بیستمین سمینار جبر،
۲ و ۳ اردیبهشت ۱۳۸۸، صفحه ۱–۳،
دانشگاه تربیت معلم

الگوریتمی بری به دست آوردن نقاط گویای خمهای بیضوی E/Q با رتبه یک

مهرداد خزلی *
دانشگاه کاشان
mehrdad.khazali@gmail.com
حسن دقیق
دانشگاه کاشان
hassan@kashanu.ac.ir

چکیده

در این مقاله با ارئه الگوریتمی، نقاط گویای خمهای بیضوی $E/\mathbb{Q}$ ر با رتبه یک به دست می‌آوریم. در این روش ابزار اصلی کار عبارت است از، ارتفاع متعارف خم بیضوی $E/\mathbb{Q}$، رتبه یک خم بیضوی $E/\mathbb{Q}$، $L^{'}(E,1)$ و حدس بیرچ و سوینرتون ـ دایر. کلیه محاسبات مورد نظردر این مقاله، به وسیله نرم افزار تخصصی نظریه اعداد با عنوان ari » [۱]، انجام شده‌است.

۱ معرفی

در این مقاله خم بیضوی $E/\mathbb{Q}$ ر با رتبه یک مفروض می‌گیریم. برای خم‌بیضوی مورد نظر، نمایش مینیمال وایراشتراس [۲] ر در نظر می‌گیریم. در نتیجه معادله آن به صورت زیر است:

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

در هر خم بیضوی با معادله بالا[۲]، می توان مقادیر b_2، b_4، b_6، b_8، c_4، c_6، Δ و j ر به دست آورد [۲]. گروه آبلی $(E(\ ),+)$، با توجه به قضیه مورنل ویل[۲]، داری تعداد

واژه های کلیدی: خمهای بیضوی، ارتفاع متعارف، رتبه خمهای بیضوی.
رده‌بندی موضوعی (MSC2000): 11Y50, 1G05.

متناهی مولد می‌باشد. بنابراین مجمو ه $E(\mathbb{Z})$ تعداد متناهی ضو خواهد داشت. از ضوهای $E(\mathbb{Z})$ برای به دست آورن مولدهای $E(\ )$ استفاده می‌کنیم. ون خم بیضوی مور نظر از رتبه یک می‌باشد، بنابراین قط یک مولد دار. در نتیجه کافی است از میان ضوهای $E(\mathbb{Z})$ مولد مور نظر را جستجو کنیم. بنابراین نمایشی که نقا ویای خم بیضوی دارند، از اهمیت زیادی برخوردار است. قضیه زیر نحوه نمایش این نقا ر ن ان می‌دهد.

قضیه ۱. فرض کنیم $E : y^۲ = x^۳ + ax^۲ + bx + c$ معادله خم بیضوی باشد. در این صورت هر نقطه گویای P این خم بیضوی دارای نمایش $\left(\frac{m}{e^۲}, \frac{n}{e}\right)$ P است. که در آن $a, b, c, e \in \mathbb{Z}$ و $(m, e) = (n, e)$ ۱.

برهان: ابتدا نقطه دلخواهی مانند $P \in E(\ )$ را انتخاب می‌کنیم. بنابراین برای P نمایشی مانند $\left(\frac{m}{M}, \frac{n}{N}\right) \in E(\ )$ را که در آن $(m, M) = (n, \ )$ ۱، در نظر می‌گیریم. بدون اینکه خللی به کلیت استدلال وارد شود، N, M را مثبت فرض می‌کنیم. حال با قرار دادن نقطه گویای P در معادله خم بیضوی داریم:

$$M^۳n^۲ = N^۲m^۳ + aN^۲Mm^۲ + bN^۲M^۲m + cN^۲M^۳. \qquad (۱)$$

چون $N^۲$ طرف راست معادله (۱) را می‌شمارد، بنابراین $N^۲ | M^۳n^۲$. با توجه به فرض $(n, \ ) \ ۱$ خواهیم داشت، $N^۲ | M^۳$. حال عکس این حکم را ثابت می‌کنیم. چون $M | M^۳n^۲$، بنابراین M طرف راست (۱) را می‌شمارد و در نتیجه $M | N^۲m^۳$. با توجه به فرض $(m, M) \ ۱$ خواهیم داشت، $M | N^۲$. از این و (۱) نتیجه می‌شود $M^۲ | N^۲m^۳$ و با توجه به فرض $(m, M) \ ۱$ خواهیم داشت، $M^۲ | N^۲$ بنابراین $M | N$. از این و با استفاده مجدد از (۱) نتیجه می‌شود، $M^۳ | N^۲m^۳$ و با توجه به فرض $(m, M) \ ۱$ خواهیم داشت، $M^۳ | N^۲$. حال با توجه به روابط موجود در بالا $M^۳ = N^۲$. اکنون قرار می‌دهیم $\frac{N}{M} =: \ ،$ در نتیجه داریم، $N = e^۳, M = \ ^۲$. بنابراین اثبات کامل می‌شود. □

