات در فرم وایرشتراس تعمیم یافته بطور مشابه انجام می شود)

توان q- ام به فرم زیر می باشد $x_3^q = m'^2 - x_1^q - x_2^q$ و $y_3^q = m'(x_1^q - x_3^q) - y_1^q$ بطوریکه $m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}$

یعنی $\varphi_q(x_3, y_3) = \varphi_q(x_1, y_1) + \varphi_q(x_2, y_2)$

حالت هایی که $x_1 = x_2$ یا حالتی که یکی از نقاط بینهایت شود براحتی بررسی می شوند.

این فرمول بیانگر این است که $2(x_1, y_1) = (x_2, y_2)$ که $x_3 = m^2 - 2x_1$ و

$y_3 = m(x_1 - x_3) - y_1$ که در آنها $m = \frac{3x_1^2 - A}{2y_1}$

وقتی این عبارت ها به توان q برسند خواهیم داشت $x_3^q = m'^2 - 2x_1^q$ و $y_3^q = m'(x_1^q - x_3^q) - y_1^q$

بطوریکه $m' = \frac{3^q (x_1^q)^2 - A^q}{2^q y_1^q}$

چون $2,3, A \in \mathbb{F}_q$ داریم $A^q = A\ , 2^q = 2\ , 3^q = 3$ و این یعنی ما فرمول دوگانه سازی را برای نقطه (x_1^q, y_1^q) در E بدست آوردیم (اگر $A^q \neq A$ با خم بیضوی دیگری که $A^q = A$ باشد کار می کنیم)

چون φ_q همریختی است که توسط توابع گویا داده شده یک درونریختی در E است. چون $q = 0$ پس در $\mathbb{F}_q$ مشتق x^q متحد با صفر است بنابراین φ_q جداشدنی نیست.

قضیه ۲.۲۱

فرض کنید α یک درونریختی جداشدنی از خم بیضوی E باشد آنگاه $deg\alpha = \#\ker(\alpha)$ که در آن $\ker(\alpha)$ هسته همریختی $\alpha: E(\bar{K}) \longrightarrow E(\bar{K})$ می باشد.

اگر α جدا شدنی نباشد آنگاه $deg\alpha > \#\ker(\alpha)$

اثبات

فرض کنیم $\alpha(x,y)=(r_1(x),r_2(x)y)$ باشد که در آن $r_1(x)=p(x)/q(x)$ بطوریکه

$$\gcd(p,q)=1$$

فرض کنیم α جداشدنی باشد آنگاه $r_1'\neq 0$ پس $p'q-pq'$ بعنوان چند جمله ای صفر نیست. فرض کنیم $S=\{x\in\bar{K}\mid (p'q-pq')(x)=0\}$ و فرض کنیم $(a,b)\in E(\bar{K})$ طوری باشد که

۱- $a\neq 0, b\neq 0, (a,b)\neq 0$
۲- $\deg\big(p(x)-aq(x)\big)=\max\{\deg(p),\deg(q)\}=\deg(\alpha)$
۳- $a\notin r_1(S)$
۴- $(a,b)\in\alpha(E(\bar{K}))$

چون $p'q-pq'$ چند جمله ای صفر نیست پس S متناهی است لذا تصویرش تحت α یعنی $\alpha(S)$ نیز متناهی است لذا (a,b) ای با مشخصات فوق واقعا موجود است

ادعا می کنیم $deg\alpha=\#\{(x,y)\in E(\bar{K})\mid\alpha(x_1,y_1)=(a,b)\}$

حال ادعا را ثابت می کنیم: فرض کنیم (a,b) چنین نقاطی باشد $(\alpha(x_1,y_1)=(a,b))$

در نتیجه خواهیم داشت $y_1r_2(x_1)=b$ و $\frac{p(x_1)}{q(x_1)}=a$ چون $(a,b)\neq\infty$ بایستی $q(x_1)\neq 0$ بنابر تمرین ۲.۱۹، $r_2(x_1)$ معین است لذا خواهیم داشت $y_1r_2(x_1)=b\Longrightarrow y_1=\frac{b}{r_2(x_1)}$ (چون $b\neq 0$) یعنی y_1 توسط x_1 تعیین می شود پس کافیست x_1 ها را بشماریم که $\alpha(x_1,y_1)=(a,b)$. طبق فرض شماره ۲ درجه $p-aq$ برابر با درجه α است.

یعنی $p-aq$ به اندازه $deg\alpha$ ریشه دارد (با احتساب ریشه های تکراری) بنابراین با توجه به فرم مجموعه $\{(x,y)\in E(\bar{K})\mid\alpha(x,y)=(a,b)\}$ می توان گفت که اگر بتوانیم نشان دهیم $p-aq$ دارای ریشه تکراری نیست در این صورت ادعا ثابت خواهد شد.

فرض کنیم $x_.$ یک ریشه تکراری $p-aq$ باشد (فرض خلف) در این صورت $p(x_.)-aq(x_.)=0$ و همچنین $p'(x_.)-aq'(x_.)=0$ داریم $p=aq$ و $p'=aq'$ با ضرب طرفین خواهیم داشت

$$a(p'q-pq')=0\overset{a\neq 0}{\Longrightarrow}(p'q-pq')(x_.)=0\Longrightarrow x_.\in S$$

لذا $a = r_1(x_.) \in r_1(S)$ که با شرط سه متناقض است پس $p - aq$ ریشه تکراری ندارد. و این اثبات ادعا را کامل می کند.

فرض کنیم $(x_1, y_1) \in E(\overline{K})$ طوری باشدکه $\alpha(x_1, y_1) = (a, b)$. فرض کنیم

$ker\alpha = \{g_1, \dots, g_t\}$ در این صورت برای هر $1 \leq i \leq t$ خواهیم داشت

$\alpha(g_i + (x_1, y_1)) = (a, b)$ در نتیجه می توان گفت دقیقا $\#ker\alpha$ نقطه هست که $\alpha(x_1, y_1) = (a, b)$ با ترکیب نتیجه اخیر با ادعا نتیجه می گیریم $\#ker\alpha = deg\alpha$

حال اگر α جداشدنی نباشد در این صورت $p'q - pq'$ همواره صفر خواهد بود لذا $p(x) - aq(x) = 0$ همواره دارای ریشه های تکراری خواهد بود پس $\{(x, y) \in E(\overline{K}) | \alpha(x, y) = (a, b)\} = \#ker\alpha$ کمتر از $deg\alpha$ خواهد بود پس $deg\alpha > \#\ker(\alpha)$.

قضیه

فرض کنید E یک خم بیضوی روی میدان K باشد. فرض کنید $\alpha \neq 0$ یک درون ریختی از E باشد آنگاه $\alpha: E(\overline{K}) \longrightarrow E(\overline{K})$ پوشاست

اثبات

باید نشان دهیم برای هر $(a, b) \in E(\overline{K})$ یک (x, y) هست که $\alpha(x, y) = (a, b)$ اگر $(a, b) = 0$ حکم بدیهی است پس فرض کنیم $(a, b) \neq 0$ فرض کنیم $r_1(x) = {p(x)}/{q(x)}$ بطوریکه

$$\gcd(p, q) = 1$$

حالت اول: $p - aq$ چند جمله ای ثابت نیست

در این حالت ریشه ای مثل $x_.$ خواهد داشت. چون $\gcd(p, q) = 1$ پس باید $q(x_.) \neq 0$ در غیر این صورت از $p(x_.) - aq(x_.) = 0$ نتیجه می شود $p(x_.) = 0$ یعنی $x_.$ ریشه p است. فرض کنیم $y_. \in \overline{K}$ $\sqrt{a^3 + aA + B} = y_.$ پس بنابر تمرین ۲.۱۹، $\alpha(x_., y_.)$ تعریف شده و داریم $\alpha(x_., y_.) = (a, b')$ که در آن $b' \in \overline{K}$. حال با توجه به این که $(a, b) \in E(\overline{K})$ می توان نوشت $(a, b') \in E(\overline{K}) \Longrightarrow b'^2 = a^3 + aA + B = b^2$ لذا $b' = \pm b$

اگر $b' = b$ آنگاه $\alpha(x_., y_.) = (a, b)$

اگر $b' = -b$ آنگاه $\alpha(x_., -y_.) = -\alpha(x_., y_.) = -(a, b') = -(a, -b) = (a, b)$

حالت دوم: $p - aq$ چند جمله ای ثابت باشد

از آنجا که $\alpha(E(\bar{K}))$ نامتناهی و $\#ker\alpha$ متناهی است می توان گفت که تنها تعدادی متناهی نقطه می توانند به نقطه ای با مختص x داده شده تصویر شوند (حداکثر برابر با $۲\#ker\alpha$) پس p و q هر دو باید غیر ثابت باشند اگر p ثابت باشد، چون $p - aq$ ثابت است پس q نیز ثابت خواهد بود در این حالت تعداد نقاطی که به یک نقطه با مختص x داده شده تصویر می شوند بینهایت است.

$$\#\{(x,y)|\alpha(x,y) = (x,-) \Longrightarrow \#\{(x,y)|\ (\frac{p(x)}{q(x)}\ , y)\} = (a,b) \Longrightarrow$$
$$\#\{(x,y)\ |\ (c, yr_۲(x) = (x,-) = \infty$$

که بحث بالا را نقض می کند پس p و q هر دو باید غیر ثابت باشند حداکثر یک تابع مثل a می توان یافت که $p - aq = const$ زیرا اگر a' ثابت دیگری باشد که $p - a'q = const$ آنگاه از این دو رابطه خواهیم داشت $(a - a')q = const \ \Longrightarrow q = const$

می خواهیم نشان دهیم $(a, b) \in Im\alpha$

اگر $(a, b) \notin Im\alpha$ آنگاه $(a, -b) \notin Im\alpha$ پس با توجه به بحث بالا می توان گفت *حداکثر دو نقطه مثل (a, b) و $(a, -b)$ می توان یافت که در $Im\alpha$ نیست. *

فرض کنیم $(a_۱, b_۱)$ نقطه ای غیر از (a, b) باشد پس در $Im\alpha$ قرار دارد. لذا می توان $(a_۱, b_۱)$ را طوری برگزید که

$$\exists P_۱ \in E(\bar{K}) \quad s.t. \quad \alpha(P_۱) = (a_۱, b_۱)$$

پس بنابر *

$$(a_۱, b_۱) + (a, b) \in Im\alpha \Longrightarrow \ \exists P_۲ \in E(\bar{K})\ \ s.t. \alpha(P_۲) = (a_۱, b_۱) + (a, b)$$
$$\Longrightarrow \alpha(P_۲ - P_۱) = \alpha(P_۲) - \alpha(P_۱) = (a, b) \bullet$$

برای کاربردهای بعدی محک مناسبی برای جداشدنی لازم داریم اگر (x,y) نقطه متغیر در $y^2 = x^3 + Ax + B$ باشد آنگاه می توان از y نسبت به x مشتق گرفته و نوشت $2yy' = 3x^2 + A$

بطور مشابه می توانیم از تابع گویای $f(x,y)$ نسبت به x مشتق بگیریم:

$$\frac{d}{dx}f(x,y) = f_x(x,y) + f_y(x,y)$$ که در آن f_x و f_y مشتقات جزئی هستند.

لم

فرض کنید E خم بیضوی $y^2 = x^3 + Ax + B$ باشد. نقطه ثابت (u,v) راروی E درنظر می گیریم. فرض می کنیم $(x,y) + (u,v) = (f(x,y) + g(x,y))$ که در آن $f(x,y)$ و $g(x,y)$ توابع گویا از x و y (با ضرایب (u,v)) هستند و y بعنوان تابع به x وابسته است که در معادله زیر صدق می کند $\frac{dy}{dx} = \frac{3x^2+A}{2y}$ آنگاه داریم $\frac{\frac{d}{dx}f(x,y)}{g(x,y)} = \frac{1}{y}$

نکته

لم فوق بیان می کند که دیفرانسیل $\frac{dx}{y}$ یک تبدیل پایاست.

لم

فرض کنید $\alpha_1, \alpha_2, \alpha_3$ درونریختی های ناصفر از خم بیضوی E باشند که $\alpha_1 + \alpha_2 = \alpha_3$ فرض کنیم

$$\alpha_j(x,y) = \left(R_{\alpha_j}(x), yS_{\alpha_j}(x)\right)$$

فرض کنیم C_{α_1} و C_{α_2} موجود باشند بطوریکه $\frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = C_{\alpha_2}$ و $\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = C_{\alpha_1}$ آنگاه

$$\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = C_{\alpha_1} + C_{\alpha_2}$$

نکته

طبق نکته قبلی $\alpha \circ (\frac{dx}{y})$ یک تبدیل دیفرانسیل پایا در E است لذا ضرب اسکالر $C_\alpha \, dx/y$ از dx/y را داریم. یعنی هر درون ریختی ناصفر در فرضیات قضیه ۲.۲۶ صدق می کند.

قضیه ۲.۲۸

فرض کنید E یک خم بیضوی باشد که روی میدان K تعریف شده است و فرض کنید n یک عدد صحیح ناصفر باشد فرض کنید ضرب توسط n در E با معادله $n(x,y) = \left(R_n(x), yS_n(x)\right)$ داده شده باشد (برای تمام $(x,y) \in E(\overline{K})$ که R_n و S_n توابع گویا هستند) در این صورت $\frac{R_n'(x)}{S_n(x)} = n$

لذا ضرب در n جدا شدنی است اگر و تنها اگر n مضربی از مشخصه p نباشد.

یادآوری

فرض کنیم E یک خم بیضوی باشد که روی میدان متناهی $\mathbb{F}_q$ تعریف می شود. درونریختی فروبینوس φ_q که توسط $\varphi_q(x,y) = (x^q, q^q)$ تعریف می شود. که طبق ۲.۲۰ یک درون ریختی روی E است.

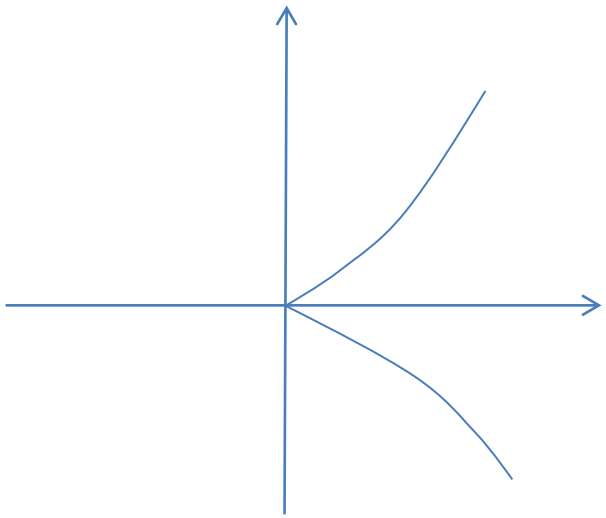
قضیه ۲.۲۹

فرض کنیم E یک خم بیضوی باشد که روی میدان متناهی $\mathbb{F}_q$ تعریف می شود که q توانی از عدد اول p است. فرض کنید r و s اعداد صحیح باشند که هر دو صفر نیستند درونریختی $r\varphi_q + s$ جداشدنی است اگر و تنها اگر $p \nmid s$

خم‌های منفرد

تا حال با خم بیضوی $y^2 = x^3 + Ax + B$ با این فرض که $x^3 + Ax + B$ دارای ریشه های مجزا باشد کار کرده ایم. اما مطالعه حالتی که $x^3 + Ax + B$ دارای ریشه های تکراری باشد جالب خواهد بود.

ابتدا حالتی را بررسی می کنیم که $x^3 + Ax + B$ دارای سه ریشه $x = 0$ را بررسی می کنیم آنگاه معادله خم بصورت $y^2 = x^3$ است. نقطه $(0,0)$ تنها نقطه منفرد این خم است، همچنین نمودار این خم را برای تصور بصورت زیر می توانیم رسم کنیم.



هر خط گذرا از این نقطه خم را در حداکثر یک نقطه دیگر قطع می کند.

اضافه کردن نقطه $(۰,۰)$ به گروه باعث بروز مشکلاتی خواهد شد. لذا ما آن را کنار خواهیم گذاشت. نقاط باقیمانده را با $E_{ns}(K)$ نمایش می دهیم که یک گروه است که قوانین گروهی آن مشابه وقتی است که مکعب دارای ریشه های متمایز بود. تنها چیزی که باید بررسی شود این است که جمع دو نقطه نباید $(۰,۰)$ باشد ولی چون خط گذرا از $(۰,۰)$ خم را حداکثر در یک نقطه قطع می کند خط گذرا از دو نقطه دیگر نمی تواند از $(۰,۰)$ بگذرد.

قضیه ۲.۳۰

فرض کنید E خم بیضوی $y^۲ = x^۳$ و $E_{ns}(K)$ نقاط نامنفرد این منحنی با مختصات در K باشند. که شامل نقطه $\infty = (0:1:0)$ می باشند نگاشت $\varphi: E_{ns}(K) \longrightarrow K$ (K گروه جمعی) با معادله $\varphi((x,y)) = \frac{x}{y}$ و $\varphi(\infty) = ۰$ یک یکریختی گروهی جمعی بین K و $E_{ns}(K)$ است.

اثبات

فرض کنیم $t = \frac{x}{y}$ آنگاه چون $y^۲ = x^۳$ خواهیم داشت $x = (\frac{y}{x})^۲ = \frac{۱}{t^۲}$ و $y = \frac{x}{t} = \frac{۱}{t^۳}$ بنابراین می توان تمام نقاط $E_{ns}(K)$ را توسط t پارامتری کرد

برای اثبات یک بیک بودن کافیست نشان داده شود که $\varphi(\infty) = 0$ و این طبق پارامتری کردن بالا بدیهی است زیرا $t = 0$ متناظر با $(x, y) = \infty$. پس نگاشت بالا یک بیک است.

