

1 実験整数論について

山本芳彦 (阪大理)

「実験整数論」といっても素数分布についてとか、Goldbachの問題、不定方程式の整数解の個数を求めることなど沢山の分野があると思うが、ここではいわゆる「佐藤の予想」(有理数体上で定義された楕円曲線のHasseゼータ関数の零点の偏角の分布に関する予想)及びその超楕円曲線への拡張について報告する。

C を有理数体上で定義された超楕円曲線、その定義方程式を

$$y^2 = f(x) = a_0 x^N + a_1 x^{N-1} + \dots + a_N$$

とし、 $a_0 \neq 0, a_1, \dots, a_N$ は有理整数、 $f(x)$ の判別式 $\Delta \neq 0$ とする。このとき C の種数 g は $g = [(N-1)/2]$ ($[]$ は Gauss の記号で $[]$ の中の数を越えない最大の整数を表わす。) である。

いま p を 2Δ を割り切らない素数とし、 C を mod p で reduction してできる超楕円曲線 (それは標数 p の素体上で定義される) を \tilde{C}_p とする。

\tilde{C}_p の合同ゼータ関数 $Z(u)$ は

$$Z(u) = \frac{P(u)}{(1-u)(1-pu)}$$

という形をしている。ここで $P(u)$ は定数項 = 1 となる $2g$ 次の u の多項式である。

$$P(u) = 1 + c_1 u + \dots + c_{2g} u^{2g}$$

とおくとき、 c_1, \dots, c_{2g} は次の式により求められる。

$$c_k = \sum_{j=0}^k \epsilon^j d_{k-j}$$

$$\epsilon = \begin{cases} 0 & N = \text{奇数のとき} \\ \left(\frac{a_0}{p}\right) & N = \text{偶数のとき} \end{cases}$$

$$d_n = \sum_{u_1, \dots, u_n=0}^{p-1} \left(\frac{f(u_1, \dots, u_n)}{p} \right)$$

$$f(u_1, \dots, u_n) = R(x^n + u_1 x^{n-1} + \dots + u_n, f(x))$$

$$= \left[\begin{array}{cccc} 1 & u_1 & \dots & u_n \\ 1 & u_1 & \dots & u_n \\ \dots & \dots & \dots & \dots \\ a_0 & a_1 & \dots & a_N \\ a_0 & a_1 & \dots & a_N \\ \dots & \dots & \dots & \dots \end{array} \right] \begin{array}{l} N \\ \\ \\ n \end{array} \quad (N+n \text{ 次の行列式})$$

($R(g, f)$ は g と f の終結式)

また $P(u) = (1 - \alpha_1 u) \cdots (1 - \alpha_{2g} u)$

と分解するとき (α_i は複素数)

$$|\alpha_i| = \sqrt{p} \quad i=1, 2, \dots, 2g$$

となることも知られている。

特に $g=1$ のとき ($i, e, N=3, 4$ のとき) C は楕円曲線と呼ばれて

$N=3$ のとき

$$c_1 = \sum_{u=0}^{p-1} \left(-\frac{f(u)}{p} \right), \quad c_2 = p$$

$N=4$ のとき

$$c_1 = \left(\frac{a_0}{p} \right) + \sum_{u=0}^{p-1} \left(\frac{f(u)}{p} \right), \quad c_2 = p$$

となる。

$$P(u) = 1 + c_1 u + pu^2 = (1 - \alpha_1 u)(1 - \alpha_2 u)$$

$$|\alpha_1| = |\alpha_2| = \sqrt{p}$$

より $\alpha_1 = \sqrt{p} e^{i\theta}, \quad \alpha_2 = \sqrt{p} e^{-i\theta} \quad 0 \leq \theta \leq \pi$

とおくと $\theta = \theta_p$ は 2Δ を割り切らない素数 p に対する \tilde{C}_p の合同ゼータ函数の零点の偏角を表わしている。

$y^2 = f(x)$ を一つ固定して、数多く素数 p について $\theta = \theta_p$ を求めてその分布を調べたとき、次の二つの場合があることがわかった。(佐藤-難波)

(a) 実験したすべての素数 p の約 50% に対して $\theta_p = \pi/2$ で、残りの 50% の p に対しては θ_p は $0 \leq \theta \leq \pi$ の間に一様に分布する。

(b) θ_p は $0 \leq \theta \leq \pi$ の間に $\sin^2 \theta$ に比例して分布する。

またこの二通りしかないらしいこともわかった。ところで、(a) の場合にあってはまる曲線はすべて“虚数乗法をもつ楕円曲線”であって、このときには (a) のような分布をすることが証明されている。(E. Hecke)

問題なのは虚数乗法をもたない楕円曲線であるが、多くの実験から“有理数体上で定義された虚数乗法をもたない楕円曲線に対しては θ_p の分布は $\sin^2 \theta$ に比例する。”(佐藤の予想)。この予想に対して、(J. Tate の研究があるが)未だ解決されていない。

