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

الگوریتمی برای 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 ارائه الگوریتمی، نقاط گویای خمهای بیضوی $E/\mathbb{Q}$ را 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 $E/\mathbb{Q}$، $L^{'}(E,۱)$ و حدس بیرچ و سوینرتون ـ دایر. کلیه محاسبات مورد نظردر این مقاله، به وسیله نرم افزار تخصصی نظریه اعداد با عنوان « $Pari$ » [۱]، انجام شده‌است.

۱ معرفی

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

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

در هر خم بیضوی با معادله بالا[۲]، می توان مقادیر $b_{۲}$، $b_{۴}$، $b_{۶}$، $b_{۸}$، $c_{۴}$، $c_{۶}$، Δ و j را به دست آورد [۲]. گروه آبلی $(E(\mathbb{Q}),+)$، با توجه به قضیه موردل ویل[۲]، دارای تعداد

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

متناهی مولد می‌باشد. بنابراین مجموعه $E(\mathbb{Z})$ تعداد متناهی عضو خواهد داشت. از عضوهای $E(\mathbb{Z})$ برای به دست آوردن مولدهای $E(\mathbb{Q})$ استفاده می‌کنیم. چون خم بیضوی مورد نظر از رتبه یک می‌باشد، بنابراین فقط یک مولد دارد. در نتیجه کافی است از میان عضوهای $E(\mathbb{Z})$ مولد مورد نظر را جستجو کنیم. بنابراین نمایشی که نقاط گویای خم بیضوی دارند، از اهمیت زیادی برخوردار است. قضیه زیر نحوه نمایش این نقاط را نشان 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 $P = \left(\frac{m}{e^۲}, \frac{n}{e^۳}\right)$ است. که در آن $a, b, c, e \in \mathbb{Z}$ و $(m, e) = (n, e) = ۱$.

برهان: ابتدا نقطه دلخواهی مانند $P \in E(\mathbb{Q})$ را انتخاب می‌کنیم. بنابراین برای P نمایشی مانند $\left(\frac{m}{M}, \frac{n}{N}\right) \in E(\mathbb{Q})$ را که در آن $(m, M) = (n, N) = ۱$، 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 $(n, N) = ۱$ 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 $e := \frac{N}{M}$، در نتیجه داریم، $e^۲ = M$, $e^۳ = N$. بنابراین اثبات کامل می‌شود. □

۲ بیان الگوریتم

حال به نحوه عمل این الگوریتم می‌پردازیم. ابتدا با استفاده از $L'(E, ۱)$ [۲]، صحت رتبه یک بودن خم بیضوی را مشخص می‌کنیم، سپس $H = \left(\frac{L'(E, ۱)T^۲}{۲\Omega c}\right)$ را به دست می‌آوریم. که در آن T, c, Ω مقادیری هستند که در حدس بیرچ وسوینرتون ـدایر [۲] آمده‌اند. اینک $\hat{h}(P)$ ارتفاع متعارف خم بیضوی را در نظرمی‌گیریم[۲]. در نتیجه $P \in E(\mathbb{Q})$ ای وجود دارد به طوری که $\hat{h}(P) = H$. اما از طرفی معادله زیر را داریم:

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

در رابطه بالا $\hat{\lambda}_\infty(P)$ بیانگر ارتفاع ارشمیدسی موضعی خم بیضوی و $\hat{\lambda}_{bad}(P) \in \lambda_{bad}$ فهرستی از تحویلهای بد خم بیضوی را مشخص می‌کند. d مخرج نقطه‌ای گویا مانند P است، که در قضیه (۱) به آن اشاره شده‌است. به علاوه $\hat{\lambda}_\infty$ تابعی از $\mathbb{C}/L$ به $\mathbb{R} \cup \infty$ می‌باشد که در آن L شبکه‌ای است که رابط ه $E(\mathbb{C}) \neq \mathbb{C}/L$ [۲] را داریم. در نتیجه برای هر مخرج d، و برای هر $\lambda \in \lambda_{bad}$، $\hat{\lambda}_\infty(z)$ را بر حسب z به دست می‌آوریم. بنابراین به ازای هر $r \in \mathbb{R}$، $\hat{\lambda}_\infty^{-1}(r)$ خمی در $\mathbb{C}/L$ است. پس داریم، $E(\mathbb{Q}) \subset E(\mathbb{R})$. ولی چون $E(\mathbb{R})$ خودش یک یا دو دایره در $E(\mathbb{C})$ می‌شود، در نتیجه از اشتراک خم $\hat{\lambda}_\infty^{-1}(r)$ با $E(\mathbb{R})$ فقط تعداد متناهی نقطه به دست می‌آید. 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 $d^2x = a$ و $d^3y = b$، 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 نقاط گویا را به وسیله آن به دست آورد. کلیه محاسبات این روش به وسیله نرم‌افزار تخصصی نظریه اعداد، با نام « $Pari$ » انجام شده‌است [۱]. اکنون مثال زیر را که نقطه گویای مولد آن به وسیله این روش به دست آمده است، می‌آوریم.

مثال ۱. با استفاده از روش بالا می‌توان نقطه گویای

$$P = \left(\frac{۶۶۳۷۱۳۷۱۷۲۹}{۲۱۰۳۰۸۰۰۴}, \frac{۱۹۷۹۷۴۹۹۰۵۹۳۹۹۹۱۷}{۳۰۴۹۸۸۶۶۷۴۰۰۸}\right).$$

را برای خم بیضوی با معادله

$$y^2 + y = x^3 + ۱۶۴۲۱۱x - ۴۱۱۱۳۲۸۷$$

، به دست آورد.

روشهای دیگری نیز برای به دست آوردن نقاط گویای خمهای بیضوی وجود دارد که برای آگاهی بیشترمی‌توان به [۳] مراجعه کرد.

مراجع

[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.