برای اثبات همریختی فرض می کنیم $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ بایستی نشان دهیم

$$\varphi\big((x_1, y_1) + (x_2, y_2)\big) = \varphi(x_1, y_1) + \varphi(x_2, y_2) \Longrightarrow t_1 + t_2 = t_3$$

همریختی را درحالت های مختلف زیر بررسی می کنیم

$(x_1, y_1) \neq (x_2, y_2)$ آنگاه یا $y_1 \neq y_2$ و $x_1 = x_2$ یا $y_1 = y_2$ و $x_1 \neq x_2$

در حالت $y_1 \neq y_2$ و $x_1 = x_2$ داریم $(x_1, y_1) + (x_2, y_2) = P_1 + P_2 = \infty$ لذا

$\varphi(P_1 + P_2) = \varphi(\infty) = 0$ چون بنابر تقارن داریم $y_1 = -y_2$ پس

$$\varphi(P_1) + \varphi(P_2) = \left(\frac{x_1}{y_1}\right) + \left(\frac{x_2}{y_2}\right) = \left(\frac{x_1}{y_1}\right) + \left(\frac{x_1}{-y_1}\right) = 0$$

در حالت $x_1 \neq x_2$ داریم

$x_3 = m^2 - x_1 - x_2$ و $y_3 = m(x_1 - x_3) - y_1$ بطوریکه $m = \frac{y_2 - y_1}{x_2 - x_1}$

پس با محاسبه روابط فوق خواهیم داشت

$$x_3 = \frac{(y_2 - y_1)^2 - (x_1 + x_2)(x_2 - x_1)^2}{(x_2 - x_1)^2} = \frac{(y_2 - y_1)^2 - x_1^3 - x_2^3 x_1 x_2^2 + x_2 x_1^2}{(x_2 - x_1)^2}$$

با جایگذاری $y_i = t_i^{-3}$ و $x_i = t_i^{-2}$ خواهیم داشت

$$t_3^{-2} = \frac{-2t_1^{-3}t_2^{-3} + t_1^{-2}t_2^{-4} + t_1^{-4}t_2^{-2}}{(t_2^{-1} - t_1^{-1})^2(t_2^{-1} + t_1^{-1})^2} = \frac{t_1^{-2}t_2^{-2}(t_1^{-1} - t_2^{-1})^2}{(t_2^{-1} - t_1^{-1})^2(t_2^{-1} + t_1^{-1})^2}$$

در نتیجه $t_3^{-2} = (t_1 + t_2)^{-2}$

حال برای y_3 داریم

$$-y_3 = m(x_3 - x_1) + y_1 = \frac{(y_2 - y_1)x_3 - (y_2 - y_1)x_1 + (x_2 - x_1)y_1}{x_2 - x_1} = \frac{(y_2 - y_1)x_3 - (y_2)x_1 + (x_2)y_1}{x_2 - x_1}$$

در نتیجه

$$t_3^{-3} = \frac{(t_2^{-3} - t_1^{-3})^2 (t_1 + t_2)^2 - t_1^{-2} t_2^{-3} + t_1^{-3} t_2^{-2}}{(t_2^{-1} - t_1^{-1})(t_2^{-1} + t_1^{-1})} = \frac{t_1^{-2} t_2^{-2} (t_1^{-1} - t_2^{-1})^2}{(t_1 + t_2)/t_1 t_2}$$

$$= -(t_1 + t_2)^{-3}$$

حال اگر از t_3^{-2} و t_3^{-3} نسبت بگیریم خواهیم داشت $t_1 + t_2 = t_3$

در حالتی که $(x_1, y_1) = (x_2, y_2)$ داریم $x_1 = x_2$ و $y_1 = y_2$ در این حالت $x_3 = m^2 - 2x_1$ و

$y_3 = m(x_1 - x_3) - y_1$ که در آنها $m = \frac{3x_1^2}{2y_1}$ (زیرا $y^2 = x^3 \Longrightarrow 2yy' = 3x^2$)

پس اگر $y_1 = 0$ آنگاه داریم $P_1 + P_2 = \infty$ که قبلا بررسی شده است

لذا $y_1 \neq 0$ و داریم

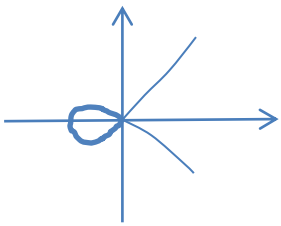
$$x_3 = \frac{4x_1^4 - 8x_1 y_1^2}{4y_1^2} \Longrightarrow t_3^{-2} = \frac{9t_1^{-8} - 8t_1^{-2} t_1^{-6}}{4t_1^{-6}} = \frac{1}{4} t_1^{-2}$$

$$y_3 = \frac{3x_1^3}{2y_1} - \frac{3x_1^3}{8y_1} - y_1 = \frac{9x_1^3 - 8y_1^2}{8y_1} \Longrightarrow t_3^{-3} = \frac{1}{8} t_1^{-3}$$

در نتیجه با توجه به روابط بالا خواهیم داشت $t_3 = 2t_1 = t_1 + t_2$

نکته

در حالتی که خم بیضوی E دارای ریشه مضاعف دوگانه است معادله منحنی بصورت $y^2 = x^3 + x^2$ است و نموداری به فرم زیر دارد



اگر ریشه های مضاعف را صفر بگیریم معادله خم را می توان بصورت $y^2 = x^2(x + a)$ نوشت که در آن $a \neq 0$ و $(0,0)$ تنها نقطه منفرد E است همانند قبل $E_{ns}(K)$ را نقاط نامنفرد E با مختصات در K فرض می کنیم. معمولا معادله بالا را بصورت $(\frac{y}{x})^2 = (x + a)$ نمایش مید هیم. وقتی x به صفر نزدیک می شود سمت راست معادله بالا به سمت a میل می کند لذا برای خم E داریم $(\frac{y}{x})^2 = a$ یا $\frac{y}{x} = \pm a$ (در نزدیکی $x = 0$) یعنی دو مماس در نقطه $(0,0)$ برابر $y = -ax$ و $y = ax$ می باشد.

قضیه ۲.۳۱

فرض کنید E خم $y^2 = x^2(x+a)$ با $0 \neq a \in K$ باشد فرض کنید $E_{ns}(K)$ نقاط نامنفرد E با مختصات در K باشند و فرض کنید $\alpha^2 = a$

نگاشت زیر را در نظر بگیرید $\psi: (x,y) \longmapsto \frac{y+\alpha x}{y-\alpha x}$ و $\infty \longmapsto 1$

۱-اگر $\alpha \in K$ آنگاه ψ یک یکریختی از $E_{ns}(K)$ به $K^\times$ (گروه ضربی K) می باشد

۲-اگر $\alpha \notin K$ آنگاه ψ یکریختی زیر را نتیجه میدهد

$$E_{ns}(K) \equiv \{u + \alpha v \mid u, v \in K\ , u^2 + av^2 = 1\}$$

که در آن عبارت سمت راست گروه ضربی است.

تمرینات فصل دوم

۱- (a) نشان دهید قسمت ثابت یک چند جمله ای درجه ۳ برابر منفی حاصلضرب ریشه هاست.
(b) با استفاده از قسمت اول فرمولی برای جمع دو نقطه P_1 و P_2 وقتی $x_1 \neq x_2$ بدست آورید.

جواب:

(a):

فرض کنیم a و b و c سه ریشه مکعب $x^3 + rx^2 + sx + t$ باشد در این صورت داریم

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc$$

لذا حکم برقرار است.

(b):

جمع دو نقطه در کلیه حالت ها در بخش قوانین گروهی بررسی شده (مخصوصا در این حالت)

۲- نقطه $(3,5)$ در خم $E: y^2 = x^3 - 2$ واقع است که این خم روی $\mathbb{Q}$ تعریف می شود. نقطه ای غیر از ∞ بیابید که گویا، غیر صحیح با مختصات در $\mathbb{Q}$ باشد.

جواب:

فرض کنیم $x = 4/3$ در این صورت $y^2 = \left(4/3\right)^3 - 2 = \frac{64}{27} - 2 = \frac{10}{27} \Rightarrow y = \sqrt{\frac{10}{27}}$

نقطه مورد نظر $\left(4/3, \sqrt{\frac{10}{27}}\right)$ می باشد که یک نقطه گویا و غیر صحیح است.

۳- نقاط $P = (2,9)$ و $Q = (3,10)$ و $R = (-4,-3)$ روی خم $E: y^2 = x^3 + 73$ واقعند.
(a): $P + Q$ و $(P + Q) + R$ را محاسبه کنید

(b): $Q+R$ و $P+(Q+R)$ را محاسبه کنید جواب شما برای $P+(Q+R)$ باید با نتایج (a) سازگار باشد با این حال توجه داشته باشید که یک محاسبه در هر دو فرمول مورد استفاده قرار می گیرد (در واقع در این سوال شرکت پذیری جمع گروهی را با مثال نشان می دهیم)

جواب

برای محاسبه $P+Q$ خط گذرا از دو نقطه P و Q را می نویسیم که دارای شیب $m=۱$ می باشد و معادله خط نیز بصورت $y=x+۷$ است با جایگذاری معادله خط در معادله خم خواهیم داشت.

$$(x+۷)^۲=x^۳+۷۳\Rightarrow x^۳-x^۲-۱۴x+۲۴=۰$$

چون دو ریشه را می شناسیم پس $x=۱-x_۱-x_۲=-۴$ و با توجه به معادله خط داریم $y=۳$ پس $(-۴,۳)$ روی منحنی است ولی با توجه به قوانین گروهی ، وارون این نقطه نسبت به محور x را به عنوان حاصل جمع می گیریم پس $P+Q=(-۴,-۳)=R$

حال برای محاسبه $(P+Q)+R$ در واقع $R+R=۲R$ را محاسبه می کنیم.

شیب خط با مشتق گیری ضمنی از معادله خم بدست می آید داریم $۲yy'=۳x^۲\Rightarrow m=y'=\frac{۳x^۲}{۲y}$

پس معادله خط به صورت زیر است $y=-۸(x+۴)-۳\Rightarrow y=-۸x-۳۵$.

با جایگذاری معادله خط در معادله خم (قطع خم و خط) داریم

$$(-۸x-۳۵)^۲=x^۳+۷۳\Rightarrow x^۳--۶۴x^۲+\cdots=۰$$

پس جمع ریشه ها برابر ۶۴ است و چون -۴ ریشه مضاعف است پس $x-۸=۶۴\Rightarrow x=۷۲$. حال با توجه به معادله خم داریم $y=-۶۱۱$ پس $(۷۲,-۶۱۱)$ روی خم قرار دارد و وارون آن برابر حاصل جمع مطلوب است یعنی $(P+Q)+R=R+R=۲R=(۷۲,-۶۱۱)$

(b):

حال به روش مشابه $Q+R$ را محاسبه می کنیم

۴- فرض کنید E خم بیضوی $y^۲=x^۳-۳۴x+۳۷$ باشد. فرض کنید $P=(۱,۲)$ و $Q=(۶,۷)$ در این صورت $P+Q$ را محاسبه کنید و همچنین با توجه به این مطلب که $P\equiv Q\ \ (mod۵)$، $۲P$ را در پیمانه ۵

محاسبه کنید. نشان دهید جواب مشابه $P+Q$ در پیمانه ۵ است. ملاحظه می کنیم چون $P \equiv Q$ فرمول جمع نقاط در پیمانه ۵ با فرمول جمع $P+Q$ برابر نیست. با این حال جواب ها یکسان اند این نشان می دهد که تحویل در پیمانه یک عدد فرد همریختی است.

جواب:

داریم $m=۱$ و $y=x+۱$ پس $(x+۱)^۲=x^۳-۳۴x+۳۷$ لذا $x^۳-x^۲+\cdots=۰$ پس ریشه سوم برابر $x=-۶$ است و با توجه به معادله خم بدست می آوریم $y=-۵$ پس

$$P+Q=(-۶,۵)$$

برای یافتن $۲P$ شیب خط را از طریق مشتق گیری جزئی بدست می آوریم که در پیمانه ۵ خواهیم داشت $m=۱$ پس $y=x+۱$ خط مماس در نقطه $(۱,۲)$ است با قطع خم و خط داریم

$(x+۱)^۲=x^۳-۳۴x+۳۷$ لذا $x^۳-x^۲+\cdots=۰$ پس $x=۱$ و لذا $y=۲$ پس $۲P$

همچنین در پیمانه ۵ داریم $P+P=(۱,-۲)\equiv(۱,۳) \pmod ۵$

$(-۶,۵)=(۱,۳)$ پس حکم برقرار است.

۵- فرض کنید (x,y) نقطه ای روی خم بیضوی E به معادله $y^۲=x^۳+Ax+B$ باشد. نشان دهید اگر $y=۰$ آنگاه $۳x^۲+A\neq۰$ (راهنمایی: شرط این که یک چند جمله ای ریشه مضاعف داشته باشد چیست؟)

جواب:

چون $y=o$ پس $x^۳+Ax+B=۰$ یعنی x ریشه این خم است و چون خم نامنفرد است یعنی دارای ریشه تکراری نیست یعنی اگر x ریشه $x^۳+Ax+B=۰$ باشد ریشه مشتق آن نیست یعنی ریشه $۳x^۲+A$ نیست. پس حکم برقرار است یعنی $۳x^۲+A\neq۰$.

۶- نشان دهید جمع سه نقطه روی خم بیضوی برابر ∞ می شود اگر و تنها اگر این سه نقطه هم خط باشند.

جواب:

فرض کنیم $P_۱$ و $P_۲$ و $P_۳$ سه نقطه روی خم بیضوی باشند که هم خط هستند در این صورت با توجه به خاصیت شرکت پذیری جمع خواهیم داشت $P_۱+P_۲+P_۳=(P_۱+P_۲)+P_۳$ و خط گذرا از دو نقطه $P_۱$ و $P_۲$ از

نقطه سوم $P_۳$ نیز خواهد گذشت پس بنابر خواص جمع گروهی $P_۱ + P_۲ = -P_۳$ پس داریم $P_۱ + P_۲ + P_۳ = (P_۱ + P_۲) + P_۳ = P_۳ - P_۳ = \infty$

برعکس اگر $P_۱ + P_۲ + P_۳ = \infty$ در این صورت بنابرخاصیت شرکت پذیری داریم $P_۱ + P_۲ = -P_۳$ و $P_۲ + P_۳ = -P_۱$. حال استفاده از خاصیت جمع گروهی بیان می کندکه P_i ها هم خط هستند.

۷- فرض کنید C خم $u^۲ + v^۲ = c^۲(۱ + du^۲v^۲)$ باشد. همانند بخش ۲.۶.۳ نشان دهید $(c, ۰)$ دارای مرتبه چهار است

جواب:

بحث مورد نظر همان مختصات ادواردز است و میدانیم در این مختصات جمع نقاط به صورت زیر است.

$$(u_۱, v_۱) + (u_۲, v_۲) = \left(\frac{u_۱v_۲ + u_۲v_۱}{c(۱ + du_۱u_۲v_۱v_۲)}, \frac{v_۱v_۲ - u_۱u_۲}{c(۱ - du_۱u_۲v_۱v_۲)}\right)$$

برای محاسبه $۴c$ ابتدا $۲c$ را محاسبه می کنیم زیرا $۴c = ۲c + ۲c$. پس طبق فرمول بالا خواهیم داشت.

$$(c, ۰) + (c, ۰) = \left(۰, \frac{-c^۲}{c}\right) = (۰, -c)$$

$$۴c = ۲c + ۲c = (۰, -c) + (۰, -c) = \left(۰, \frac{c^۲}{c}\right) = (۰, c)$$

لذا حکم برقرار است.

۸- نشان دهید روش بخش ۲.۱ واقعا kP را محاسبه می کند (راهنمایی: با استقرا روی طول بسط دوتایی k ثابت کنید)

اثبات:

طبق راهنمایی با استقرا مسئله را ثابت می کنیم. طول بسط دوتایی k را برابر l درنظر می گیریم و روی l استقرا می بندیم یعنی فرض کنیم که l عدد صحیحی باشد که $۲^l \leq k \leq ۲^{l+۱}$. فرض کنیم $l = ۰$ در این صورت $k = ۱$ پس $۱ \times ۲^۰ = ۱$

فرض کنیم حکم برای مقادیر کمتر از l برقرار باشد یعنی $k' = k_. + ۲k_۱ + \cdots + ۲^{l-۱}a_{l-۱}$ حال برای l ثابت می کنیم چون $۲^l \leq k \leq ۲^{l+۱}$ پس $k - ۲^l \leq ۲^l$ پس طبق فرض استقرا خواهیم داشت.
$k = k_. + ۲k_۱ + \cdots + ۲^{l-۱}a_{l-۱} + ۲^l$ در نتیجه $k - ۲^l = k_. + ۲k_۱ + \cdots + ۲^{l-۱}a_{l-۱}$

پس حکم برقرار است.

۹- اگر $P = (x, y) \neq \infty$ روی خم باشد آنگاه نشان دهید $-P = (x, -a_۱x - a_۳ - y)$ که $-P$ نقطه اشتراک خط عمودی و خم است

جواب:

خطی که از نقطه $(x_., y_.)$ و ∞ می گذرد $x = x_.$ است. پس با جایگذاری در معادله خم داریم

$$y^۲ + a_۱x_.y + a_۳y = x_.^۳ + a_۲x_.^۲ + a_۴x_. + a_۶$$

$$y^۲ + a_۱x_.y + a_۳y = y_.^۲ + a_۱x_.y_. + a_۳y_.$$

$$\Rightarrow y^۲ - y_.^۲ = (a_۱x_. + a_۳)(y - y_.)$$

$$\Rightarrow (y - y_.)(y + y_.) = (a_۱x_. + a_۳)(y - y_.) \Rightarrow (y + y_.) = -(a_۱x_. + a_۳)$$

$$\Rightarrow y = -a_۱x_. - a_۳ - y_.$$

پس حکم برقرار است.

۱۰-فر ض کنید $\mathbb{R}$ اعداد حقیقی باشد نشان دهید نگاشت $(x, y, z) \longmapsto (x: y: z)$ یک نگاشت دو به یک از کره $x^۲ + y^۲ + z^۲ = ۱$ در $\mathbb{R}^۳$ به $P^۲_{\mathbb{R}}$ می دهد. چون کره فشرده است پس $P^۲_{\mathbb{R}}$ تحت توپولوژی القایی از از کره فشرده است.

جواب:

چون نگاشت $(x, y, z) \longmapsto (x: y: z)$ فقط دو مقدار (x, y, z) و $(-x, -y, -z)$ را به $(x: y: z)$ می برد

فصل سوم: نقاط تاب

در یک جمله می توان گفت نقاط تاب یعنی نقاطی که مرتبه متناهی دارند این نقاط در مطالعه خم های بیضوی نقش مهمی دارند. در بخش ۴ نشان داده خواهد شد که تمام نقاط E روی میدان متناهی K تاب هستند.

نقاط تاب

تعریف

فرض کنید E یک خم بیضوی باشد که روی میدان K تعریف شده است. فرض کنید n یک عدد صحیح مثبت باشد در این صورت مجموعه $E[n]$ را بصورت زیر تعریف می کنیم $E[n] = \{p \in E(\overline{K}) | np = ۰\}$

تاکید می کنیم که $E[n]$ دارای نقاطی با مختصات در $\overline{K}$ و نه صرفا در K می باشد.

مثال

وقتی مشخصه میدان ۲ باشد E را می توان به‌فرم $y^۲ = cubic$ نوشت. در این صورت تعیین $E[۲]$ کار مشکلی نخواهد بود. فرض کنید $y^۲ = (x - e_۱)(x - e_۲)(x - e_۳)$ باشد که $e_۱, e_۲, e_۳ \in \overline{K}$ نقطه P در رابطه $۲P = \infty$ صدق می کند اگرو تنها اگر خط مماس در نقطه P عمودی باشد. یعنی $y = ۰$ لذا $E[۲] = \{\infty, (e_۱, ۰), (e_۲, ۰), (e_۳, ۰)\}$ و $E[۲]$ گروهی است که با $\mathbb{Z}_۲ \oplus \mathbb{Z}_۲$ یکریخت است.

