超楕円曲線とチェビシェフ多項式

難波完爾（Kanji Namba）

所属（なし）

463-3 Kitamizote Sojya Okayama 719-1117

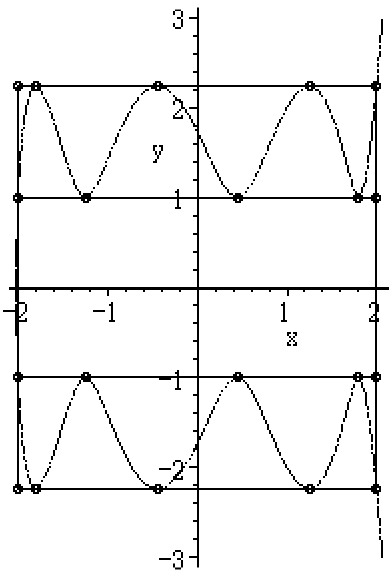
tel/fax. 0866-90-1886

2014.03.02

key words:
hyper-elliptic curve, finite field, Tschebysheff polynomial, congruence ζ-function, resultant transform, angular distribution, $\sin^2$-conjecture, coefficient polynomial, Poincaré-Mordell group, Jacobian Manifold, cyclic orthogonal system

この講演では Tschebysheff の shift、例えば、7 次の Tschebysheff 多項式 $x^7-7x^5+14x^3-7x$ の定数 3 だけの shift できまる超楕円曲線などについて論ずる。

$$C: \quad y^2 = x^7-7x^5+14x^3-7x+3$$



については、その終結変換多項式（= resultant transform polynomial, congruence ζ-function）の根は常に絶対値 $\sqrt{p}$ の複素数です。また、$p \neq \pm 1 \mod 7$ の素数に対する係数多項式は 3 次 Tschebysheff-shift、つまり、x^3-3x+k と予想されています。Tschebysheff 多項式は $y = 2\cos(nt)$ を $x = 2\cos(t)$ で表現した多項式、言い換えると余弦の n 倍角公式を多項式として表現したものです。

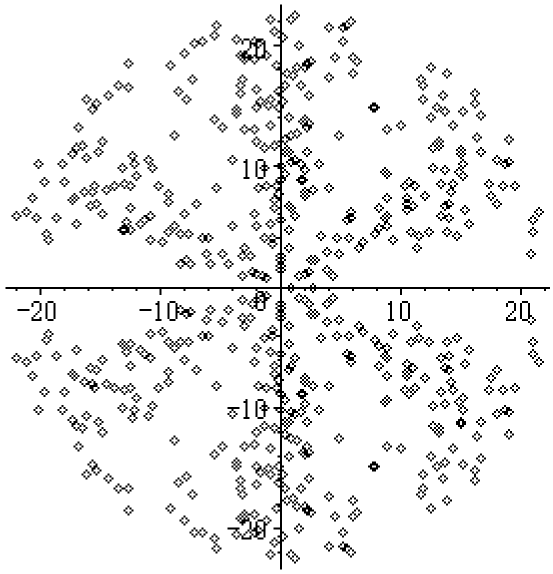
種数（genus）g の超楕円曲線の標準係数多項式は志村・谷山理論によると

$$\eta f(x) = 2\cos(gt) + 2a_1\cos((g-1)t) + \cdots + 2a_{g-1}\cos(t) + a_g, \quad x = 2\cos(t)$$

という[-2,2]に g 個の実根をもつ余弦展開多項式です。以下の図は合同ゼータ根：

$$C: \quad y^2 = x^7-7x^5+14x^3-7x+3$$

$$p = 2 \sim 521,\ gal = 7{:}6,\ det = 5^3 \cdot 7^7$$



のようです。偏角の分布に関する、(楕円曲線の場合の)Sato-Tate sin square 予想の拡張版(= extended $\sin^2$-conjecture)の主張は、一般のガロア群が非可解な(有理係数)多項式 f(x)については、種数 g(= genus)の超楕円曲線

$$y^2 = f(x),\ g = [(\deg(f(x))-1)/2]$$

の偏角の分布は

$$\sin^2(\theta)+\sin^2(2\theta)+\cdots+\sin^2(g\theta)$$

に比例するという予想です。

勿論、g = 1 の場合、虚数乗法(complex multiplication)をもたない場合は 2006 年の R. Taylor によって証明されています。また、上記の曲線の場合は可解な場合で、分布は単独の $\sin^2(3\theta)$に近いものになると思います。「思います」と言葉をにごしたのには訳がありまして状況はなかなか複雑そうなのです。

特に 2n+1 を繰り返した素数、例えば

1, 3, 7, (15), 31, (63), 127, …; 2, 5, 11, 23, 47, (95), 191, 383,…

などは興味があります。つまり、素数 11, 23, 47 に関する

$$y^2 = x^{11}-11x^9+44x^7-77x^5+55x^3-11x+5$$

$$y^2 = x^{23}-23x^{21}+230x^{19}-1311x^{17}+4692x^{15}-10948x^{13}+16744x^{11}-16445x^9+9867x^7-3289x^5+506x^3-23x+11$$

など終結変換多項式が、例えば、23 の場合ですと、$p \neq \pm 1 \bmod 23$ に対しては 11 次 Tschebysheff-shift

$$x^{11}-11x^9+44x^7-77x^5+55x^3-11x+k$$

になることが、p = 3, 5, 7, 11 に対して確かめられています。勿論、重要なのは Tschebysheff-shift から、次数は異なりますが、Tschebysheff-shift が得られることです。(preservation of Tschebysheff-shift)。例えば、p = 13, 17 などのデータが得られればと思っています。計算量は p^{11} に比例します。