この予想を $g > 1$ の場合にまで拡張するために、まず $g=2$ ($N=5, 6$) のときに実験を行なった。すなわち

$N=5$ のとき

$$c_1 = \sum_{u=0}^{p-1} \left(\frac{f(u)}{p} \right), \quad c_3 = c_1 p$$

$$c_2 = \sum_{u_1, u_2=0}^{p-1} \left(\frac{f(u_1, u_2)}{p} \right), \quad c_4 = p^2$$

$N=6$ のとき

$$c_1 = \left(\frac{a_0}{p} \right) + \sum_{u=0}^{p-1} \left(\frac{f(u)}{p} \right),$$

$$c_2 = 1 + \left(\frac{a_0}{p} \right) \sum_{u=0}^{p-1} \left(\frac{f(u)}{p} \right) + \sum_{u_1, u_2=0}^{p-1} \left(\frac{f(u_1, u_2)}{p} \right)$$

$$c_3 = c_1 p, \quad c_4 = p^2$$

により, $c_1 \sim c_4$ を求め,

$$\begin{aligned} P(u) &= 1 + c_1 u + c_2 u^2 + c_1 p u^3 + p^2 u^2 \\ &= (1 - \alpha_1 u)(1 - \bar{\alpha}_1 u)(1 - \alpha_2 u)(1 - \bar{\alpha}_2 u) \end{aligned}$$

$$\alpha_1 = \sqrt{p} e^{i\theta_1}, \quad \alpha_2 = \sqrt{p} e^{i\theta_2}$$

$$0 \leq \theta_1 \leq \pi, \quad 0 \leq \theta_2 \leq \pi$$

において, (θ_1, θ_2) の二次元分布を調べた. 今までのところ, 大体 4 種の分布があって, その分布の型は, その曲線から作られるヤコビ多様体の自己準同型環の型と 1 対 1 に対応するらしいことがわかった.

とにかく, 全く単純な計算の繰り返しにもかかわらず, その計算量が極度に多い (例えば $p=1000$ のとき, (θ_1, θ_2) 一つだけを求めるためには, 7 次又は 8 次の行列式に相当する $f(u_1, u_2)$ を約 100 万个計算する必要がある) ため, 分布がわかる程充分なデータが得られないというのが現状である.

< 文 献 >

- [1] E. Hecke, Werke 14 "Eine neue Art von Zetafunktionen....."
- [2] 志村, 谷山, 近代的整数論 共立現代数学講座
- [3] J. Tate, Algebraic cohomology classes, A.M.S. Summer Institute 1964
- [4] A. Weil, Sur les Courbes Algebriques....., Hermann, Paris.

本 PDF ファイルは 1966 年発行の「第 7 回プログラミング・シンポジウム報告集」をスキャンし、項目ごとに整理して、情報処理学会電子図書館「情報学広場」に掲載するものです。

この出版物は情報処理学会への著作権譲渡がなされていませんが、情報処理学会公式 Web サイトに、下記「過去のプログラミング・シンポジウム報告集の利用許諾について」を掲載し、権利者の検索をおこないました。そのうえで同意をいただいたもの、お申し出のなかったものを掲載しています。

https://www.ipsj.or.jp/topics/Past_reports.html

過去のプログラミング・シンポジウム報告集の利用許諾について

情報処理学会発行の出版物著作権は平成 12 年から情報処理学会著作権規程に従い、学会に帰属することになっています。

プログラミング・シンポジウムの報告集は、情報処理学会と設立の事情が異なるため、この改訂がシンポジウム内部で徹底しておらず、情報処理学会の他の出版物が情報学広場 (=情報処理学会電子図書館) で公開されているにも拘らず、古い報告集には公開されていないものが少からずありました。

プログラミング・シンポジウムは昭和 59 年に情報処理学会の一部門になりましたが、それ以前の報告集も含め、この度学会の他の出版物と同様の扱いにしたいと考えます。過去のすべての報告集の論文について、著作権者 (論文を執筆された故人の相続人) を探し出して利用許諾に関する同意を頂くことは困難ですので、一定期間の権利者搜索の努力をしたうえで、著作権者が見つからない場合も論文を情報学広場に掲載させていただきたいと思えます。その後、著作権者が発見され、情報学広場への掲載の継続に同意が得られなかった場合には、当該論文については、掲載を停止致します。

この措置にご意見のある方は、プログラミング・シンポジウムの辻尚史運営委員長 (tsuji@math.s.chiba-u.ac.jp) までお申し出ください。

加えて、著作権者について情報をお持ちの方は事務局まで情報をお寄せくださいますようお願い申し上げます。

期間：2020 年 12 月 18 日 ~ 2021 年 3 月 19 日

掲載日：2020 年 12 月 18 日

プログラミング・シンポジウム委員会

情報処理学会著作権規程

<https://www.ipsj.or.jp/copyright/ronbun/copyright.html>