یادآوری و مثال

در فصل دوم نشان داده شد که خم بیضوی E را می توان به یکی از دو فرم زیر نوشت:

$$(۱): y^۲ + xy + x^۳ + a_۲x^۲ + a_۶ = ۰ \ , \ \ (۲): y^۲ + a_۳y + x^۳ + a_۴x + a_۶ = ۰$$

در حالت اول $a_۶ \neq ۰$ و در حالت دوم $a_۳ \neq ۰$ (زیرا در غیر این صورت خم ها منفرد خواهند شد)

اگر $P = (x, y)$ نقطه ای از مرتبه ۲ باشد آنگاه مماس بر P باید عمودی باشد و این یعنی مشتقات جزیی نسبت به y باید صفر باشد.

در حالت اول این یعنی $x = ۰$ که با جایگذاری آن در معادله اول خواهیم داشت

$y^2 = x^3 + a_4 = (y + \sqrt{a_4})^2$ لذا $(0, \sqrt{a_4})$ تنها نقطه از مرتبه می باشد و چون ریشه دوم در مشخصه ۲ منحصر به فرد است پس $E[2] = \{\infty, (0, \sqrt{a_4})\}$ که گروهی است که با گروه $\mathbb{Z}_2$ یکریخت است.

مباحث فوق را در قضیه زیر خلاصه می کنیم

قضیه ۳.۱

فرض کنید E یک خم بیضوی روی میدان K باشد اگر مشخصه میدان ۲ نباشد آنگاه $E[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ و اگر مشخصه میدان ۲ باشد آنگاه $E[2] \cong \mathbb{Z}_2$ یا $E[2] \cong 0$

مثال

حال $E[3]$ را بررسی می کنیم

ابتدا فرض کنیم مشخصه میدان ۲ یا ۳ نباشد لذا E را می توان بصورت $y^2 = x^3 + Ax + B$ بیان کرد.

نقطه P در رابطه $3P = \infty$ صدق می کند اگر و تنها اگر $2P = -P$ یعنی مختصات x نقطه $2P$ با مختصات x نقطه P برابر است (و مختصات y همانند همین است ولی از لحاظ علامت متفاوت خواهد بود زیرا اگر مختصات y برابر باشد رابطه $2P = P$ نتیجه میدهد $P = \infty$)

لذا $m^2 - 2x = x$ که $m = \frac{3x^2 + A}{2y}$ با استفاده از $y^2 = x^3 + Ax + B$ خواهیم داشت

$$(3x^2 + A)^2 = 12x(x^3 + Ax + B) \Longrightarrow 3x^4 + 6Ax^2 + 12Bx - A^2 = 0$$

مبین چند جمله ای اخیر $-6912(4A^3 + 27B^2)^2$ می باشد که ناصفر است.

پس چند جمله ای دارای ریشه چندگانه نیست لذا چهار مقدار مجزا برای x (در $\overline{K}$) وجود دارد و هر x دو y را نتیجه می دهد. پس ما ۸ نقطه از مرتبه ۳ خواهیم داشت. و چون ∞ نیز عضوی از $E[3]$ است مشاهده می کنیم که $E[3]$ گروهی با ۹ عنصر است که هر عنصر آن ۳- تاب هستند. یعنی $E[3] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$

حالتی که مشخصه میدان ۲ باشد در تمرین ۳.۲ بررسی می شود

حال به مشخصه ۳ می رسیم. می توانیم فرض کنیم E به فرم $y^2 = x^3 + a_2x^2 + a_4x + a_6$ است. بطور مشابه مختصات x برای $2P$ برابر با مختصات x برای P است. با روال معمول مختصات x را برای $2P$

محاسبه کرده و آن را بجای مختصات x برای P جایگذاری می کنیم. برخی از مراحل محاسبات از بین خواهد رفت زیرا $۳x = ۰$ با محاسبات خواهیم داشت $\left(\frac{۲a^{۲}x+a_{۴}}{۲y}\right)^{۲} - a_{۲} = ۰$ چون $۴ = ۱$ نتیجه می گیریم $a_{۲}x^{۳} + a_{۲}a_{۶} - a_{۴}^{۲} = ۰$ توجه می کنیم که $a_{۲} = a_{۶} = ۰$ درست نیست زیرا در این صورت $x^{۳} + a_{۶} = (x + a_{۶}^{۱/۳})^{۳}$ دارای ریشه های چند گانه خواهد بود پس حداقل یکی از $a_{۲}$ یا $a_{۶}$ بایستی مخالف صفر باشند.

اگر $a_{۲} = ۰$ خواهیم داشت $-a_{۴}^{۲} = ۰$ که نمی تواند اتفاق بیفتد پس x دارای هیچ مقداری نیست لذا $E[۳] = \{\infty\}$

اگر $a_{۲} \neq ۰$ معادله ای به فرم $a_{۲}(x^{۳} + a)$ بدست می آوریم که دارای ریشه سه تایی منفرد در مشخصه ۳ می باشد.

لذا برای x یک مقدار موجود است و دو مقدار نیز متناظر با y است. که دو نقطه از مرتبه ۳ را بدست می دهد. و چون ∞ نقطه ای است که همواره وجود دارد لذا $E[۳]$ از مرتبه ۳ می باشد و در نتیجه $E[۳] \cong \mathbb{Z}_{۳}$

قضیه ۳.۲

فرض کنید E یک خم بیضوی روی میدان K و n یک عدد صحیح مثبت باشد اگر $p \nmid n$ (که p مشخصه میدان است) یا مشخصه صفر باشد آنگاه $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$

اگر $p \mid n$ و n را بصورت $n = p^r n'$ بنویسیم که $p \nmid n'$. آنگاه
$E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ or $\mathbb{Z}_n \oplus \mathbb{Z}_{n'}$

اثبات

(با ذکر این نکته که مقدمات مربوط به اثبات این قضیه در بخش بعدی یعنی چندجمله ای های تقسیم ارائه می شود ولی بخاطر حفظ ترتیب اثبات را همین جا می آوریم)

اگر $\alpha(x, y) = \big(R(x), yS(x)\big)$ یک درونریختی از خم بیضوی E باشد آنگاه α جداشدنی است هرگاه $R'(x)$ متحد با صفر نباشد

حالت اول:

فرض کنید n ضریبی از مشخصه میدان یعنی p نباشد طبق قضیه ۳.۶ نگاشت ضرب توسط n دارای $R(x) = \frac{x^{n^2}+\cdots}{n^2 x^{n^2-1}+\cdots}$ است که مشتق مخرج $n^2 x^{2n^2-2} + \cdots \neq 0$ است پس ضرب توسط n یعنی α جداشدنی است.

طبق نتیجه ۳.۷ و قضیه ۲.۲۱، $E[n]$ (هسته ضرب توسط n یعنی α) دارای مرتبه n^2 است پس $deg\alpha =$
n^2 قضیه ساختاری برای گروه های آبلی بیان می کند $E[n] \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_k}$

که $n_i \mid n_{i+1}$ (برای تمام i ها)

فرض کنید l عدد اولی باشد که n_1 را عاد می کند پس برای تمام i ها $l \mid n_i$

(توجه داریم که بنابر تعریف $E[n]$ داریم $E[n] = \{p \in E(\overline{K}) | np = 0\} = ker\alpha$ در نتیجه

$(\#E[n] = \#ker\alpha \implies \#E[n] = n^2)$

یعنی $E[l] \subseteq E[n]$ دارای مرتبه l^k است.

همانند اثبات برای $E[n]$، $E[l]$ دارای مرتبه l^2 است لذا باید $k = 2$ لذا $E[n] \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ پس
$n_2 \mid n$ و چون $n^2 = \#E[n] = n_1 n_2$ لذا $n_1 = n_2 = n$ پس $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$

حالت دوم:

فرض کنیم $p \mid n$ (p مشخصه میدان است) با توجه به گزاره ۲.۲۸ (که بیان می کند: فرض کنید E یک خم بیضوی باشد که روی میدان K تعریف شده است و فرض کنید n یک عدد صحیح ناصفر باشد فرض کنید ضرب بوسیله n در E توسط $n(x,y) = \big(R_n(x), yS_n(x)\big)$ داده شده باشد (برای تمام $(x,y) \in E(\overline{K})$ که R_n و S_n توابع گویا هستند در این صورت $\frac{R_n'(x)}{S_n(x)} = n$

لذا ضرب در n جدا شدنی است اگر و تنها اگر n مضربی از مشخصه p نباشد.)

نتیجه می شود pP جداشدنی نیست $(P \in E(\overline{K}))$

طبق قسمت دوم ۲.۲۱ (که بیان می کند: فرض کنید α یک درونریختی جداشدنی از خم بیضوی E باشد که در آن $\ker(\alpha)$ هسته همریختی $\alpha: E(\overline{K}) \longrightarrow E(\overline{K})$ می باشد. اگر α جدا شدنی نباشد آنگاه $deg\alpha > \#\ker(\alpha)$) و بنابر اثبات حالت اول $\#kerpP = \#E[p]$ بطوریکه تعداد اعضای $E[p]$ کمتر از درجه

درونریختی pP است. بنابر ۳.۷ درجه درونریختی pP برابر p^2 می باشد از طرفی هر عضو $E[p]$ از مرتبه ۱ یا p می باشد پس مرتبه $E[p]$ توانی از p است و چون بطور اکید کمتر از p^2 است پس مرتبه $E[p]$ برابر ۱ یا p می باشد پس $E[p] = \infty$ در این صورت برای هر k خواهیم داشت

$E[p^k] = \{\infty\}$ اگر مرتبه $E[p]$ برابر p باشد در این صورت ادعا می کنیم که برای هر k،

$$E[p^k] \cong \mathbb{Z}_{p^k}$$

برای اثبات ادعا نشان می دهیم که $E[p^k]$ از مرتبه p^k است $(p^j P = \infty)$

فرض کنیم نقطه P از مرتبه p^j باشد با توجه به قضیه ۲.۲۲، $pP: E(\bar{K}) \longrightarrow E(\bar{K})$ پوشاست پس $Q \in E(\bar{K})$ هست که $pQ = P$ لذا $p^j Q = p^{j-1} P \neq \infty$ پس $p^{j+1} Q = p^j P = \infty$ یعنی مرتبه Q برابر p^{j+1} است. با توجه به بحث بالا به استقرا معلوم می شود که به ازای هر k می توان عنصری از مرتبه p^k ساخت بنابراین $E[p^k]$ دوری از مرتبه p^k می باشد.

این اثبات ادعا را کامل می کند.

n را بصورت $n = p^r n'$ که $r \geq 0$ و $p \nmid n'$ تجزیه می کنیم آنگاه $E[n] = E[n'] \oplus E[p^r]$ *

چون $p \nmid n'$ پس بنابر حالت اول $E[n'] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ چون $(p^r, n') = 1$ داریم

$$\mathbb{Z}_{n'} \oplus \mathbb{Z}_{p^r} = \mathbb{Z}_{n' p^r} = \mathbb{Z}_n$$

اگر $E[p^r] = \infty$ بنابر * داریم $E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$

اگر $E[p^r] \cong \mathbb{Z}_{p^r}$ آنگاه بنابر * داریم $E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \oplus \mathbb{Z}_{p^r} \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n' p^r} \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_n$

تعریف

خم بیضوی E از مشخصه p را معمولی نامیم هرگاه $E[p] \cong \mathbb{Z}_p$

و هرگاه $E[p] \cong 0$ باشد آنگاه این خم بیضوی را فوق منفرد می نامیم

تذکر

واژه فوق منفرد هیچ ارتباطی با واژه منفرد (تاثیر نقاط بدرفتار روی E) ندارد

نکته

فرض کنید n یک عدد صحیح مثبت باشد که بر مشخصه میدان K بخش پذیر نیست یک پایه$\{\beta_1, \beta_2\}$، برای $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ برمی گزینیم. یعنی هر عنصر $E[n]$ بصورت $m_1\beta_1 + m_2\beta_2$ بیان می شود که m_1 و m_2 اعداد صحیح هستند.

فرض کنید $\alpha: E(\bar{K}) \longrightarrow E(\bar{K})$ همریختی باشد پس α، $E[n]$ را به $E[n]$ می نگارد. یعنی $a, b, c \in \mathbb{Z}_n$ موجودند بطوریکه $\alpha(\beta_1) = a\beta_1 + c\beta_2$ و $\alpha(\beta_2) = b\beta_1 + d\beta_2$ لذا همریختی $\alpha: E(\bar{K}) \longrightarrow E(\bar{K})$ توسط ماتریس ۲ × ۲، $\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ نمایش داده می شود.

ترکیب همریختی ها بصورت ترکیب ماتریس های متناظر می باشد.

مثال

فرض کنید E یک خم بیضوی باشد که روی $\mathbb{R}$ تعریف شده و $y^2 = x^3 + Ax + B$ و فرض کنید $n = 2$ در این صورت $E[2] = \{\infty, (2^{1/3}, 0), (\xi 2^{1/3}, 0), (\xi^2 2^{1/3}, 0)\}$ که در آن ξ ریشه سوم واحد است.

فرض کنید $\beta_1 = (2^{1/3}, 0)$ و $\beta_2 = (\xi 2^{1/3}, 0)$ در این صورت $\{\beta_1, \beta_2\}$ پایه ای برای $E[2]$ می باشد و $\beta_3 = (\xi^2 2^{1/3}, 0) = \beta_1 + \beta_2$

مثال

فرض کنید $\alpha: E(\mathbb{C}) \longrightarrow E(\mathbb{C})$ مختلط مزدوج $\alpha(x, y) = (\bar{x}, \bar{y})$ باشد.

براحتی نشان داده می شود که α همریختی است در واقع چون تمام مضارب در فرمول قانون گروه ها حقیقی هستند خواهیم داشت $\overline{P_1} + \overline{P_2} = \overline{P_1 + P_2}$

یعنی $\alpha(P_1) + \alpha(P_2) = \alpha(P_1 + P_2)$

داریم $\alpha(\beta_1) = 1.\beta_1 + 0.\beta_2$ و $\alpha(\beta_2) = 1.\beta_1 + 1.\beta_2$ پس ماتریس $\alpha_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ را خواهیم داشت. توجه داریم که $\alpha \circ \alpha$ همانی خواهد شد.

چندجمله‌ای‌های‌تقسیم

هدف از این بخش فراهم سازی مقدمات مربوط به قضیه ۳.۲ است همچنین برخی نتایج مورد نیاز برای اثبات های بخش ۴.۲ بدست خواهد آمد.

برای مطالعه زیرگروه های تابی به مطالعه نگاشتهای یک خم بیضوی که توسط ضرب عدد صحیح داده می شود می پردازیم

برای درونریختی ها که توسط توابع گویا داده می شوند بایستی فرمولی ارائه دهیم برای این منظور با متغیر های A و B شروع می کنیم

تعریف

چند جمله ای تقسیم $\psi_m \in \mathbb{Z}[x, y, A, B]$ را بصورت زیر تعریف می کنیم.

$$\psi_{۰} = ۰$$

$$\psi_{۱} = ۱$$

$$\psi_{۲} = ۲y$$

$$\psi_{۳} = ۳x^{۴} + ۶Ax^{۲} + ۱۲Bx - A^{۲}$$

$$\psi_{۴} = ۴y(x^{۶} + ۵Ax^{۴} + ۲۰Bx^{۳} - ۵A^{۲}x^{۲} - ۴ABx - ۸B^{۲} - A^{۳})$$

$$\psi_{۲m+۱} = \psi_{m+۲}{\psi_m}^{۳} - \psi_{m-۱}\psi_{m+۱} \qquad for\ m \geq ۲$$

$$\psi_{۲m} = (۲y)^{-۱}(\psi_m)(\ \psi_{m+۲}{\psi_{m-۱}}^{۲} - \psi_{m-۲}{\psi_{m+۱}}^{۲}) \qquad for\ m \geq ۳$$

لم ۳.۳

اگر n فرد باشد ψ_n یک چند جمله ای در $\mathbb{Z}[x, y^2, A, B]$ است و اگر n زوج باشد ψ_n یک چند جمله ای در $۲y\mathbb{Z}[x, y^2, A, B]$ است.

اثبات

حذف

تعریف

چند جمله ای های زیر را تعریف می کنیم

$$\varphi_m = x\psi_m{}^{۲} - \psi_{m+۱}\psi_{m-۱}$$

$$\omega_m = (۴y^{-۱})(\psi_{m+۲}\psi_{m-۱}{}^{۲} - \psi_{m-۲}\psi_{m+۱}{}^{۲})$$

لم ۳.٤

برای تمام n ها داریم $\varphi_n \in \mathbb{Z}[x, y, A, B]$. و اگر n فرد باشد ω_n یک چند جمله ای در $y\mathbb{Z}[x, y^2, A, B]$ است و اگر n زوج باشد آنگاه ω_n یک چند جمله ای در $\mathbb{Z}[x, y^2, A, B]$ است

اثبات

حذف

لم ۳.۵

$\varphi_n(x) = x^{n^{۲}} +$ چند جمله ای های با درجه کمتر

$\psi_n^{۲}(x) = n^{۲}x^{n^{۲}-۱} +$ چند جمله ای های با درجه کمتر

اثبات

حذف

قضیه ۳.٦

فرض کنید $P = (x, y)$ یک نقطه روی خم بیضوی $y^{۲} = x^{۳} + Ax + B$ (روی میدانی که مشخصه آن ۲ نیست) باشد و فرض کنید n یک عدد صحیح مثبت باشد آنگاه $nP = \left(\frac{\varphi_n(x)}{\psi_n^{۲}(x)}, \frac{\omega_n(x,y)}{\omega_n(x,y)^{۳}}\right)$

اثبات

در بخش ۹.۵ آمده است

قضیه ۳.۷

فرض کنید E یک خم بیضوی باشد. درونریختی که در قضیه بالا داده شد (یعنی درون ریختی ضرب توسط n) دارای درجه n^2 است.

اثبات

حذف

در واقع لم های فوق ابزاری برای اثبات قضیه ۳.۲ بودند که در این بخش بیان شدند

جفت‌سازی Weil

جفت سازی ویل نقش عمده ای در مطالعه خم های بیضوی در n- تابها دارد یک نمونه از کاربرد آن در اثبات لم هس (تعداد نقاط خم بیضوی روی میدان متناهی) می باشد.

