あるタイプの超楕円曲線の虚2次整数点の強有限性について

小松 亨

1 導入

本研究集会における講演では, 論文 [3] に掲載されている内容の概要を紹介した. 論文 [3] の詳細は

https://bulletin.math.uoc.gr/issues.html

にて available online for free のため, そちらで確認いただくとして, 本稿では 2 つの不変量 $B(x)$ と α に関して論文 [3] では触れていない考察を紹介する.

本研究集会の初回は, 2006 年 8 月, 九州大学箱崎キャンパスにて著者 (当時, 九州大学 21 世紀 COE 学術研究員) が世話人をつとめ開催しました. そののち, 金子昌信先生, 権寧魯先生, 岸康弘先生などのご尽力のおかげにより継続され, 今回の第 15 回を迎えることができました. この場を借りて心より感謝申し上げます. そして, 第 15 回福岡数論研究集会において講演の機会をいただき, 世話人の金子昌信先生 (九州大学), 権寧魯先生 (九州大学), 岸康弘先生 (愛知教育大学), 高妻倫太郎先生 (立命館アジア太平洋大学), 松坂俊輝先生 (九州大学) に重ねて感謝申し上げます.

2 2つの不変量

定義. 正の整数 k に対し

$$\mathcal{F}_{2k} := \{f(x) \in \mathbb{Z}[x] \mid f(x) \text{ はモニック}, \deg f = 2k, f(x) \notin \mathbb{C}[x]^2\}.$$

1 つめの不変量 $B(x)$ は次の補題による.

補題 (Szalay [5])**.** $f(x) \in \mathcal{F}_{2k}$ のとき, ある $B(x), C(x) \in \mathbb{Q}[x]$ $(\deg B = k > \deg C)$ が存在し $f(x) = B(x)^2 + C(x)$ をみたす.

多項式 $f(x) = x^{2k} + a_{2k-1}x^{2k-1} + \cdots + a_1x + a_0 \in \mathcal{F}_{2k}$ に対し, 上記の $B(x)$ と $C(x)$ を求める方法を考える. 例えば具体的に $B(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1x + b_0$ とおき, 等式 $f(x) = B(x)^2 + C(x)$ における k 次から $(2k-1)$ 次までの項の係数比較により, k 本の連立式をつくり, k コの未知数 $b_0, b_1, \ldots, b_{k-1}$ について解く方法がまず考えられる. もちろん, その方法で可能であるが, 下記の補題 A のような方法もある.

定義. 正の整数 m に対し $\mathbb{C}[x]$ の部分集合 $\mathbb{C}[x]_{\leq m}$ と写像 ι_m, ρ_m を次で定義する:

$$\begin{aligned}
&\mathbb{C}[x]_{\leq m} := \{g(x) \in \mathbb{C}[x] \mid \deg g \leq m\},\\
&\iota_m : \mathbb{C}[x]_{\leq m} \to \mathbb{C}[x]_{\leq m},\ g(x) \mapsto g(1/x)x^m,\\
&\rho_m : \mathbb{C}[x] \to \mathbb{C}[x]_{\leq m},\ h(x) \mapsto r(x),\ \text{ただし } h(x) - r(x) \in x^{m+1}\mathbb{C}[x].
\end{aligned}$$

注意. 写像 ι_m は対合, つまり $\iota_m \circ \iota_m = \mathrm{id}$. 写像 ρ_m はいわゆる $\bmod x^{m+1}$ 写像.

補題 A. $f(x) \in \mathcal{F}_{2k}$ に対し, $\widehat{f}(x) = \iota_{2k}(f(x))$, $\overline{\widehat{f}}(x) = \rho_k(\widehat{f}(x))$ とおき,

$$\widehat{B}(x) = 1 + \sum_{j=1}^{k} \binom{1/2}{j} \rho_k(\rho_{k+1-j}(\overline{\widehat{f}}(x) - 1)^j)$$

とおくとき, $B(x) = \iota_k(\widehat{B}(x))$ と $C(x) = f(x) - B(x)^2$ は $B(x), C(x) \in \mathbb{Q}[x]$, $\deg B = k > \deg C$, $f(x) = B(x)^2 + C(x)$ をみたす. ただし $\binom{1/2}{j}$ は一般二項係数とする.

証明. z に関する形式的ベキ級数として

$$1 + z = \Big(1 + \sum_{j=1}^{\infty} \binom{1/2}{j} z^j\Big)^2.$$

□

例. $f(x) = x^6 + 2x^5 + 3x^4 + 4x^3 + 5x^2 + 6x + 7$ のとき, $k = 3$ で

$$\begin{aligned}
\widehat{f}(x) &= 1 + 2x + 3x^2 + 4x^3 + 5x^4 + 6x^5 + 7x^6,\\
\overline{\widehat{f}}(x) &= 1 + 2x + 3x^2 + 4x^3
\end{aligned}$$

