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”（有理数体上定義された楕円曲線のHasseゼータ函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を有理数体上定義された超楕円曲線，その定義方程式を

$$y^2=f(x)=a_0x^N+a_1x^{N-1}+\cdots\cdots+a_N$$

とし，$a_0\neq 0$, $a_1,\cdots\cdots a_N$ 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の素体の上で定義される）を$\tilde{C}_p$とする。

$\tilde{C}_p$ の合同ゼータ函数$Z(u)$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。

$$P(u)=1+c_1u+\cdots\cdots+c_{2g}u^{2g}$$

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

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

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

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

$$f(u_1,\cdots,u_n)=R(x^n+u_1x^{n-1}+\cdots\cdots u_n,f(x))$$

$$=\begin{vmatrix}1 & u_1 & \cdots\cdots & u_n & & \\ & 1 & u_1 & \cdots\cdots & u_n & \\ & & \cdots\cdots & & & \\ a_0 & a_1 & \cdots\cdots & a_N & & \\ & a_0 & a_1 & \cdots\cdots & a_N & \\ & & \cdots\cdots & & & \end{vmatrix}\begin{matrix}\}N\\ \\ \\ \}n\end{matrix}$$

（$N+n$次の行列式）

（$R(g, f)$はgとfの終結式）

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

と分解するとき（α_i は複素数）

$$|\alpha_i|=\sqrt{p} \qquad i=1, 2, \cdots\cdots, 2g$$

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

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つた．（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 $0\leqq\theta\leqq\pi$ の間に一様に分布する．

(b) θ_p は $0\leqq\theta\leqq\pi$ 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つた．ところで，(a)の場合にあ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

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

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

$N = 6$ のとき

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

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

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

により，$c_1 \sim c_4$ を求め，

$$P(u) = 1 + c_1 u + c_2 u^2 + c_1 p\, u^3 + p^2 u^2$$

$$= (1 - \alpha_1 u)(1 - \overline{\alpha_1}\, u)(1 - \alpha_2 u)(1 - \overline{\alpha_2} u)$$

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

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

とおいて，(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つた．

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 $p \fallingdotseq 1000$ のとき，(θ_1, θ_2) 一つだけを求めるためには，7次又は8次の行例式に相当する $f(u_1, u_2)$ を約100万個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.