تعریف

فرض کنید E یک خم بیضوی روی میدان K باشد و n عدد صحیحی باشد که مشخصه میدان آن را عاد نمی کند آنگاه $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. فرض کنید $\mu_n = \{x \in \overline{K} | x^n = 1\}$ گروه ریشه های nام واحد در $\overline{K}$ باشد چون مشخصه میدان n راعاد نمی کند معادله $x^n = 1$ دارای ریشه چندگانه نیست لذا دارای n ریشه در $\overline{K}$ است. بنابراین μ_n گروه دوری از مرتبه n است. هر مولد ξاز μ_n را ریشه nام اولیه می نامیم. بطور معادل $\xi^k = 1$ اگر و تنها اگر $n \mid k$

تعریف و قضیه ۳.۹

فرض کنید E یک خم بیضوی روی میدان K باشد و n عدد صحیحی باشد که مشخصه میدان آن را عاد نمی کند آنگاه یک جفت $e_n : E[n] \times E[n] \longrightarrow \mu_n$ بنام جفت سازی ویل موجود است که در شرایط زیر صدق می کند

۱- e_n نسبت به هر یک از متغیرها دو خطی است. یعنی

$$e_n(S_1 + S_2, T) = e_n(S_1, T) + e_n(S_2, T)$$

$$e_n(S, T_1 + T_2) = e_n(S, T_1) + e_n(S, T_2)$$

برای تمام نقاط $S, S_1, S_2, T, T_1, T_2 \in E[n]$

۲- e_n نسبت به هر یک از متغیرها ناتباهیده است یعنی اگر برای تمام $T \in E[n]$ داشته باشیم $e_n(S,T) = ۱$ آنگاه $S = \infty$ و همچنین اگر برای تمام $S \in E[n]$ داشته باشیم $e_n(S,T) = ۱$ آنگاه $T = \infty$

۳- برای تمام نقاط $T \in E[n]$ داریم $e_n(T,T) = ۱$

٤- برای تمام نقاط $S,T \in E[n]$ داریم $e_n(S,T) = e_n(T,S)^{-۱}$

٥- برای تمام خودریختی های σ از $\overline{K}$ بطوریکه σ نگاشت همانی با ضرایب در K باشد (اگر E در فرم وایرشتراس باشد و این یعنی $\sigma(A) = A \ , \sigma(B) = B$) داریم $e_n(\sigma S, \sigma T) = \sigma(e_n(S,T))$

٦- برای تمام درونریختی های جداشدنی α از E داریم $e_n(\alpha(S), \alpha(T)) = e_n(S,T)^{deg\alpha}$ اگر ضرایب E در میدان متناهی $\mathbb{F}_q$ قرار گیرند آنگاه گزاره فوق برای حالتی که α درون ریختی فروبینوس باشد نیز برقرار است (در واقع گزاره برای تمام درونریختی های جداشدنی و جدانشدنی برقرار است [۳.۸] را ببینید.)

نتنجه ۳.۱۰

فرض کنید $\{T_۱, T_۲\}$ پایه ای برای $E[n]$ باشند. آنگاه $e_n(T_۱, T_۲)$ یک ریشه n– ام اولیه است.

اثبات

فرض کنید $e_n(T_۱, T_۲) = \xi$ که درآن $\xi^d = ۱$ آنگاه $e_n(T_۱, dT_۲) = ۱$ همچنین طبق قسمت های اول و سوم قضیه قبل $e_n(T_۱, dT_۲) = e_n(T_۱, T_۲)^d = ۱$

فرض کنید $S \in E[n]$ آنگاه برای اعداد صحیح a,b خواهیم داشت $S = aT_۱ + bT_۲$ بنابراین
$e_n(S, dT_۲) = e_n(T_۱, dT_۲)^a e_n(T_۲, dT_۲)^b = ۱$

چون این عبارت برای تمام S ها برقرار است پس با توجه به قسمت دوم قضیه قبل خواهیم داشت $dT_۲ = \infty$.

چون $dT_۲ = \infty$ اگر و تنها اگر $n \mid d$ نتیجه می گیریم که ξ یک ریشه n– ام اولیه است.

نتیجه ۳.۱۱

اگر $E[k] \subseteq E[n]$ آنگاه $\mu_n \subseteq K$

نتیجه ۳.۱۲

فرض کنیم E یک خم بیضوی باشد که روی $\mathbb{Q}$ تعریف شده باشد آنگاه برای $n \geq ۳$، $E[n] \nsubseteq E[\mathbb{Q}]$

یادآوری

وقتی $n = ۲$ ممکن است $E[۲] \subseteq E[\mathbb{Q}]$. برای مثال اگر E توسط $y^۲ = x(x-۱)(x+۱)$ داده شده باشد آنگاه $E[۲] = \{\infty, (۰,۰), (۱,۰), (-۱,۰)\}$

اگر $n = ۳,۴,۵,۶,۷,۸,۹,۱۰,۱۲$ آنگاه خم E روی $\mathbb{Q}$ هست که نقاط آن دارای مرتبه n و مختصات گویا هستند. هر چند نتیجه بیان می کند که این برای تمام نقاط از مرتبه n که دارای مختصات گویا هستند برقرار است ولی برای $n = ۲$ نتیجه برقرار نیست.

حال از جفت سازی ویل برای بدست آوردن دو قضیه که در اثبات قضیه هس نقش دارند استفاده خواهیم کرد. یادآوری می کنیم که اگر α یک درون ریختی از خم بیضوی E باشد آنگاه ماتریس $\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ با مولفه های در $\mathbb{Z}_n$، اثر α بر پایه $\{T_۱, T_۲\}$ از $E[n]$ را نشان می دهد.

قضیه ۳.۱۵

فرض کنید α یک درونریختی از خم بیضوی E روی میدان K باشد. فرض کنید n عدد صحیح مثبتی باشد که توسط مشخصه میدان عاد نمی شود. آنگاه $det(\alpha_n) \equiv deg(\alpha) \pmod n$

اثبات

طبق نتیجه ۳.۱۰، $e_n(T_۱, T_۲) = \xi$ یک ریشه n- ام اولیه است طبق قسمت ۶ از قضیه ۳.۹ داریم

$$\xi^{deg(\alpha)} = e_n(\alpha(T_۱), \alpha(T_۲)) = e_n(aT_۱ + cT_۲, bT_۱ + dT_۲) =$$
$$e_n(T_۱, T_۱)^{ab} e_n(T_۱, T_۲)^{ab} e_n(T_۲, T_۱)^{cb} e_n(T_۲, T_۲)^{cd} = \xi^{ad-bc}$$

چون ξ یک ریشه n- ام اولیه است پس $deg(\alpha) \equiv ad - bc \pmod n$

تعریف

فرض کنید α, β درونریختی های از E و a, b اعداد صحیح باشند. درونریختی $a\alpha + b\beta$ را بصورت زیر تعریف می کنیم $(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P)$ که در آن $a\alpha(P)$ همان ضرب عنصر $\alpha(P)$ توسط a در E می باشد

قضیه ۳.۱۶

$$deg(a\alpha + b\beta) = a^{۲}deg(\alpha) + b^{۲}deg(\beta) + ab\left(deg(\alpha + \beta) - deg(\alpha) - deg(\beta)\right)$$

جفت‌سازی Tate - lichtenbaum

قضیه ۳.۱۷

فرض کنید E یک خم بیضوی روی $\mathbb{F}_q$ باشد فرض کنید n عدد صحیحی باشد که $n \mid q - ۱$.

عناصر از مرتبه n، $E(\mathbb{F}_q)$ را با $E(\mathbb{F}_q)[n]$ نمایش می دهیم. فرض کنید $\mu_n = \{x \in \mathbb{F}_q | x^n = ۱\}$

و فرض کنید $R \in E(\overline{\mathbb{F}_q})$, $P \in E(\mathbb{F}_q)[n], Q \in E(\mathbb{F}_q)$ طوری انتخاب شوند که $nR = Q$.

e_n نشان دهنده n- امین جفت سازی ویل و $\varphi = \varphi_q$ نشان دهنده q- امین توان درونریختی فروبینیوس باشد. تعریف می کنیم $\tau_n(P, Q) = e_n(P, R - \varphi(R))$ در این صورت

$\tau_n: E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \longrightarrow \mu_n$ یک جفت سازی دو خطی ناتباهیده و البته خوش تعریف است.

این جفت سازی را جفت سازی تعدیل یافته **Tate – lichtenbaum** نامیده می شود.

جفت سازی اصلی **Tate – lichtenbaum** روی ریشه n- ام τ_n بصورت زیر تعریف می شود.

$$\langle \cdot, \cdot \rangle_n: E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \longrightarrow {\mathbb{F}_q}^{\times}/({\mathbb{F}_q}^{\times})^n$$

فصل چهارم: خم های بیضوی روی میدان های متناهی

فرض کنید $\mathbb{F}$ یک میدان متناهی و E یک خم بیضوی روی $\mathbb{F}$ باشد. چون فقط تعداد متناهی جفت (x,y) که $x,y \in \mathbb{F}$ وجود دارد، گروه $E(\mathbb{F})$ متناهی است.

از جزئیات این گروه می توان روی مرتبه آن متمرکز شد

در این بخش قضیه اساسی خم های بیضوی روی میدان های متناهی را بررسی خواهیم کرد.

مثال ٤.١

فرض کنید E خم بیضوی $y^2 = x^3 + x + 1$ روی میدان $\mathbb{F}_5$ باشد نقاط قابل شمارش $\mathbb{F}_5$ این امکان را می دهد که مقادیر ممکن برای x را بدانیم. با دانستن مقادیر x مقادیر $x^3 + x + 1$ در پیمانه ۵ را نیز می توان بدست آورد و سپس ریشه دوم را برای مقادیر y نیز می توان در پیمانه ۵ یافت. تمامی این کارها نقاط خم بیضوی E را مشخص می کنند

x	$x^3 + x + 1$	y	$points$
۰	۱	± 1	(۰,۱), (۰,۴)
۱	۳	-	-
۲	۱	± 1	(۲,۱), (۲,۴)
۳	۱	± 1	(۳,۱), (۳,۴)
۴	۴	± 2	(۴,۲), (۴,۳)
∞	∞	∞	∞

لذا $E(\mathbb{F}_5)$ دارای مرتبه ۹ است

می خواهیم $(۲,۴) + (۳,۱)$ را در E محاسبه کنیم

شیب خط گذرا از این دو نقطه برابر $\frac{۴-۱}{۲-۳} = -۳ \equiv ۲ \pmod 5$ است. پس خط گذرا دارای معادله $y = ۲(x-۳) + ۱ \equiv ۲x$ می باشد با جایگذاری $y^2 = x^3 + x + 1$ و محاسبه خواهیم داشت $x^3 - ۴x^2 + x + ۱ = ۰$ لذا حاصل جمع ریشه ها ۴ است و چون $y = ۲x$ پس $y \equiv ۳$ (چون ریشه

های ۲ و ۳ را می شناسیم پس ریشه سوم ۴ است) حال با انعکاس نسبت به محور x ها نتیجه می گیریم

$$(۳,۱) + (۲,۴) = (۴,۲)$$

کمی محاسبه نشان می دهدکه $E(\mathbb{F}_۵)$ دوری باملود $(۰,۱)$ است.

مثال ٤.٢

فرض کنید E خم بیضوی $y^۲ = x^۳ + ۲$ روی میدان $\mathbb{F}_۷$ باشد آنگاه با محاسباتی مثل مثال قبل خواهیم داشت

$$E(\mathbb{F}_۷) = \{\infty, (۳,۴), (۰,۴), (۳,۱), (۳,۶), (۵,۱), (۵,۶), (۶,۱), (۶,۶)\}$$

یک محاسبه نشان می دهد که تمام نقاط P در رابطه $۳P = P$ صدق می کند پس این گروه با $\mathbb{Z}_۳ \oplus \mathbb{Z}_۳$ یکریخت است.

مثال ٣.٤

فرض کنید E خم بیضوی $y^۲ + xy = x^۳ + ۱$ روی میدان $\mathbb{F}_۲$ باشد. مانند مثال اول می توانیم نقاط را بدست بیاوریم. داریم:

$$E(\mathbb{F}_۲) = \{\infty, (۰,۱), (۱,۰), (۱,۱)\}$$

این گروه یک گروه دوری از مرتبه ۴ است. نقاط $(۱,۱), (۱,۰)$ از مرتبه ۴ و نقطه $(۰,۱)$ از مرتبه ۲ است.

حال نگاهی بر $E(\mathbb{F}_۴)$ می اندازیم. می دانیم $\mathbb{F}_۴$ میدانی متناهی با ۴ عنصر است. می توانیم آن را بصورت $\mathbb{F}_۴ = \{۰,۱, \omega, \omega^۲\}$ بنویسیم که در آن رابطه $\omega^۲ + \omega + ۱ = ۰$ برقرار است (که بعد از ضرب طرفین در $\omega + ۱$ نتیجه می گیریم $\omega^۳ + ۱ = ۰$)

حال عناصر $E(\mathbb{F}_۴)$ را مشخص می کنیم:

$$x = ۰ \Rightarrow y^۲ = ۱ \Rightarrow y = ۱$$

$$x = ۱ \Rightarrow y^۲ + y = ۰ \Rightarrow y = ۰,۱$$

$$x = \omega \Rightarrow y^۲ + \omega y = ۰ \Rightarrow y = ۰, \omega$$

$$x = \omega^۲ \Rightarrow y^۲ + \omega^۲ y \Rightarrow y = ۰, \omega^۲$$

$$x = \infty \Rightarrow y = \infty$$

پس

$$E(\mathbb{F}_4) = \{\infty, (0,1), (1,0), (1,1), (\omega, 0), (\omega, \omega), (\omega^2, 0), (\omega^2, \omega^2)\}$$

چون در مشخصه ۲ کار می کنیم حداکثر یک نقطه از مرتبه ۲ وجود دارد. در واقع $(0,1)$ از مرتبه ۲ است پس $E(\mathbb{F}_4)$ دوری از مرتبه ۸ است. هر یک از ۴ نقطه که شامل ω و ω^2 هستند مولد برای $E(\mathbb{F}_4)$ هستند.

فرض کنید $\varphi_2(x,y) = (x^2, y^2)$ نگاشت فروبینوس باشد براحتی دیده می شود که φ_2 یک جایگشت روی عناصر $E(\mathbb{F}_4)$ است و $E(\mathbb{F}_2) = \{(x,y) \in E(\mathbb{F}_4) \mid \varphi_2(x,y) = (x,y)\}$.

در واقع برای هر خم بیضوی E روی $\mathbb{F}_q$ و هر توسیع $\mathbb{F}$ از $\mathbb{F}_q$ نگاشت فروبینیوس φ_q یک جایگشت روی عناصر $E(\mathbb{F})$ است و همچنین عنصر همانی زیر گروه $E(\mathbb{F}_q)$ نیز هست.

لم ٤.١

فرض کنید E یک خم بیضوی روی میدان متناهی $\mathbb{F}_q$ باشد آنگاه برای برخی $n \geq 1$ و یا برای برخی $n_1, n_2 \geq 1$ که $n_1 \mid n_2$ داریم $E(\mathbb{F}_q) \cong \mathbb{Z}_n \ Or \ \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$

اثبات:

از نظریه گروه ها می دانیم که یک گروه آبلی متناهی با جمع مستقیم گروه های دوری یکریخت است یعنی با $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_r}$ که برای هر $i \geq 1$ داریم $n_i \mid n_{i+1}$.

چون برای هر i، $\mathbb{Z}_{n_i}$ دارای n_1 عضو با مرتبه ای که n_1 را عاد می کنند هست پس $E(\mathbb{F}_q)$ دارای n_1^r عضو است که مرتبه شان n_1 را عاد می کند. صبق قضیه ۳.۲ حدکثر n_1^2 نقطه با این خاصیت موجود است (حتی اگر مختصات را در $\overline{\mathbb{F}_q}$ در نظر بگیریم) پس $r \leq 2$. و این اثبات را کامل می کند. (اگر $r = 0$ در این صورت گروه بدیهی (معادل با زمانی است که $n = 1$) است.)

قضیه ٤.٢ (قضیه هس)

فرض کنید E یک خم بیضوی روی میدان متناهی $\mathbb{F}_q$ باشد آنگاه درجه $E(\mathbb{F}_q)$ در رابطه زیر صدق می کند

$$|q + ۱ - \#E(\mathbb{F}_q)| \leq ۲\sqrt{q}$$

اثبات

این قضیه در بخش بعدی اثبات خواهد شد.

قضیه ٤.٣

فرض کنید $q = p^n$ توانی از عدد اول p باشد و فرض کنید $N = q + ۱ - a$.

در این صورت یک خم بیضوی E روی $\mathbb{F}_q$ موجود است بطوریکه $\#E(\mathbb{F}_q) = N$ اگر و تنها اگر $|a| \leq ۲\sqrt{q}$ و همچنین برای a یکی از شرایط زیر برقرار باشد:

۱- $gcd(a, p) = ۱$
۲- $a = \pm ۲\sqrt{q}$ و n زوج
۳- $a = \pm\sqrt{q}$ و n زوج و $p \not\equiv ۱ \pmod ۳$
۴- n فرد و $p = ۲ \; or \; ۳$ و $a = \pm p$
۵- $a = ۰$ و n زوج و $p \not\equiv ۱ \pmod ۴$
۶- n فرد و $a = ۰$

قضیه ٤.٤

فرض کنید N عدد صحیحی باشد که مرتبه یک خم بیضوی روی میدان متناهی $\mathbb{F}_q$ است که در قضیه قبل اشاره شد N را بصورت زیر می نویسیم $N = p^e n_۱ n_۲$ که $p \nmid n_۱ n_۲$ و $n_۱ \mid n_۲$ (ممکن است $n_۱ = ۱$)
در این صورت خم بیضوی E روی $\mathbb{F}_q$ وجود دارد بطوریکه $E(\mathbb{F}_q) \cong \mathbb{Z}_{p^e} \oplus \mathbb{Z}_{n_۱} \oplus \mathbb{Z}_{n_۲}$ اگر و تنها اگر

۱- $n_۱ \mid q - ۱$ (در حالت های ۱ و ۳ و ۴ و ۵ و ۶ قضیه قبل)
۲- $n_۱ = n_۲$ (در حالت ۲ قضیه قبل)

این ها تنها گروه هایی هستند که با گروه $E(\mathbb{F}_q)$ می آیند

٤.٢درونریختی های فروبینوس

فرض کنید $\mathbb{F}_q$ یک میدان متناهی با بستار جبری $\overline{\mathbb{F}_q}$ باشد و فرض کنید $\varphi_q: \overline{\mathbb{F}_q} \longrightarrow \overline{\mathbb{F}_q}$ با ضابطه $x \longmapsto x^q$ باشد.

فرض کنیم E یک خم بیضوی روی $\mathbb{F}_q$ باشد آنگاه تاثیر φ_q بر نقاط با مختصات در $E(\overline{\mathbb{F}_q})$ بصورت زیر است. $\varphi_q(\infty) = \infty \quad , \quad \varphi_q(x,y) = (x^q, y^q)$

لم ٤.٥

فرض کنید E یک خم بیضوی روی $\mathbb{F}_q$ باشد و فرض کنید و $(x,y) \in E(\overline{\mathbb{F}_q})$ در این صورت

۱- $\varphi_q(x,y) \in E(\overline{\mathbb{F}_q})$

۲- $(x,y) \in E(\mathbb{F}_q)$ اگر و تنها اگر $\varphi_q(x,y) = (x,y)$

اثبات

وقتی q توانی از مشخصه میدان باشد داریم $(a+b)^q = a^q + b^q$ و همچنین برای تمام $a \in \mathbb{F}_q$ داریم $a^q = a$ (ضمیمه C را ببینید)

چون اثبات برای فرم وایرشتراس و فرم وایرشتراس تعمیم یافته یکی است لذا ما روی معادله اصلی کار می کنیم. داریم $y^۲ + a_۱xy + a_۳y = x^۳ + a_۲x^۲ + a_۴x + a_۶$ که $a_i \mathbb{F}_q$. اگر این معادله را به توان q برسانیم خواهیم داشت

$$(y^q)^۲ + a_۱(x^q y^q) + a_۳(y^q) = (x^q)^۳ + a_۲(x^q)^۲ + a_۴(x^q) + a_۶$$

یعنی (x^q, y^q) در معادله صدق می کند. پس اثبات ۱ تمام شد.