۲ بیان الگوریتم

حال به نحو، مل این الگوریتم می ردازیم. ابتدا با استفاده از $L'(E, ۱)$ [۲]، صحت رتبه یک بودن خم بیضوی را مشخص ی‌کنیم، سپس H ر به $\left(\frac{L(E, ۱) T^۲}{۲\Omega c}\right)$ دست می‌آوریم. که در آن T, c, Ω مقادیری هستند که در دس بیر سوینرتون دایر [۲] آمده‌اند. اینک $\hat{h}(P)$ ارتفا تعار م بیضوی را در نظرمی‌گیریم[۲]. در نتیجه $P \in E(\ )$ ای وجود دار به ری $\hat{h}(P)$. اما از ی معادله زیر را داریم:

$$\hat{h}(P) = \hat{\lambda}_{\infty}(P) \quad Lo \ d) + \hat{\lambda}_{bad}(P).$$

در رابطه بالا $\hat{\lambda}_\infty(P)$ بیانگر ارتفاع رشمیدسی مو عی خم بیضوی و $\hat{\lambda}_{bad}(P) \in \lambda_{bad}$ فهرستی از تحویلهای بد خم بیضوی را مشخص می کند. خر قطه‌ای گویا مانند P است، که در قضیه (۱) به آن اشاره شده‌است. به علاوه $\hat{\lambda}_\infty$ تابعی از / به $\mathbb{R} \cup \infty$ می‌باشد که در آن یکه‌ای است که رابطه $E(\mathbb{C}) \cong \mathbb{C}/L$ [۲] را داریم. در نتیجه برای هر مخر ، و برای هر $\lambda \in \lambda_{bad}$، $\hat{\lambda}_\infty(z)$ را بر سب z به دست می‌آوریم. بنابراین به ازی هر $r \in \mathbb{R}$ ، $\hat{\lambda}_\infty^{-1}(r)$ خمی در $E(\mathbb{C}) \subset E(\mathbb{R})$ است. پس داریم، $E(\mathbb{C}) \cong \mathbb{C}/L$. ولی ون $E(\mathbb{R})$ خودش یک یا دو دایر، در $E(\mathbb{C})$ می‌شود، در نتیجه از اشتراک م $\hat{\lambda}_\infty^{-1}(r)$ با $E(\mathbb{R})$ فقط عداد متناهی نقطه به دست می آید. بنابراین اگر (x,y) متعلق به این اشتراک باشد، آنگاه به امتحان می‌توان به نتیجه رسید. بنابراین اگر $d^2x, d^3y \in \mathbb{Z}$، آنگاه با قرار دادن $d^3y = bx^2 + ax$، نقطه مورد نظر را به دست آورده‌ایم. این نقطه، نمایشی چون $P \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ دارد و چون تنها مولد می‌باشد، پس می‌توان بقیه نقا ویا را به وسیله آن به دست آورد. کلیه محاسبات این رو به وسیله نر ا زار تخصصی نظریه ا داد، با نام « $Pari$ » نجام داده‌است [ ]. ا نون مثال زیر را به نقطه گویای مولد آن به وسیله این رو به دست آمده است، می آوریم.

مثال . با استفاده از روش الا می‌توان نقطه گویای

$$P \left(\frac{۶۶۳۷۱۳۷۱۷ ۹}{۲۰۳۰۸۰۰۴}, \frac{۱۹۷۹۷۴۹۹۰۵۹۳۹۹۹۱۷}{۳۰۴۹۸۸۶۶۷۴۰۰۸}\right).$$

را برای خم بیضوی با معادله

$$y^2 + y = x^3 + ۱۶۴۲۱۰ - ۱۱۱۳۲۸۷$$

، به دست آورد.

روشهای دیگری نیز رای به دست آورن نقا ویای خمهای بیضوی وجود دارد که برای آگاهی بی رمی‌توان به [۳] مراجعه رد.

مرجع

[1] K. Belabas,H. cohen, *Pari*, V, 2.4.1.

[2] J.H.Silverman., ' The arithmetic of elliptic curver', *Graduate Text in Math., Vol.106, Springer-verlag*, 1986.

[3] J.H.Silverman., ' Computing rational points on rank 1 elliptic curves via L-series and canonical heights.', *Math.comp*, Vol. 68, pp. 835-858, 1999.