であり,

$$\begin{aligned}
\widehat{B}(x) &= 1 + \sum_{j=1}^{3} \binom{1/2}{j} \rho_3(\rho_{4-j}(2x + 3x^2 + 4x^3)^j)\\
&= 1 + \frac{1/2}{1!}\rho_3(2x + 3x^2 + 4x^3) + \frac{(1/2)(-1/2)}{2!}\rho_3((2x + 3x^2)^2)\\
&\quad + \frac{(1/2)(-1/2)(-3/2)}{3!}\rho_3((2x)^3)\\
&= 1 + \frac{1}{2}(2x + 3x^2 + 4x^3) - \frac{1}{8}(4x^2 + 12x^3) + \frac{1}{16}(8x^3)\\
&= 1 + x + x^2 + x^3
\end{aligned}$$

であるので,

$$\begin{aligned}
B(x) &= \iota_3(\widehat{B}(x)) = x^3 + x^2 + x + 1,\\
C(x) &= f(x) - B(x)^2 = 2x^2 + 4x + 6.
\end{aligned}$$

例. $f(x) = x^8 + x^7 + x^2 + 3x - 5$ のとき, $k = 4$ で

$$\begin{aligned}
\widehat{f}(x) &= 1 + x + x^6 + 3x^7 - 5x^8,\\
\overline{\widehat{f}}(x) &= 1 + x
\end{aligned}$$

であり,

$$\begin{aligned}\widehat{B}(x) &= 1+\sum_{j=1}^{4}\binom{1/2}{j}\rho_4(\rho_{5-j}(x)^j)\\ &= 1+\frac{1/2}{1!}\rho_4(x)+\frac{(1/2)(-1/2)}{2!}\rho_4(x^2)+\frac{(1/2)(-1/2)(-3/2)}{3!}\rho_4(x^3)\\ &\quad+\frac{(1/2)(-1/2)(-3/2)(-5/2)}{4!}\rho_4(x^4)\\ &= 1+\frac{1}{2}x-\frac{1}{8}x^2+\frac{1}{16}x^3-\frac{5}{128}x^4\end{aligned}$$

であるので,

$$\begin{aligned}B(x) &= \iota_4(\widehat{B}(x)) = x^4+\frac{1}{2}x^3-\frac{1}{8}x^2+\frac{1}{16}x-\frac{5}{128},\\ C(x) &= f(x)-B(x)^2 = \frac{7}{128}x^3+\frac{505}{512}x^2+\frac{3077}{1024}x-\frac{81945}{16384}.\end{aligned}$$

2 つめの不変量 α の定義は

$$\alpha := \min\{\alpha\in\mathbb{N}\,|\,\alpha B(x)\in\mathbb{Z}[x]\}$$

である. 具体的に $B(x)=x^k+b_{k-1}x^{k-1}+\cdots+b_1x+b_0$ とおき, 係数比較により求める手法で考えると, 連立式で $+2b_i$ の項が現れ, b_i について解くので b_i の分母は高々2 ベキであることが観察できて, 解くごとに分母の 2 ベキが高々1 つずつ増えそうに思える. しかし, その予測ならば直前の例において α が 2^4 の約数になりそうだが, 実際は $\alpha=128=2^7$ である. この疑問を明確に解消するために, 上記の補題 A を利用することで, 下記の補題 B がえられる.

補題. 正の整数 j に対し

$$\mathrm{ord}_2\left(\binom{1/2}{j}\right)\geq -(2j-1)$$

であり, 等号成立は j が 2 ベキ ($2^0=1$ を含む) のときのみ. ただし $\mathrm{ord}_2(a)$ は有理数 a の加法的 2 進付値とする.

証明. $\mathrm{ord}_2(j!)\leq j-1$ であり, 等号成立は j が 2 ベキ ($2^0=1$ を含む) のときのみ. □

補題 B. α は 2^{2k-1} の約数. 特に, k が 2 ベキ ($2^0=1$ を含む) ならば $\alpha=2^{2k-1}$ の場合が存在し, k が 2 ベキ ($2^0=1$ を含む) でないならば α は 2^{2k-2} の約数.

参考文献

[1] P. Borwein and T. Erdélyi, Polynomials and polynomial inequalities, Grad. Texts in Math., 161, Springer-Verlag, New York, 1995.

[2] C. U. Jensen, A. Ledet and N. Yui, Generic polynomials. Constructive aspects of the inverse Galois problem, Math. Sci. Res. Inst. Publ., 45, Cambridge University Press, Cambridge, 2002.

[3] T. Komatsu, Imaginary quadratic integral points on a hyperelliptic curve of certain type, Bull. Hell. Math. Soc. **67** (2023), 59–72.

[4] D. Poulakis, A simple method for solving the Diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$, Elem. Math. **54** (1999), no. 1, 32–36.

[5] L. Szalay, Fast algorithm for solving superelliptic equations of certain types, Acta Acad. Paedagog. Agriensis Sect. Math. (N.S.) **27** (2000), 19–24.

[6] L. Szalay, Superelliptic equations of the form $y^p = x^{kp} + a_{kp-1}x^{kp-1} + \cdots + a_0$, Bull. Greek Math. Soc. **46** (2002), 23–33.

[7] N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations, Acta Arith. **75** (1996), no. 2, 165–190.