برای اثبات ۲ یادآوری می کنیم (طبق ضمیمه C) $x \in \mathbb{F}_q$ اگر و تنها اگر $\varphi_q(x) = x$ و همین طور $\varphi_q(y) = y$ بنابراین

$$(x,y) \in E(\mathbb{F}_q) \Leftrightarrow x,y \in \mathbb{F}_q \Leftrightarrow \varphi_q(x) = x \;\&\; \varphi_q(y) = y$$

لم ٤.٦

فرض کنید E یک خم بیضوی روی میدان $\mathbb{F}_q$ باشد در این صورت φ_q یک درونریختی از E با مرتبه q است و φ_q جداشدنی نیست.

اثبات

همانند قضیه ۲.۲۰

توجه

هسته درونریختی φ_q همانی است

نکته

چون φ_q یک درونریختی از E است پس $\varphi_q{}^{۲} = \varphi_q \circ \varphi_q$ و همچنین برای $n \geq ۱$ داریم $\varphi_q{}^{n} = \varphi_q \circ \varphi_q \circ \varphi_q \circ \dots \circ \varphi_q{}^{۲} = \varphi_q \circ \varphi_q$ و چون ضرب توسط ۱− نیز یک درونریختی است پس $\varphi_q{}^{n} - ۱$ نیز یک درونریختی از E است.

قضیه زیر نقش مهمی در شمارش نقاط یک خم بیضوی روی میدان متناهی دارد.

قضیه ٤.٧

فرض کنید E یک خم بیضوی روی میدان $\mathbb{F}_q$ باشد و $n \geq ۱$

۱- $ker(\varphi_q{}^{n} - ۱) = E(\mathbb{F}_{q^n})$

۲- $\varphi_q{}^{n} - ۱$ یک درونریختی جداشدنی است، پس $\#E(\mathbb{F}_{q^n}) = deg(\varphi_q{}^{n} - ۱)$

اثبات

چون $\varphi_q{}^{n}$ نگاشت فروبینوس برای میدان $\mathbb{F}_{q^n}$ است پس ۱ درواقع بیان دیگری از لم ۴.۵ است.

اینکه $\varphi_q{}^{n} - ۱$ یک درونریختی جداشدنی است در قضیه ۲.۲۹ ثابت شد. پس ۲ از لم ۲.۲۱ نتیجه می شود.

اثبات قضیه هس

حال می توانیم قضیه هس (۴.۲) را اثبات کنیم

فرض کنید $a = q + ۱ - \#E(\mathbb{F}_q) = q + ۱ - deg(\varphi_q - ۱)$ می خواهیم نشان دهیم $|a| \leq ۲\sqrt{q}$ برای این منظور به لم زیر نیاز خواهیم داشت.

لم ٤.٨

فرض کنید r و s اعداد صحیحی باشندکه $gcd(r,s) = ۱$ در این صورت

$$deg(r\varphi_q - s) = r^۲q + s^۲ - ras$$

اثبات

فضیه ۳.۱۶ نتیجه می دهد

$$deg(r\varphi_q - s) = r^۲deg(\varphi_q) + s^۲deg(-۱) - rs\left(deg(\varphi_q - ۱) - deg(\varphi_q) - deg(-۱)\right)$$

و چون $deg(-۱) = ۱$ و $deg(\varphi_q) = q$ لذا از لم ۴.۱ نتیجه حاصل می شود.

تذکر

فرض $gcd(r,s) = ۱$ در لم فوق مورد نیاز نبود این شرط برای این منظور آورده شده که قضیه ۳.۱۶ در حالت کلی نمی تواند درست باشد بلکه زمانی اثبات می شود که درونریختی جداشدنی باشد و یا درونریختی فروبینوس φ_q باشد

حال به ادامه اثبات قضیه هس می پردازیم.

چون $deg(r\varphi_q - s) \geq ۰$ از لم نتیجه می گیریم برای تمام r و s هایی که $gcd(r,s) = ۱$ داریم

$$q\left(\frac{r}{s}\right)^۲ - a\left(\frac{r}{s}\right) + ۱ \geq ۰$$

مجموعه تمام اعداد گویا $\frac{r}{s}$ که $gcd(r,s) = ۱$ در $\mathbb{R}$ چگال است (اثبات: s را توانی از ۲ یا توانی از ۳ در نظر بگیرید. هر کدام از این ها را که در نظر بگیریم نسبت به q اول هستند. اعداد گویای به فرم $r/_{۲m}$ و

$\varphi(x)^2 - a(x) + 1 \geq 0$ داریم x بوضوح در $\mathbb{R}$ چگال اند.) بنابراین برای تمام اعداد حقیقی $r/3m$. لذا مبین چندجمله ای منفی و یا صفر است. و این یعنی $a^2 - 4q \leq 0$ بنابراین $|a| \leq 2\sqrt{q}$

و این اثبات قضیه هس را کامل می کند.

نتیجه

قضیه هس نتایج مفید بسیاری دارد یکی از آن ها این است که ما می توانیم $E(\mathbb{F}_q)$ را به عنوان هسته همریختی $\varphi_q - 1$ در نظر بگیریم.

نتیجه دیگر آن است که $\varphi_q - 1$ جداشدنی است بنابراین مرتبه هسته همریختی برابر درجه $\varphi_q - 1$ است.

سومین نتیجه مهم جفت سازی ویل مخصوصا قسمت ۶ قضیه ۳.۹ و نتیجه قضیه ۳.۱۶ است

قضیه ٤.١٠

فرض کنید E یک خم بیضوی روی میدان $\mathbb{F}_q$ باشد و فرض کنیم

$a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - deg(\varphi_q - 1)$ در این صورت درونریختی

$\varphi_q{}^2 - a\varphi_q + q = 0$ را داریم و a تنها عدد صحیح می باشد که در معادله $\varphi_q{}^2 - k\varphi_q + q = 0$ صدق می کند. بعبارتی دیگر اگر $(x, y) \in E(\overline{\mathbb{F}_q})$ داریم

$\left(x^{q^2}, y^{q^2}\right) - a(x^q, y^q) + q(x, y) = \infty$ و a تنها عدد صحیح می باشد که به روش زیر بدست می آید بعلاوه a تنها عدد صحیح می باشد که برای تمام m هایی که $gcd(m, q) = 1$ داریم $a \equiv Trace\left((\varphi_q)_m\right) \pmod m$ که $(\varphi_q)_m$ ماتریس درونریختی φ_q است.

اثبات

به روش عکس نقیض: اگر $\varphi_q{}^2 - a\varphi_q + q$ بعنوان درونریختی مخالف صفر باشد آنگاه بنابر قضیه ۲.۲۱ برای هر $\alpha \neq 0$ نامساوی زیر را داریم $\#ker\alpha \leq deg\alpha$

هسته $\varphi_q^{۲} - a\varphi_q + q = ۰$ متناهی می باشد پس کافیست ثابت کنیم این هسته نامتناهی است یعنی درون ریختی مورد نظر صفر است. فرض کنیم $m \in \mathbb{Z}^+$ که $gcd(m,q) = ۱$ در این صورت از قبل می دانیم که φ_q روی $E[m]$ بصورت زیر عمل می کند $\alpha_n = \left((\varphi_q)_m\right) = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$.

بنابر قضیه ۲.۲۱ درونریختی $\varphi_q - ۱$ جداشدنی می باشد. حال

$$\#ker\alpha_n \equiv deg\alpha \ (mod\ m) \Longrightarrow \#ker(\varphi_q - ۱) = deg(\varphi_q - ۱)$$
$$\equiv deg(\varphi_q)_m \ (mod\ m) = sv - tu - (s+v) + ۱$$

حال بنابر گزاره ۳.۱۵ داریم $sv - tu = deg(\varphi_q) \equiv deg\varphi_q = q \ (mod\ m)$ بنابراین $sv - tu \equiv q \ (mod\ m)$ حال داریم

$$a = q + ۱ - deg(\varphi_q - ۱) \equiv q + ۱ - (sv - tu - (s+v) + ۱) \ (mod\ m)$$
$$\Longrightarrow Trace(\varphi_q)_m \equiv a \equiv s + v \ (mod\ m)$$

حال ماتریس $(\varphi_q)_m$ در رابطه زیر صدق می کند

$$\left((\varphi_q)_m\right)^{۲} - a\left((\varphi_q)_m\right) + qI \equiv ۰ \ (mod\ m)$$

این مطلب را بررسی می کنیم

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix}\begin{pmatrix} s & t \\ u & v \end{pmatrix} = \begin{pmatrix} s^{۲} + tu & st + tv \\ su + vu & vt + v^{۲} \end{pmatrix}$$

$$\begin{pmatrix} s^{۲} + tu - as + q & st + tv - at \\ su + vu - au & vt + v^{۲} - av + q \end{pmatrix} = \left((\varphi_q)_m\right)^{۲} - a\left((\varphi_q)_m\right) + qI$$

$$a_{۱۱} = s^{۲} + tu - as + q \equiv s^{۲} + sv - as \equiv sa - as = ۰ \ (mod\ m)$$

$$a_{۱۲} = st + tv - at \equiv ta - at = ۰ \ (mod\ m)$$

$$a_{۱۳} = su + vu - au \equiv ua - au = ۰ \ (mod\ m)$$

$$a_{۱۴} = vt + v^{۲} - av + q \equiv sv + v^{۲} - av \equiv va - av = ۰ \ (mod\ m)$$

بنابراین $\left((\varphi_q)_m\right)^2 - a\left((\varphi_q)_m\right) + qI \equiv 0 \pmod m$ یعنی روی $E[m]$ داریم
$\varphi_q{}^2 - a\varphi_q + q = 0$

حال چون بینهایت $m \in \mathbb{Z}^+$ که $gcd(m,q) = 1$ وجود دارد بنابراین هسته $\varphi_q{}^2 - a\varphi_q + q$ نامتناهی می باشد. بنابراین روی $E(\mathbb{F}_q)$ داریم $\varphi_q{}^2 - a\varphi_q + q = 0$.

حال کافیست ثابت کنیم a تنها عدد صحیحی است که در رابطه $\varphi_q{}^2 - k\varphi_q + q = 0$ صدق می کند.
فرض کنیم $a_1 \neq a$ عدد صحیح دیگری باشد که رابطه زیر برای آن برقرار باشد $\varphi_q{}^2 - a\varphi_q + q = 0$
داریم $(a - a_1)\varphi_q = \left(\varphi_q{}^2 - a\varphi_q + q\right) - \left(\varphi_q{}^2 - a_1\varphi_q + q\right) = 0$.

بنابر قضیه ۲.۲۲ (اگر خم بیضوی E روی میدان K باشد و α یک درونر یختی از E باشد آنگاه $\alpha: E[K] \longrightarrow E[K]$ پوشاست.) پس درونریختی $\varphi_q: E(\overline{\mathbb{F}_q}) \longrightarrow E(\overline{\mathbb{F}_q})$ پوشاست فلذا

$$\forall P \in E(\overline{\mathbb{F}_q});\ \exists Q \in E(\overline{\mathbb{F}_q})\ \ s.t.\ \varphi_q(Q) = P$$

$$\forall Q \in E(\overline{\mathbb{F}_q});\ \ (a - a_1)\varphi_q(Q) = 0$$

با توجه به روابط اخیر $(a - a_1)\varphi_q P = \infty \ ;\ \ \forall P \in E(\overline{\mathbb{F}_q})$ در واقع درونریختی

$P \longmapsto (a - a_1)$ روی $E(\overline{\mathbb{F}_q})$ صفر است چون $E[m] \subseteq E(\overline{\mathbb{F}_q})$ پس درونریختی فوق روی $E[m]$ نیز صفر است چون $E[m]$ شامل نقاطی از مرتبه m می باشد بنابر تعریف مرتبه داریم

$m \mid (a - a_1)$. پس $a - a_1 \equiv 0 \pmod m$ و چون بینهایت $m \in \mathbb{Z}^+$ که $gcd(m,q) = 1$
وجود دارد بنابراین $a - a_1 = 0$ در نتنجه $a = a_1$

نکته: روابط زیر را داریم $\left((\varphi_q)_m\right)^2 - a\left((\varphi_q)_m\right) + qI \equiv 0 \pmod m$ و

$$\left((\varphi_q)_m\right) = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

رابطه اول را می توان با استفاده از قضیه کیلی همیلتون در جبر خطی نیز ثابت کرد: چند جمله ای مشخصه $(\varphi_q)_m$ بصورت زیر است

$$det\left|xI - (\varphi_q)_m\right| = \begin{vmatrix} x - t & -t \\ -u & x - v \end{vmatrix} = x^2 - (s+v)x + sv - ut$$

پس بنابر قضیه کیلی همیلتون داریم $(\varphi_q)_m^{\,2} - (s+v)(\varphi_q)_m + sv - ut = 0$

۴.۳ تعیین مرتبه خم های بیضوی

در قضیه هس توانستیم کران هایی برای گروه نقاط یک خم بیضوی روی میدان متناهی بدست آوریم، در این بخش درباره روش هایی برای تعیین مرتبه گروه بحث خواهیم کرد.

خم روی زیر میدان ها

گاهی خم E روی میدان متناهی کوچک $\mathbb{F}_q$ داده می شود و هدف ما یافتن مرتبه $E(\mathbb{F}_q{}^n)$ برای برخی n ها است. برای $n = 1$ این کار به راحتی با نوشتن اعضا یا برخی کارهای ابتدایی انجام می شود. و نکته جالب توجه این است که ما می توانیم این کار را برای تمامی n ها انجام دهیم.

قضیه ۴.۱۲

فرض می کنیم $\#E(\mathbb{F}_q) = q + 1 - a$ و می نویسیم $X^2 - aX + q = (X-\alpha)(X-\beta)$ در این صورت برای تمام $n \geq 1$ داریم $\#E(\mathbb{F}_q{}^n) = q^n + 1 - (\alpha^n + \beta^n)$

اثبات

$\alpha^n + \beta^n$ یک عدد صحیح است. این گزاره را می توان برای تمام اعداد صحیح جبری و همچنین اعداد گویا نیز ثابت کرد. برای ادامه اثبات به لم زیر نیاز خواهیم داشت

لم ۴.۱۳

فرض کنید $s_n = \alpha^n + \beta^n$. آنگاه $s_0 = 2$، $s_1 = a$ و $s_{n+1} = as_n - qs_{n-1}$ برای تمام $n \geq 1$

اثبات

اگر طرفین معادله $\alpha^2 - \alpha + q = 0$ را در α^{n-1} ضرب کنیم داریم $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$ رابطه مشابهی نیز برای β داریم که با جمع آن ها لم اثبات می شود

حال به ادامه اثبات قضیه می پردازیم

از لم نتیجه می گیریم که برای تمام $n \geq 0$، $\alpha^n + \beta^n$ یک عدد صحیح است. فرض کنید

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{۲n} - (\alpha^n + \beta^n)X^n + q^n$$

در این صورت $X^۲ - aX + q = (X - \alpha)(X - \beta)$ چند جمله ای $f(X)$ را عاد می کند لذا بنابر الگوریتم تقسیم برای چند جمله ای ها، خارج قمست، یک چند جمله ای $Q(X)$ است که ضرایب آن صحیح است (یعنی نقاط $X^۲ - aX + q$ دارای ضریب پیشروی ۱ هستند یعنی این چندجمله ای و $f(X)$ دارای ضرایب صحیح هستند.) بنابراین طبق قضیه ۴.۱۰ داریم

$$\left(\varphi_q{}^n\right)^۲ - (\alpha^n + \beta^n)\varphi_q{}^n + q^n = f\left(\varphi_q\right) = Q\left(\varphi_q\right)\left(\varphi_q{}^۲ - a\varphi_q + q\right) = ۰$$

یک درونریختی از E است. توجه کنید که $\varphi_q{}^n = \varphi_{q^n}$. طبق قضیه ۴.۱۰ یک عدد صحیح k وجوددارد که $\varphi_{q^n}{}^۲ - k\varphi_{q^n} + q^n = ۰$ و همچنین یک k توسط $k = q^n + ۱ - \#E\left(\mathbb{F}_q{}^n\right)$ تعیین می شود بنابراین $\alpha^n + \beta^n = q^n + ۱ - \#E\left(\mathbb{F}_q{}^n\right)$. و این اثبات را کامل می کند.

مثال ٤.٤

در مثال ۴.۳ نشان داده شد که در خم $y^۲ + xy = x^۳ + ۱$ روی $\mathbb{F}_۲$ داریم $\#E(\mathbb{F}_۲) = ۴$. بنابراین $a = ۲ + ۱ - ۴ = -۱$ و چندجمله ای زیر را داریم

$$X^۲ + X + ۲ = \left(X - \frac{-۱ + \sqrt{-۷}}{۲}\right)\left(X - \frac{-۱ - \sqrt{-۷}}{۲}\right)$$

قضیه ۴.۱۲ بیان می کند

$$\#E(\mathbb{F}_۴) = ۴ + ۱ - \left(\frac{-۱ + \sqrt{-۷}}{۲}\right)^۲ - \left(\frac{-۱ - \sqrt{-۷}}{۲}\right)^۲$$

بدون محاسبه مستقیم عبارت اخیر می توان از رابطه بازگشتی لم ۴.۱۳ استفاده کرد

$$s_۲ = as_۱ - ۲s_۰ = -(-۱) - ۲(۲) = -۳$$

در نتیجه $\#E(\mathbb{F}_۴) = ۴ + ۱ - (-۳) = ۸$. یعنی ما با فهرست کردن نقاط می توانیم مرتبه را بیابیم.

بطور مشابه با استفاده از رابطه بازگشتی یا محاسبات دقیق نتیجه می گیریم که

$$\left(\frac{-۱ + \sqrt{-۷}}{۲}\right)^{۱۰۰} + \left(\frac{-۱ - \sqrt{-۷}}{۲}\right)^{۱۰۰} = ۲۹۶۹۲۹۲۲۱۰۶۰۵۲۶۹$$

در نتیجه

$$\#E(\mathbb{F}_{۱۰۰}) = ۲^{۱۰۱} + ۱ - ۲۹۶۹۲۹۲۲۱۰۶۰۵۲۶۹ = ۲۵۳۵۳۰۱۲۰۰۴۵۶۴۵۵۸۳۳۷۰۱۱۹۵۸۰۵۴۸۴$$

توجه

مزیت قضیه ۴.۱۲ این است که این امکان را می د هد که مرتبه برخی خم ها را سریع محاسبه کنیم و اشکال این قضیه این است که به یک خم بیضوی که روی میدان متناهی کوچک تر تعریف شده نیاز هست

نماد لژاندر

برای تهیه فهرستی از نقاط خم $y^۲ = x^۳ + Ax + B$ روی میدان متناهی، تمام نقاط ممکن برای x را می آزماییم پس ریشه دوم y از $x^۳ + Ax + B$ را در صورت وجود می یابیم این یک الگوریتم اولیه برای شمارش نقاط است

نماد لژاندر $\left(\frac{x}{p}\right)$ را برای تمام اعداد اول فرد p بصورت زیر تعریف می کنیم

$$\left(\frac{x}{p}\right) = \begin{cases} +۱ & if\ t^۲ \equiv x\ (mod\ p) \Rightarrow t \not\equiv ۰\ (mod\ p) \\ ۰ & if\ t^۲ \equiv x\ (mod\ p) \Rightarrow \\ -۱ & if\ x \equiv ۰\ (mod\ p) \end{cases}$$

دارای جواب باشد

دارای جواب نباشد

این تعریف را می توان برای هر میدان متناهی $\mathbb{F}_q$ که q عدد اولی است و برای هر $x \in \mathbb{F}_q$ بصورت زیر تعمیم داد.

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +۱ & \text{اگر } x = t^۲ \text{ دارای جواب } t \in \mathbb{F}_q{}^{\times} \text{ باشد} \\ ۰ & \text{اگر } x = t^۲ \text{ دارای جواب } t \in \mathbb{F}_q{}^{\times} \text{ نباشد} \\ -۱ & \text{اگر } x = ۰ \end{cases}$$

قضیه ٤.١٤

فرض کنید E خم بیضوی $y^۲ = x^۳ + Ax + B$ روی $\mathbb{F}_q$ باشد در این صورت داریم

$$\#E(\mathbb{F}_q) = q + ۱ + \sum_{x \in \mathbb{F}_q} \left(\frac{x^۳ + Ax + B}{\mathbb{F}_q}\right)$$

اثبات

فرض کنیم نقطه x_0 مفروض باشد در این صورت اگر $x_0^3 + Ax_0 + B$ در $\mathbb{F}_q$ مخالف صفر و نامربع باشد آنگاه دو نقطه با مختصات x_0 مانند (x, y) وجود دارد که یکی از این نقاط صفر است و اگر چندجمله ای بالا نامربع باشد چنین نقاطی موجود نیستند. پس تعداد اعدادی که مختصات x شان برابر x_0 است

$\left(\frac{x_0^3+Ax_0+B}{\mathbb{F}_q}\right) + 1$ است. جمع روی $x_0 \in \mathbb{F}_q$ و اضافه کردن نقطه یک برای ∞، اثبات قضیه را کامل می کند.

قضیه ٤.١٥

فرض کنید $x^3 + Ax + B$ یک چندجمله ای با $A, B \in \mathbb{F}_q$ باشد که در آن q فرد است. در این صورت

$$\left|\sum_{x\in\mathbb{F}_q}\left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)\right| \leq 2\sqrt{q}$$

اثبات

وقتی $x^3 + Ax + B$ داری ریشه تکراری نباشد $y^2 = x^3 + Ax + B$ معادله یک خم بیضوی است لذا قضیه ۴.۱۴ بیان می کند که

$q + 1 - \#E(\mathbb{F}_q) = -\sum_{x\in\mathbb{F}_q}\left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)$ حال بنابر قضیه هس نتیجه برقرار است.

حالتی که $x^3 + Ax + B$ دارای ریشه تکراری است در تمرین ۴.۳ آمده است.

مثال ٤.٥

فرض کنید E خم $y^2 = x^3 + x + 1$ روی $\mathbb{F}_5$ باشد. ۱ و ۴ مربع های ناصفر در پیمانه ۵ هستند پس

$$\#E(\mathbb{F}_5) = 5 + 1 + \sum_{x=0}^{4}\left(\frac{x^3 + x + 1}{5}\right) = 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{4}{5}\right) = 9$$

مرتبه نقاط

طریقه پیدا کردن مرتبه نقاط و یک تعریف

فرض کنید $P \in E(\mathbb{F}_q)$ در این صورت مرتبه P را کوچکترین عدد صحیح مثبت k در نظر می گیریم بطوریکه $kP = \infty$

طبق قضیه لاگرانژ مرتبه نقاط همواره مرتبه گروه $E(\mathbb{F}_q)$ را عاد می کنند. پس برای تمام اعداد صحیح n داریم $nP = \infty$ اگر و تنها اگر مرتبه P، n را عاد کند.

با توجه به بازه هس داریم $q + ۱ - ۲\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + ۱ + ۲\sqrt{q}$. طول بازه برابر $۴\sqrt{q}$ است برای یافتن مرتبه نقاط دو حالت را بررسی می کنیم

وضعیت مطلوب:

اگر بتوانیم نقطه ای مثل P با مرتبه بزرگتر از $۴\sqrt{q}$ پیدا کنیم آنگاه دقیقا یک مضرب از مرتبه این نقطه در بازه هس خواهد بود از طرفی می دانیم مرتبه هر عضو مرتبه گروه راعاد می کند پس می توان گفت آن مضرب از مرتبه P که در بازه هس است مرتبه گروه خواهد بود.

وضعیت نامطلوب

این است که نتوانیم نقطه ای مثل P با مرتبه بزرگتر از $۴\sqrt{q}$ پیدا کنیم در این حالت می توانیم با پیدا کردن نقاط دیگر و با توجه به این که کوچکترین مضرب مشترک مرتبه های اعضا مرتبه گروه را عاد می کند می توان در برخی مواقع مرتبه گروه را محاسبه کرد.

مثال ٤.٦

فرض کنید E خم $y^۲ = x^۳ + ۷x + ۱$ روی $\mathbb{F}_{۱۰۱}$ باشد. می توان نشان داد $(۰,۱)$ دارای مرتبه ۱۱۶ است پس $N_{۱۰۱} = \#E(\mathbb{F}_{۱۰۱})$ مضربی از ۱۱۶ است با توجه به قضیه هس داریم

$$۱۰۱ + ۱ - ۲\sqrt{۱۰۱} \leq \#E(\mathbb{F}_{۱۰۱}) = N_{۱۰۱} \leq ۱۰۱ + ۱ + ۲\sqrt{۱۰۱}$$

یعنی$۸۲ \leq N_{۱۰۱} \leq ۱۲۲$ تنها ضریب ۱۱۶ که در این بازه است خود ۱۱۶ است پس $N_{۱۰۱} = ۱۱۶$. به عنوان یک نتیجه می توان گروه های دوری از مرتبه ۱۱۶ را یافت که مولدشان $(۰,۱)$ است.

مثال ٤.٧

فرض کنید E خم $y^2 = x^3 - 16x + 21$ روی $\mathbb{F}_{557}$ باشد. می توان نشان داد $(2,3)$ دارای مرتبه ۱۸۹ است پس قضیه هس نتیجه می دهد $511 \leq N_{557} \leq 605$ تنها ضریب ۱۸۹ که در این بازه است خود $189 \cdot 3 = 567$ است پس $N_{557} = 567$.

مثال ٤.٨

فرض کنید E خم $y^2 = x^3 + 7x + 12$ روی $\mathbb{F}_{103}$ باشد نقطه $(-1,2)$ از مرتبه ۱۳ و نقطه $(0,19)$ از مرتبه ۲ است. پس مرتبه $E(\mathbb{F}_{103})$ یعنی N_{103} مضربی از ۲۶ است. طبق قضیه هس داریم $84 \leq N_{103} \leq 124$ و تنها مضرب ۲۶ که در این بازه است ۱۰۴ است پس $N_{103} = 104$.

مثال ٤.٩

فرض کنید E خم $y^2 = x^3 + 2$ روی $\mathbb{F}_7$ باشد. در مثال ۴.۲ دیده شد که $E(\mathbb{F}_7)$ با گروه $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ یکریخت است و تمام نقاط غیر از نقطه در بینهایت دارای مرتبه ۳ هستند. پس طبق روال نتیجه می گلیریم که مرتبه N_7 مضربی از ۳ است. قضیه هس بیان می کند $3 \leq N_7 \leq 13$ پس مرتبه برابر یکی از اعداد ۳ یا ۶ یا ۹ و یا ۱۲ خواهد شد. البته اگر بتوان دو نقطه مستقل از مرتبه ۳ (یعنی یکی از نقاط مضربی از دیگری نباشد) یافت آنگاه آن ها نیز زیرگروهی از مرتبه ۹ می سازند. یعنی مرتبه کل گروه ضریبی از ۹ است پس $N_7 = 9$.

ملاحظه کردیم که در این مثال در حالتی که $E(\mathbb{F}_q) \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ یافتن مرتبه گروه کاری دشوار بود برای تسهیل این موضوع قضیه زیر را بیان می کنیم.

قضیه ٤.١٦

فرض کنید E خم بیضوی روی $\mathbb{F}_q$ باشد و برای برخی n ها داشته باشیم $E(\mathbb{F}_q) \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ در این صورت $q = n^2 + 1$ یا $q = n^2 \pm n + 1$ یا $q = (n \pm 1)^2$

اثبات

طبق قضیه هس $n^2 = q + 1 - a$ که $|a| \leq 2\sqrt{q}$. برای اثبات قضیه از لم زیر استفاده می کنیم که محدودیت هایی برای a تعیین می کند.

لم ٤.١٧

$$a \equiv ٢ \pmod{n}$$

اثبات

فرض کنید p مشخصه $\mathbb{F}_q$ باشد. آنگاه $p \nmid n$. در غیر این صورت ممکن است $E[p]$ دارای $p^٢$ نقطه باشد که طبق قضیه ٣.٢ در مشخصه p ممکن نیست.

چون $E[n] \subseteq E[\mathbb{F}_q]$ نتیجه ٣.١١ نتیجه می دهد که ریشه $n-$ام واحد $\mathbb{F}_q$ است پس $q - ١$ باید ضریبی از n باشد. لذا $a = q + ١ - n^٢ \equiv ٢ \pmod{n}$

ادامه اثبات:

برای برخی k می نویسیم $a = ٢ + kn$ در این صورت $n^٢ = q + ١ - a = q - ١ - kn$ لذا $q = n^٢ + kn + ١$. طبق قضیه هس داریم $|٢ + kn| \leq ٢\sqrt{q}$ با مربع کردن نامساوی اخیر داریم $k^٢n^٢ + ۴kn + ۴ \leq ۴q = ۴(n^٢ + kn + ١)$ پس $|k| \leq ٢$. با بیان این مطلب که $k = ٠, \pm١, \pm٢$ مقادیر احتمالی q هستند اثبات به پایان می رسد.

تعریف

عدد n را مانده مربعی به پیمانه p نامیم هرگاه n با مربع یک عدد در پیمانه p همنهشت باشد.

عدد n را نامانده مربعی به پیمانه p نامیم هرگاه n با مربع هیچ عددی در پیمانه p همنهشت نباشد.

مثال

در پیمانه ١٣ مانده های مربعی اعداد $١^٢ \equiv ١, ٣^٢ \equiv ٩, ٢^٢ \equiv ۴, ۴^٢ \equiv ٣, ۶^٢ \equiv ١٠, ٨^٢ \equiv ١٢$ هستند و اعداد ٢,٥,۶,٧,٨,١١ نامانده های مربعی هستند

توجه

بسیاری از مواقع مقادیر q همانند قضیه قبل داده نمی شوند و در بسیاری از خم ها رابطه

$E(\mathbb{F}_q) \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ برقرار نیست (فقط تعداد کمی کسر از مرتبه n^2 داریم) پس حالت $\mathbb{Z}_n \oplus \mathbb{Z}_n$ به ندرت اتفاق می افتد یعنی تعداد زیادی q موجود است که خم بیضوی روی میدان $\mathbb{F}_q$ دارای نقاط با مرتبه بیشتر از $4\sqrt{q}$ هستند (تمرن ۴.۶) پس به ندرت می توانیم نقاط را پیدا کنیم که مرتبه شان باعث تعیین $E(\mathbb{F}_q)$ شوند

در زیر نشان داده بیان می شود که برای خم E روی میدان $\mathbb{F}_q$ نقطه ای با مرتبه به طور کافی بزرگ هست که روی E و هم روی پیچش مربعی آن موجود است.

تعریف

فرض کنید $d \in \mathbb{F}_q^{\times}$ یک نامانده مربعی در پیمانه p باشد اگر E دارای معادله $y^2 = x^3 + Ax + B$ باشد آنگاه پیچش مربعی E' دارای معادله $y^2 = x^3 + Ad^2x + Bd^3$ است. (تمرین ۲.۲۳)

نکته

طبق تمرین ۴.۱۰ اگر $\#E(\mathbb{F}_q) = p + 1 - a$ آنگاه E' دارای $p + 1 + a$ نقطه است. پس اگر ما مرتبه یکی از این دو گروه را بدانیم آنگاه a را می یابیم و از روی آن می توانیم مرتبه هر دو گروه را محاسبه کنیم.

قضیه ٤.١٨(مهم)

فرض کنید $p > 229$ یک عدد اول باشد و E یک خم بیضوی روی $\mathbb{F}_q$ باشد در این صورت هر دو گروه E و E' (پیچش مربعی) دارای نقطه ای مثل p هستند که مرتبه اش یک ضریب در بازه

$(p + 1 - 2\sqrt{q}, p + 1 + 2\sqrt{q})$ دارد.

اثبات

حذف

مثال ٤.١٩

در این مثال نشان می دهیم که قضیه بالا برای $p = 229$ درست نیست زیرا خم $E: y^2 = x^3 - 1$ را در نظر بگیرید محاسبات نشان می دهد که $E(\mathbb{F}_{229}) \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{42}$. پس $42P = \infty$ برای تمام $P \in E(\mathbb{F}_{229})$. کران های هس بیان می کند $200 \leq \#E(\mathbb{F}_{229}) \leq 260$ پس وجود یک نقطه از مرتبه ۴۲ هر

دو مقدار ۲۱۰ و ۲۵۲ را نتیجه می دهد. چون ۲ نامانده مربعی به پیمانه ۲۲۹ است خم $E': y^2 = x^3 - 8$ پیچش مربعی E است یک محاسبه نشان می دهد $E'(\mathbb{F}_{229}) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_{52}$ پس $52P = \infty$ برای تمام نقاط $P \in E'(\mathbb{F}_{229})$. وجود نقطه ای از مرتبه ۵۲ دو مقدار ۲۰۸ و ۲۶۰ را نتیجه می دهد پس نه E و نه E' دارای نقطه ای که ضریب اش در بازه هس باشد نیستند.

گام کوچک، گام بزرگ Baby step, Giant step

فرض کنیم $P \in E(\mathbb{F}_q)$. می خواهیم مرتبه P را محاسبه کنیم. ابتدا یک عدد صحیح مثل k را پیدا می کنیم که $kP = \infty$. فرض کنید $\#E(\mathbb{F}_q) = N$. طبق قضیه لاگرانژ $NP = \infty$ البته ما هنوز مقدار دقیق N را نمی دانیم ولی می دانیم $q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$. باید تمام مقادیر N را در این رابطه قرار داده و مشخص کنیم کدام یک در $NP = \infty$ صدق می کند. این کار به $4\sqrt{q}$ مرحله نیازمند است. ولی ممکن است آن را به تعداد $4q^{1/4}$ مرحله طبق الگوریتم زیر کاهش دهیم.

۱- محاسبه کن $Q = (q+1)P$

۲- عدد صحیح m را که $m > q^{1/4}$ انتخاب کن و نقاط jP را برای $j = 0,1,2,\dots,m$ محاسبه و ذخیره کن.

۳- نقاط $Q + k(2mP)$ را به ازای $k = -m, -(m-1), \dots, m$ تا زمانی که این نقاط با $\pm j$ برخورد کنند یعنی $Q + k(2mP) = \pm j$

۴- نتیجه بگیر $(q + 1 + 2m \mp j)P = \infty$. فرض کن $M = q + 1 + 2m \mp j$

۵- M را به عوامل اول $p_1, \dots, p_r$ تجزیه کن

۶- برای $i = 1, \dots, r$، آنگاه M را با $\left(M/p_i\right)P$ را محاسبه کن. اگر $M/p_i = \infty$ برای برخی i، M/p_i عوض کن و به مرحله ۵ برگرد. و اگر $M/p_i \neq \infty$ برای تمام i ها آنگاه M مرتبه نقطه P است.

۷- برای یافتن $\#E(\mathbb{F}_q)$ مراحل اول تا ششم را برای نقاط تصادفی در $E(\mathbb{F}_q)$ تکرار می کنیم تا زمانی که کوچکترین مضرب مشترک مرتبه ها فقط یک N را که $q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$ عاد کند، در این صورت $N = \#E(\mathbb{F}_q)$.

لم ٤.٢٠

فرض کنید a یک عدد صحیح باشد که $|a| \leq ۲m^۲$. در این صورت اعداد صحیح $a_۰$ و $a_۱$ که

$a = a_۰ + ۲ma_۱$ و $-m < a_۰ \leq m$ و $-m \leq a_۱ \leq m$ موجودند بطوریکه

اثبات

فرض کنید $a_۰ \equiv a \ (mod\ ۲m)$ که $-m < a_۰ \leq m$ و در این صورت $a_۱ = {(a - a_۰)}/{۲m}$

$$|a_۱| \leq {۲m^۲ + m}/{۲m} < m + ۱$$

نکته

لم فوق بیان می کند که در مرحله ۳ برخورد اتفاق می افتد. فرض کنید $a_۰ \equiv a \ (mod\ ۲m)$ همانند لم باشد و $k = -a$. در این صورت داریم

$$Q + k(۲mP) = (q + ۱ - ۲ma_۱)P = (q + ۱ - a + a_۰)P = NP + a_۰P = a_۰P = \pm jP$$

که در آن $j = |a_۰|$

لم ٤.٢١

فرض کنید G یک گروه جمعی (با عنصر همانی ۰) و $g \in G$ باشد. فرض کنید برای برخی اعداد صحیح مثبت M داشته باشیم $Mg = ۰$ و همچنین فرض کنید $p_۱, \dots, p_r$ مقسوم علیه های دوبدو متمایز M باشند. اگر $\left({M}/{p_i}\right)g \neq ۰$ برای تمام i ها. آنگاه M مرتبه g است.

اثبات

فرض کنیم k مرتبه g باشد پس $k \mid m$ و فرض کنید $k \neq m$. فرض کنید p_i عدد اولی باشد که $m \mid k$.

لذا $p_ik \mid m$ پس $k \mid \left({M}/{p_i}\right)$ در نتیجه $\left({M}/{p_i}\right)g = ۰$ که با فرض متناقض است پس $k = m$

نکته

لم بالا بیان می کند که مرحله ۶ مرتبه P را بدست می دهد.

توجه

۱- برای صرفه جویی در حافظه ممکن است نگهداری مختصات x نقاط jP کافی باشد زیرا یافتن نقاط برخورد $\pm jP$ فقط به مختصات x بستگی دارد (با فرض این که با فرم وایرشتراس خم کار می کنیم) وقتی برخورد انجام شد، مختصات y را می توان محاسبه کرد.

۲- برای محاسبه $Q + k(۲mP)$ می توان یک بار برای همیشه Q و یک بار $۲mP$ را محاسبه کرد. برای بدست آوردن $Q + (k + ۱)(۲mP)$، $Q + k۲mP$ را با $۲mP$ جمع می بندیم. بطور مشابه یک jP محاسبه می شود و برای محاسبه $(j + ۱)P$، P را با jP جمع می بندیم.

۳- ما قبلا فرض کردیم که M را می توان تجزیه کرد. اگر چنین نباشد می توان حداقل تمام عامل های p_i کوچک را پیدا کرد و برای این ها $\left(M/p_i\right)P = ۰$ را محاسبه کرد.
در این صورت M نماینده خوبی برای مرتبه گروه خواهد شد.

۴- علت نامگذاری این روش به گام کوچک، گام بزرگ چیست؟ گام کوچک از محاسبه jP به $(j + ۱)P$ و گام بزرگ از محاسبه $k(۲mP)$ به $(k + ۱)۲mP$ می آید زیرا ما مرحله بزرگ $۲mP$ را پشت سر می گذاریم.

مثال ٤.١١

فرض کنید E خم بیضوی $y^۲ = x^۳ - ۱۰x + ۲۱$ روی $\mathbb{F}_{۵۵۷}$ باشد (همانند مثال ۴.۷) و فرض کنید $P = (۲,۳)$.

روند فوق را برای این مثال بررسی می کنیم

۱- $Q = ۵۵۸P = (۴۱۸,۳۳)$
۲- فرض کنید $m = ۵$ که بزرگتر از $۵۵۷^{۱/۴}$ است فهرست jP بصورت زیر است.

$$\infty, (۲,۳), (۵۸,۱۶۴), (۴۴,۲۹۴), (۵۶,۳۳۹), (۱۳۲,۳۶۴)$$

۳- وقتی $k = ۱$ داریم $Q + k(۲mP) = (۲,۳)$ که برخورد در نقاط در لیست ما به ازای $j = ۱$ انجام می گیرد.

۴- داریم $(q+۱+۲mk-j)P = ۵۶۷P = \infty$

۵- داریم $۵۶۷ = ۳^۴ \cdot ۷$. بدست می آوریم $\left(\frac{۵۶۷}{۳}\right)P = ۱۸۹P = \infty$. حال ۱۸۹ را به عنوان نماینده برای مرتبه P داریم.

۶- داریم $۱۸۹ = ۳^۳ \cdot ۷$. بدست می آوریم $\left(\frac{۱۸۹}{۳}\right)P = (۳۸,۵۳۵) \neq \infty$ و

$\left(\frac{۱۸۹}{۷}\right)P = (۱۳۶,۳۶۰) \neq \infty$

لذا ۱۸۹ مرتبه P است.

این نقطه را همانند مثال ۴.۷ کافیست در نظر بگیریم $\#E(\mathbb{F}_{۵۵۷}) = ۵۶۷$

خانواده منحنی ها

در این بخش فرمولی برای تعداد نقاط $E(\mathbb{F}_p)$ پیدا می کنیم که خم E خم $y^۲ = x^۳ - kx$ است و

$k \not\equiv ۰ \pmod p$

قضیه ٤.٢٣

فرض کنید p یک عدد اول فرد و $k \not\equiv ۰ \pmod p$. فرض کنید $N_p = \#E(\mathbb{F}_q)$ که E یک خم بیضوی است با معادله $y^۲ = x^۳ - kx$

۱- اگر $p \equiv ۳ \pmod ۴$ آنگاه $N_p = p + ۱$

۲- اگر $p \equiv ۱ \pmod ۴$ می نویسیم $p = a^۲ + b^۲$ که a و b اعداد صحیح و b زوج است و $a + b \equiv ۱ \pmod ۴$ در این صورت

$$N_p = \begin{cases} p + ۱ - ۲a & \text{اگر } k \text{ یک توان چهارم به پیمانه } p \text{ باشد} \\ p + ۱ + ۲a & \text{اگر } k \text{ مربع به پیمانه } p \text{ باشد ولی توان چهارم به پیمانه } p \text{ نباشد} \\ p + ۱ \pm ۲b & \text{اگر } k \text{ مربع به پیمانه } p \text{ نباشد} \end{cases}$$

اثبات: حذف

خم های فوق منفرد

تعریف

یک خم E درمرتبه p را فوق منفرد نامیم هرگاه $E[p] = \infty$. بعبارتی دیگر هیچ نقطه ای از مرتبه p، حتی با مختصات در میدان بستار جبری موجود نباشد.

توجه

خم های فوق منفرد با خم های منفرد که قبلا بررسی شده هیچ ارتباطی ندارند. واژه منفرد برای توضیح $j-$ پایاهای یک خم بیضوی با درونریختی میدان های بزرگ تر از $\mathbb{Z}$ است می پردازد. این حلقه معمولا زیر حلقه یک توسیع درجه دوم گویا است. واژه فوق منفرد به $j-$ پایاهای یک خم بیضوی با درونریختی های روی میدان بزرگتر دلخواه ارتباط دارد (زیر حلقه معادلات درجه دوم جبری)

قضیه ٤.٣١

فرض کنید E یک خم بیضوی روی $\mathbb{F}_q$ باشد. که q توانی از عدد اول p است. فرض کنید

$a = q + ١ - \#E(\mathbb{F}_q)$ در این صورت E فوق منفرد است اگر و تنها اگر $a \equiv ٠ \pmod p$. یعنی اگر و تنها اگر $\#E(\mathbb{F}_q) \equiv ١ \pmod p$

اثبات

می نویسیم $X^٢ - aX + q = (X - \alpha)(X - \beta)$. طبق قضیه ۴.۱۲ داریم

$$\#E(\mathbb{F}_{q^n}) = q^n + ١ - (\alpha^n + \beta^n)$$

لم ۴.۱۳ بیان می کند که $s_n = \alpha^n + \beta^n$ در رابطه بازگشتی زیر صدق می کند.

$$s_{n+١} = as_n - qs_{n-١}\ ،\ s_١ = a\ ،\ s_٠ = ٢$$

فرض کنید $a \equiv ٠ \pmod p$ در این صورت $s_١ = a \equiv ٠ \pmod p$ و $s_{n+١} \equiv ٠ \pmod p$ برای تمام $n \geq ١$. بنابراین $\#E(\mathbb{F}_{q^n}) = q^n + ١ - s_n \equiv ١ \pmod p$.

بنابراین برای $n \geq ١$ هیچ نقطه ای با مرتبه p در $E(\mathbb{F}_{q^n})$ وجود ندارد. چون $\overline{\mathbb{F}_q} = \bigcup_{n \geq ١} \mathbb{F}_{q^n}$ پس هیچ نقطه ای با مرتبه p در $E(\overline{\mathbb{F}_q})$ وجود ندارد. بنابراین E فوق منفرد است.

حال فرض کنید $a \not\equiv ۰ \pmod p$ رابطه بازگشتی نتیجه می دهد $s_{n+۱} \equiv as_n \pmod p$ برای تمام $n \geq ۱$. چون $s_۱ = a$ داریم $s_n \equiv a^n \pmod p$ برای تمام $n \geq ۱$. بنابراین

$$\#E(\mathbb{F}_{q^n}) = q^n + ۱ - s_n \equiv ۱ - a^n \pmod p$$

طبق قضیه کوچک فرما $a^{p-۱} \equiv ۱ \pmod p$ بنابراین $E(\mathbb{F}_{q^{p-۱}})$ دارای مرتبه بخش پذیر بر p است بنابراین دارای نقطه ای با مرتبه p است. و این یعنی E فوق منفرد نیست.

برای قسمت آخر قضیه توجه داریم که $\#E(\mathbb{F}_q) = q + ۱ - a \equiv ۱ - a \pmod p$. بنابراین $\#E(\mathbb{F}_q) \equiv ۱ \pmod p$ اگر و تنها اگر $a \equiv ۰ \pmod p$.

قضیه ٤.٣٢

فرض کنید $p \geq ۵$ عددی اول باشد و E روی $\mathbb{F}_p$ تعریف شود. در این صورت E فوق منفرد است اگر و تنها اگر $a = ۰$ و این یعنی اگر و تنها اگر $\#(\mathbb{F}_p) = p + ۱$.

اثبات

اگر $a = ۰$ آنگاه طبق قضیه قبل E فوق منفرد است. برعکس فرض کنید E فوق منفرد باشد ولی $a \neq ۰$. در این صورت $a \equiv ۰ \pmod p$ نتیجه می دهد $|a| \geq p$. طبق قضیه هس $|a| \leq ۲\sqrt{p}$ بنابر این داریم $p \leq ۲\sqrt{p}$ یعنی $p \leq ۴$.

قضیه ٤.٣٣

فرض کنید q یک عدد اول و $q \equiv ۲ \pmod ۳$. فرض کنید $B \in \mathbb{F}_q{}^{\times}$ در این صورت خم بیضوی E با معادله $y^۲ = x^۳ + B$ یک خم فوق منفرد است.

اثبات

فرض کنید $\psi: \mathbb{F}_q{}^{\times} \to \mathbb{F}_q{}^{\times}$ همریختی باشد که با معادله $\psi(x) = x^۳$ تعریف شده باشد. چون $q - ۱$ ضریبی از سه نیست،هیچ عضوی از مرتبه ۳ در $\mathbb{F}_q{}^{\times}$ وجود ندارد. بنابراین هسته ψ همانی است. بنابراین ψ یک بیک است بنابراین باید پوشا باشد زیرا یک نگاشت از یک گروه متناهی به خودش است. مخصوصا هر عضو از $\mathbb{F}_p$ دارای ریشه سوم منحصر به فرد در $\mathbb{F}_p$ است.

برای هر $y \in \mathbb{F}_p$ یک $x \in \mathbb{F}_p$ موجود است بطوریکه (x, y) در معادله خم صدق می کند یعنی x یک ریشه سوم منحصر به فرد از $x^3 + B$ است. چون q دارای مقادیر y است می توانیم q را محاسبه کنیم.

با اضافه کردن نقطه در بینهایت نتیجه می گیریم $\#E(\mathbb{F}_p) = q + 1$ بنابراین E فوق منفرد است.

ویژگی های این خم

برخی محاسبات گروهی در آن ها سریعتر انجام می گیرد. فرض کنیم E یک خم فوق منفرد روی $\mathbb{F}_p$ بوده و $P = (x, y)$ نقطه ای از $E(\mathbb{F}_{q^n})$ باشد ($n \geq 1$ معمولا بزرگ است) فرض کنیم k یک عدد صحیح مثبت باشد می خواهیم kP را محاسبه کنیم. یک روش این است که در دوبرابر کردن های متوالی kP را بدست آوریم. ولی روش سریع تر به این صورت است که فرض کنیم $a = 0$ در این صورت بنابر قضیه ۴.۱۰ داریم $\varphi_q^2 + q = 0$ از آنجا:

$$q(x, y) = -\varphi_q^2(x, y) = -\varphi_{q^2}(x, y) = -\left(x^{q^2}, y^{q^2}\right) = \left(x^{q^2}, -y^{q^2}\right)$$

همان طور که ملاحظه می شود سمت راست محاسبات در میدان انجام می گیرند که خیلی سریعتر از محاسبات گروهی است. بنابراین برای محاسبه kP، بصورت زیر عمل می کنیم:

۱- k را به مبنای q می بریم $k = k_0 + k_1 q + k_2 q^2 + \cdots + k_r q^r$

۲- $k_i P$ را محاسبه می کنیم $k_i P = (x_i, y_i)$ که $0 \leq k_i < q$ (محاسبات گروهی)

۳- محاسبه می کنیم $q^i k_i P = \left(x_i^{q^{2i}}, (-1)^i y_i^{q^{2i}}\right)$ (محاسبات میدانی)

۴- حال مجموع نهایی را از (۱) پیدا می کنیم برای هر $0 \leq i \leq r$

فرض کنیم خم های E_1 و E_2 که هر دو روی یک میدان تعریف شده اند طوری باشند که با یک تغییر متغیر به همدیگر تبدیل شوند در این صورت ثابت می شود که E_1 فوق منفرد است اگر و تنها اگر E_2 فوق منفرد باشد.

برای مثال اگر $E_1: y_1^2 = x_1^3 + B$ و $E_2: y_2^2 = x_2^3 + 1$ و با تغییر متغیر $x_2 = \frac{x_1}{\sqrt[3]{B}}$ و $y_2 = \frac{y_1}{\sqrt{2B}}$ به همدیگر تبدیل می شوند به جای این که روی خم E_1 مطالعه کنیم، روی خم E_2 مطالعه می کنیم که آسان تر است در بخش ۲.۵.۱ دیدیم که یک خم بیضوی روی یک میدان به طور جبری بسته را که مشخصه اش مخالف ۲ است می توان با نماد لژاندر زیر نوشت: $y^2 = x(x-1)(x-\lambda) \quad \lambda \neq 0,1$

قضیه ٤.٣٤

فرض کنیم p یک عدد اول فرد باشد و چند جمله ای زیر را تعریف می کنیم $H_p(T)=\sum_{i=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{i}^2 T^i$

در این صورت خم بیضوی E با معادله $y^2=x(x-1)(x-\lambda)$ که $\lambda\in\overline{\mathbb{F}_p}$ لذا n ای هست که $\lambda\in\mathbb{F}_{p^n}=\mathbb{F}_q$ (فرض می کنیم $p^n=q$ و E روی $\mathbb{F}_q$ تعریف شده است)

برای بررسی فوق منفرد بودن E روی $\mathbb{F}_q$ کافیست نقاط $E[\mathbb{F}_q]$ را بشماریم حال بنابر تمرین ۴.۴ داریم $\left(\frac{x}{\mathbb{F}_q}\right)=x^{\frac{q-1}{2}}$ در $\mathbb{F}_q$. حال بنابر قضیه ۴.۱۴ داریم

$$\#E(\mathbb{F}_q)=q+1+\sum_{x\in\mathbb{F}_q}\left(x(x-1)(x-\lambda)\right)^{\frac{q-1}{2}}$$

در ادامه اثبات قضیه به اثبات لم زیر می پردازیم

لم ٤.٣٥

فرض کنیم $i\in\mathbb{Z}^+$ در این صورت $\sum_{x\in\mathbb{F}_q}(x)^i=\begin{cases}0 & q-1\nmid i\\ -1 & q-1\mid i\end{cases}$

اثبات:

ابتدا فرض کنیم $q-1|i$ در این صورت برای هر $x\neq 0$ داریم

(چون $q-1$ مرتبه گروه ضربی است) $x^i=x^{(q-1)k}=(x^{q-1})^k=1$ در نتیجه در $\mathbb{F}_q$ داریم

$$\sum_{x\in\mathbb{F}_q}(x)^i=0+\sum_{x\in\mathbb{F}_q}(x)^i=\sum_{x\in\mathbb{F}_q}1=q-1=-1$$

حال فرض کنیم $q-1\nmid i$ در این صورت چون ${\mathbb{F}_q}^\times$ یک گروه ضربی دوری است پس دارای یک مولد مثل g می باشد پس هر عضو ${\mathbb{F}_q}^\times$ را می توان بصورت g^j نوشت که $0\leq j\leq q-2$ لذا داریم

$$\sum_{x\in\mathbb{F}_q}(x)^i=0+\sum_{x\in\mathbb{F}_q}(x)^i=\sum_{j=0}^{q-2}\left(g^j\right)^i=\sum_{j=0}^{q-2}\left(g^i\right)^j=\frac{(g^i)^{q-1}-1}{(g)^i-1}=0$$

بدین ترتیب اثبات لم به پایان رسید.

ادامه اثبات: حال اگر $\left(x(x-1)(x-\lambda)\right)^{\frac{q-1}{2}}$ را بسط دهیم یک چند جمله ای از درجه $\frac{3(q-1)}{2}$ خواهیم داشت که در آن جمله ثابت نداریم و فقط جملات x^i ظاهر می شوند. و تنها مضربی از i با خاصیت $(q-1)i$ که در جملات x^i ظاهر می شود خود $q-1$ است. لذا فقط یک جمله x^{q-1} را داریم. حال اگر ضریب x^{q-1} را A_q بنامیم آنگاه داریم: $\sum_{x\in\mathbb{F}_q}\left(x(x-1)(x-\lambda)\right)^{q-1} = A_q x^{q-1} = -A_q$ که تساوی آخر از لم نتیجه شده است.

بنابراین چون $\mathbb{F}_q$ هستیم داریم:

$$\#E(\mathbb{F}_q) = q + 1 - A_q = 1 - A_q$$

حال بنابر گزاره ۴.۳۱، E فوق منفرد است اگر و تنها اگر $1 - A_q = 1$ یا $A_q = 0$ (در $\mathbb{F}_q$)

لم زیر را ثابت می کنیم که ارتباط بین A_q و A_p را نشان می دهد.

لم ٤.٣٦

فرض می کنیم که $f(x) = x^3 + c_2x^2 + c_1x^1 + c_0$ یک چند جمله ای درجه ۳ با ضرایب در میدانی از مشخصه p باشد. فرض می کنیم برای هر $r \geq 1$، A_{p^r} ضریب x^{p^r-1} در $f(x)^{\frac{p^r-1}{2}}$ باشد در این صورت دایم $A_{p^r} = {A_p}^{1+p+p^2+\cdots+p^{r-1}}$

اثبات

داریم

$$\left(f(x)^{\frac{p-1}{2}}\right)^{p^r} = \left(x^{\frac{3(p-1)}{2}} + \cdots + A_p x^{p-1} + \cdots\right)^{p^r} =$$

$$= x^{\frac{3(p-1)p^r}{2}} + \cdots + {A_p}^{p^r} x^{(p-1)p^r} + \cdots \Longrightarrow \left(f(x)^{\frac{p-1}{2}}\right)^{p^r} = f(x)^{\frac{p^{r+1}-p^r}{2}}$$

$$= f(x)^{\frac{p^{r+1}-1}{2}} . f(x)^{\frac{-(p^r-1)}{2}}$$

$$\Longrightarrow f(x)^{\frac{p^{r+1}-1}{2}} = f(x)^{\frac{(p^r-1)}{2}} \left(f(x)^{\frac{p-1}{2}}\right)^{p^r} =$$

$$= \left(x^{\frac{۳(p^r-۱)}{۲}} + \cdots + A_{p^r} x^{p^r-۱} + \cdots\right)\left(x^{\frac{۳(p-۱)p^r}{۲}} + \cdots + A_{p}{}^{p^r} x^{p^r(p-۱)} + \cdots\right)$$

برای بدست آوردن ضریب $x^{p^{r+۱}-۱}$ اندیس های i و j را طوری انتخاب می کنم که $i + j = p^{r+۱} - ۱$ ضرایب متناظر از اولین و دومین عامل در ضرب بالا را ضرب می کنیم و روی i و j جمع می کنیم. یک جمله با $۰ \le i \le \frac{۳(p-۱)}{۲}$ از عامل اول و یک جمله با

$$p^{r+۱} - ۱ \ge j \ge (p^{r+۱} - ۱) - \tfrac{۳}{۲}(p^r - ۱) > (p - ۲)p^r$$

از عامل دوم به دست می آید از آنجایی که همه توان های عامل دوم مضرب p^r هستند تنها اندیس j در این محدوده که توان غیر صفر دارد $j = (p - ۱)p^r$ است. اندیس متناظر i نیز $p^r - ۱$ است. حاصلضرب این ضرایب به صورت زیر می باشد. $A_{p^{r+۱}} = A_{p^r}.A_{p}{}^{p^r}$

این رابطه به طور بدیهی برای $r = ۱$ برقرار است. حال فرض می کنیم که برای $r \le n$ نیز برقرار باشد برای $n + ۱$ حکم را ثابت می کنیم.

$$A_{p^{n+۱}} = A_{p^r}.A_{p}{}^{p^n} = A_{p}{}^{۱+p+p^۲+\cdots+p^{n-۱}}.A_{p}{}^{p^n} = A_{p}{}^{۱+p+p^۲+\cdots+p^{n-۱}+p^n}$$

و لذا حکم ثابت می شود.

ادامه اثبات قضیه:

بنابراین با استفاده از لم می توان گفت که E فوق منفرد است اگر و تنها اگر $A_p = ۰$. (A_p به p بستگی دارد و مستقل از توان p در $p^n = q$ است.)

حال A_p را به صورت یک چند جمله ای از λ بیان می کنیم. ضریب $x^{p-۱}$ یعنی A_p در $\left(x(x-۱)(x-\lambda)\right)^{\frac{p-۱}{۲}}$ برابر با ضریب $x^{\frac{p-۱}{۲}}$ در $\left((x-۱)(x-\lambda)\right)^{\frac{p-۱}{۲}}$ است. این ضریب را محاسبه می کنیم.

بنابر قضیه دو جمله ای داریم:

$$(x-۱)^{\frac{p-۱}{۲}} = \sum_i \binom{\frac{p-۱}{۲}}{i} x^i (-۱)^{\frac{p-۱}{۲}-i}$$

$$(x-\lambda)^{\frac{p-1}{2}} = \sum_j \binom{\frac{p-1}{2}}{j} x^{\frac{p-1}{2}-j}(-\lambda)^j$$

حال A_p (ضریب $(x)^{\frac{p-1}{2}}$) در $\left((x-1)(x-\lambda)\right)^{\frac{p-1}{2}}$ برابر

$(-1)^{\frac{p-1}{2}}\sum_{k=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{k}^2\lambda^k = (-1)^{\frac{p-1}{2}}H_p(\lambda)$ است.

بنابراین E فوق منفرد است اگر و تنها اگر $H_p(\lambda)=0$.

قضیه ۴.۳۷

فرض کنید $p \geq 5$ یک عدد اول باشد. در این صورت خم بیضوی $y^2 = x^3 + 1$ روی $\mathbb{F}_p$ فوق منفرد است اگر و تنها اگر $p \equiv 2 \pmod 3$.

و بیضوی $y^2 = x^3 + x$ روی $\mathbb{F}_p$ فوق منفرد است اگر و تنها اگر $p \equiv 3 \pmod 4$.

فصل ۸: خم های بیضوی روی $\mathbb{Q}$

همان طور که در فصل ۱ دیدیم خم های بیضوی روی $\mathbb{Q}$ رده مهمی از معادلات دیوفانت را تشکیل می دهند. در این فصل ما ساختار گروهی مجموعه نقاط با مختصات گویای یک خم بیضوی روی $\mathbb{Q}$ را مطالعه خواهیم کرد. در ابتدا نشان خواهیم داد که نقاط تاب (نقاط با مرتبه متناهی) بسیار سریعتر حاصل می شوند. سپس قضیه موردل – ویل را اثبات خواهیم کرد که بیان می کند $E(\mathbb{Q})$ یک گروه آبلی متناهیا تولید شده است.

زیرگروه تاب. قضیه لوت-ناگیل

زیرگروه تابی $\mathrm{E}(\mathbb{Q})$ به راحتی قابل محاسبه است. در این بخش مثالی ارائه می دهیم که جزئیات این کار را نشان می دهد

تعریف

فرض کنیم $\frac{a}{b} \neq ۰$ یک عدد گویا باشد که $gcd(a,b) = ۱$. فرض کنیم $\frac{a}{b} = p^r \frac{a_۱}{b_۱}$ بطوریکه $p \nmid a_۱ b_۱$ که p یک عدد اول و r یک عدد صحیح است. در این صورت ارزش p – ای $\frac{a}{b}$ را بصورت زیر تعریف می کنیم $v_p\left(\frac{a}{b}\right) = r$

قرارداد می کنیم که $v_p(۰) = \infty$

مثال

داریم $v_۷\left(\frac{۱}{۲}\right) = ۰$ و $v_۵\left(\frac{۵۰}{۳}\right) = ۲$ و $v_۲\left(\frac{۷}{۴۰}\right) = -۳$

تعریف:

فرض کنیم $y^۲ = x^۳ + Ax + B$ باشد که در آن $A, B \in \mathbb{Z}$. فرض کنیم $r \in \mathbb{Z}^+$ تعریف می کنیم

$$E_r = \left\{(x,y) \in \mathrm{E}(\mathbb{Q}) \middle| v_p(x) \leq -۲r,\ \ v_p(y) \leq -۳r\right\} \cup \{\infty\}$$

بین E_r ها رابطه زیر برقرار است: $E_۱ \subseteq E_۲ \subseteq E_۳ \ldots$

می توان گفت که هر نقطه از E_r نقطه ای است که در پیمانه توان های p به بینهایت نزدیک است. یعنی بطور $p-$ ای به بینهایت میل می کند.

قضیه ۸.۱

فرض کنید $E: y^2 = x^3 + Ax + B$ یک خم بیضوی باشد که $A, B \in \mathbb{Z}$. فرض کنیم $r \in \mathbb{Z}^+$ و p یک عدد اول باشد.

۱- E_v زیرگروهی از $\mathrm{E}(\mathbb{Q})$ است.

۲- اگر $(x,y) \in \mathrm{E}(\mathbb{Q})$ باشد آنگاه $v_p(x) < 0 \Leftrightarrow v_p(y) < 0$

در این صورت عدد صحیح r موجود است بطوری که $v_p(y) \le -3r,\ \ v_p(x) \le -2r$

۳- نگاشت $\lambda_r : \frac{E_v}{E_{5v}} \longrightarrow \mathbb{Z}_{p^{4r}}$ که $(x,y) \mapsto p^{-r}\frac{x}{y}\ (mod\ p^{4r})$ و $0 \longmapsto \infty$ یک هومرفیسم یک بیک است که در آن $\mathbb{Z}_{p^{4r}}$ یک گروه جمعی است.

۴- اگر $(x,y) \in E_r$ و $(x,y) \notin E_{r+1}$ آنگاه $\lambda_r(x,y) \not\equiv 0\ (mod\ p)$.

اثبات:

اثبات۲

مخرج کسر $x^3 + Ax + B$ معادل مخرج کسر y^2 می باشد. p مخرج کسر y را عاد می کند. اگر و تنها اکر p مخرج کسر x را عاد کند.

اگر p^j که $j > 0$ توان دقیقی از p باشد که مخرج کسر y را عاد کند آنگاه p^{2j} که $j > 0$ توان دقیقی از p می باشد که مخرج کسر y^2 را عاد می کند. به طور مشابه اگر p^k که $k > 0$ توان دقیقی از p باشد که مخرج کسر x را عاد کند آنگاه p^{3k} دقیقا مخرج کسر $x^3 + Ax + B$ را عاد می کند بنابراین $2j = 3k$ و این بیان می کند r ای موجود است که $j = 3r$ و $k = 2r$.

اثبات ۴

می دانیم

$$E_r = \{(x,y) \in \mathrm{E}(\mathbb{Q}) \mid v_p(x) \le -2r,\ \ v_p(y) \le -3r\} \cup \{\infty\}$$

همچنین می بینیم که مجموعه

$$\{(x,y)\in E_r \mid v_p(x)\le -2r,\ \ v_p(y)\le -3r\}=\left\{(x,y)\in E_r \middle| v_p\left(\frac{x}{y}\right)=r\right\}$$

یک مجموعه از E_r است که در E_{r+1} قرار ندارد. داریم

$$\lambda_r(x,y)\equiv p^{-r}\frac{x}{y}\ (mod\ p^{4r})=p^{-r}\frac{a\times p^{-2}}{b\times p^{-3}}\equiv p^{-r}p''\not\equiv 0\ (mod\ p)$$

اثبات۳

می خواهیم ثابت کنیم λ_r یک همریختی یک بیک است.

اگر $\lambda_r(x,y)\equiv 0\ (mod\ p^{4r})$ آنگاه $v_p\left(\frac{x}{y}\right)\ge 5r$ در نتیجه $(x,y)\in E_{5r}$ زیرا داریم

$$\lambda_r(x,y)\equiv p^{-r}\frac{x}{y}\ (mod\ p^{4r})\equiv 0\ (mod\ p^{4r})\xrightarrow{\text{ضرب طرفین در } p^r}\frac{x}{y}\equiv 0\ \ (mod\ p^{5r})$$
$$\Longrightarrow p^{5r}\mid\frac{x}{y}\Longrightarrow v_p\left(\frac{x}{y}\right)\ge 5r\Longrightarrow(x,y)\in E_{5r}$$

پس می توان نتیجه گرفت λ_r یک بیک است در صورتی که بپذیریم λ_r یک همریختی است.

نشان می دهیم λ_r همریختی است.

فرض کنیم $s=\frac{1}{y}$ و $t=\frac{x}{y}$ با تقسیم معادله $y^2=x^3+Ax+B$ بر y^3 خواهیم داشت

$$s=t^3+Ats^2+Bs^3$$

$p^j\mid z$ که در آن z یک عدد گویا است را با نماد $z\equiv 0\ \ (mod\ p^j)$ نمایش می دهیم.

لم زیر را بدون اثبات می پذیریم

لم ۸.۳

الف) $p^{3r}\mid s\Leftrightarrow(x,y)\in E_r$

ب) $p^{3r}\mid s$ آنگاه $p^r\mid t$

داریم

$$\lambda_r\big(-(x,y)\big) = \lambda_r(x,-y) = p^{-r}\frac{x}{y} = -\lambda_r(x,y)$$

ادعا می کنیم که اگر $P_۱ + P_۲ + P_۳ = \infty$ آنگاه

$$\lambda_r(P_۱) + \lambda_r(P_۲) + \lambda_r(P_۳) \equiv ۰ \ (mod\ p^{۴r})$$

از این ادعا استفاده می کنیم و آن را بعدا ثابت خواهیم کرد.

$$P_۱ + P_۲ + P_۳ = \infty \Longrightarrow \lambda_r(P_۱ + P_۲ + P_۳) \equiv ۰ \ (mod\ p^{۴r})$$

حال می خواهیم نشان دهیم λ_r همریختی است. در این صورت $P_۱, P_۲ \in E_r$ نتیجه می دهد $P_۳ \in E_r$ لذا E_r زیرگروهی از $\mathrm{E}(\mathbb{Q})$ است. بنابراین

$$\lambda_r(P_۱ + P_۲) = \lambda_r(-P_۳) = -\lambda_r(P_۳) = \lambda_r(P_۱) + \lambda_r(P_۲)$$

پس λ_r همریختی است.

طبق تمرین ۲.۶ سه نقطه $P_۱, P_۲, P_۳$ هم خط اند.

حال ادعا را ثابت می کنیم

فرض کنیم $P_۱, P_۲, P_۳$ روی خط $ax + by + d = ۰$ قرار بگیرد و فرض کنیم $P_۱, P_۲ \in E_r$ با تقسیم معادله فوق بر y خواهیم داشت $at + b + ds = ۰$. فرض کنیم P_i' نقطه متناظر P_i باشد، در مختصات s-t است. اگر $P_i = (x_i, y_i)$ آنگاه $P_i' = (s_i, t_i)$ که در آن $s_i = \frac{۱}{y_i}$ و $t_i = \frac{x_i}{y_i}$ می باشد.

نقاط $P_۱'$ و $P_۲'$ و $P_۳'$ روی خط $at + b + ds = ۰$ قرار می گیرد از آن جا که $P_۱, P_۲ \in E_r$ طبق لم ۸.۳ داریم $p^{۳r} \mid s_i$ و $p^r \mid t_i$ که $i = ۱,۲$ و طبق بخش ۲.۴ مرتبه اشتراک خط $ax + by + d = ۰$ و خم $y^۲ = x^۳ + Ax + B$ در نقطه متناهی (x, y) با استفاده از مختصات تصویری محاسبه می شود.

در حقیقت باید خط و خم را همگن سازی کنیم پس خط $aX + bY + dZ = ۰$ و خم

$ZY^۲ = X^۳ + AX^۲x + BZ^۳$ که $x = \frac{X}{Z}$ و $y = \frac{Y}{Z}$ در نظر می گیریم.

با خط $at+b+ds=0$ و خم $s=t^3+Ats^2+Bs^3$ آغاز می کنیم و خط و خم را همگن می کنیم. $aT+bU+dS=0$ و $SU^2=T^3+ATS^2+BS^3$ که $t=\frac{T}{U}$ و $s=\frac{S}{U}$ می باشد. اگر فرض کنیم $z=S$ و $y=U$ و $x=T$ نقطه (x,y) متناظر با نقطه (s,t) است که

$$t=\frac{T}{U}=\frac{x}{y} \text{ و } s=\frac{S}{U}=\frac{z}{y}$$

پس مرتبه اشتراک خط $ax+by+d=0$ با خم $y^2=x^3+Ax+B$ در نقطه (x,y) برابر با مرتبه اشتراک خط $at+b+ds=0$ و خم $s=t^3+Ats^2+Bs^3$ در نقطه (s,t) است. مثلا خط و خم برحسب متغیرهای x و y مماس اند اگر و تنها اگر خم و خط برحسب متغیرهای s و t مماس باشند.

لذا می توان محاسبات گروهی خم بیضوی را با استفاده از s و t به جای x و y انجام داد.

لم ۸.٤

خط $t=c$ که c یک عدد گویای ثابت است و $c\equiv 0 \pmod p$ خم $s=t^3+Ats^2+Bs^3$ را حداکثر در یک نقطه (s,t) که $s\equiv 0 \pmod p$ قطع می کند. این خم در چنین نقطه ای از اشتراک مماس نیست.

اثبات لم: حذف

اگر در معادله $at+b+ds$ داشته باشیم $d=0$ آنگاه معادله خط بصورت معادله خم در لم درمی آید یعنی

$$d=0 \Longrightarrow t=\frac{-b}{a} \text{(ثابت)}$$

اما ین خط از نقاط P_1' و P_2' عبور می کند پس $P_1'=P_2'$ و خط باید مماس بر خم باشد. مختصات را از $s-t$ به $x-y$ تغییر می دهیم در این صورت خواهیم داشت $P_1=P_2$.

از آنجا که $P_1=P_2$ بنابر قوانین گروهی معادله خط برحسب x و y در این نقطه بر خم مماس است. یعنی $at+b+ds=0$ در نقطه (s,t) مماس می شود و این بنابر لم امکان پذیر نیست پس به یک تناقض رسیدیم لذا $d\neq 0$.

حال با تقسیم بر d خواهیم داشت

$$at+b+ds=0 \xrightarrow{\text{تقسیم بر } d} \frac{a}{d}t+\frac{b}{d}+s=0 \Longrightarrow s=-\frac{a}{d}t-\frac{b}{d}$$

برای برخی $\alpha, \beta \in \mathbb{Q}$ که $\alpha = -\frac{a}{d}$ و $\beta = -\frac{b}{d}$

در این صورت P_1' و P_2' و P_3' روی خط $s = \alpha t + \beta$ قرار دارند.

لم ۸.۵

$$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + A s_2^2}{1 - A(s_1 + s_2)t_1 - B(s_2^2 + s_1 s_2 + s_1^2)}$$

اثبات: حذف

از آنجا که $s_1 \equiv s_2 \equiv 0 \pmod{p}$ داریم

$1 - A(s_1 + s_2)t_1 - B(s_2^2 + s_1 s_2 + s_1^2) \equiv 1 \pmod{p}$ و از آنجائیکه طبق لم ۸.۳،

$p^r \mid t_i$ پس $t_2^2 + t_1 t_2 + t_1^2 + A s_2^2 \equiv 0 \pmod{p^{2r}}$ در نتیجه $\alpha \equiv 0 \pmod{p^{2r}}$ و

چون $p^{3r} \mid s_1$ داریم $\beta = s_1 - \alpha t_1 \equiv 0 \pmod{p^{3r}}$ زیرا $p^{2r} \mid \alpha$ و $p^r \mid t_1$ پس $p^{3r} \mid \alpha t_1$ و

چون $p^{3r} \mid s_1$ پس همنهشتی بالا را داریم.

نقطه P_3' سومین نقطه از اشتراک خط $s = \alpha t + \beta$ با خم $s = t^3 + Ats^2 + Bs^3$ است بنابراین برای اثبات قسمت ۱ را برحسب t حل می کنیم داریم

$$\alpha t + \beta = t^3 + At(\alpha t + \beta)^2 + B(\alpha t + \beta)^3 \Longrightarrow 0$$
$$= t^3 + \frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + B\alpha^3 + A\alpha^2} t^2 + \cdots$$

حال مجموع سه نقطه برابر قرینه ضریب t^2 است یعنی

$$t_1 + t_2 + t_3 = -\frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + B\alpha^3 + A\alpha^2} t^2 \equiv 0 \pmod{p^{5r}}$$

همنهشتی اخیر برقرار است زیرا $t_1 \equiv t_2 \pmod{p^r}$ داریم ($t_3 \equiv 0 \pmod{p^r}$ چون $p^r \mid p^{5r} \mid t_1 + t_2 + t_3$)

بنابراین $s_3 = \alpha t^3 + \beta \equiv 0 \pmod{p^{3r}}$. بنابر لم ۸.۳ داریم $P_3 \in E_r$ بعلاوه

$$\lambda_r(P_1) + \lambda_r(P_2) + \lambda_r(P_3) \equiv 0 \equiv p^{-r}(t_1 + t_2 + t_3) \equiv 0 \ (mod\ p^{4r})$$

پس λ_r همریختی است و این اثبات را کامل می کند.

قضیه ۸.٦

فرض کنید شرایط قضیه ۸.۱ برقرار باشد اگر $n > 1$ و n توانی از p نباشد آنگاه E_1 دارای هیچ نقطه ای با مرتبه n نیست. (همچنین قضیه ۸.۹ را ببینید)

اثبات:

فرض کنیم $P \in E_1$ نقطه ای از مرتبه n باشد (فرض خلف) بنابر فرض n توانی از p نیست پس می توان n را بصورت زیر نوشت $n = p^r.t$ که $p \nmid t$ یا $gcd(p,t) = 1$ و $t > 1$. از این که مرتبه P برابر n نیست داریم $nP = \infty$ پس $n(p^r.t) = \infty$ در