数理解析研究所講究録
第 844 巻 1993 年 108-112

Rank $\geq$ 17 の楕円曲線の例

長尾　孝一
滋賀職業訓練短期大学校

1. 結果

最近、Mestre[1,2,3] によって rank の高い楕円曲線が作られた。まず、Mestre の結果を次の３つの propositions にまとめておく。

Proposition 1 ([1])
$\mathcal{E}$ を有理関数体 $Q(T)$ 上定義され、定義式が
$Y^2 = (429T^2 + 55260)X^4 - (5434T^2 + 1239000)X^3$
$+ (-3432T^4 - 2451T^2 + 1222156)X^2 + (21736T^4 - 3637984T^2 + 134780352)X$
$+ 6864T^6 - 1074992T^4 + 53200096T^2 - 758849264.$
で表される楕円曲線とする。このとき $\mathcal{E}$ の $Q(T)$-$rank$ は≥ 11 である。

Proposition 2 ([2])
$\mathcal{E}$ を $T = (3T'^2 - 478T' + 1287)/(T'^2 - 429)$ で特殊化して得られる $Q(T')$ ($Q(T')$ はやはり有理関数体) 上定義された楕円曲線を $\mathcal{E}'$ とおく。このとき $\mathcal{E}'$の　$Q(T')$-$rank$は $\geq$ 12 である。

Proposition 3 ([3])
Cを $\mathcal{E}'$ を $T' = 77$ で特殊化して得られる Q 上定義された楕円曲線とする。このとき Cの Q-$rank$ は≥ 15 である。

N を正整数とする。Q 上定義された楕円曲線 Eにたいして、
$S = S(N) = \sum(2 + a_p)\log p/(p + 1 - a_p)$
$S' = S'(N) = \sum -a_p \log p$
とおく。ここで、$a_p = p + 1 - \#E(F_p)$ であり又 p は $p \leq N$を満たす素数を動くものとする。我々は Sおよび S' の値の大きな楕円曲線の rank が高いことを経験的に知っている。
有理数 t に対して, $\mathcal{E}$ を $T = t$ で特殊化して得られる Q 上定義された楕円曲線を E_tとおく。我々は楕円曲線の族 $\{E_{t_1/t_2} \mid (t_1, t_2)$ は素、$1 \leq t_1 \leq 1000$, $1 \leq t_2 \leq 100\}$ を考える。この曲線の族から $S_{401} > 39$, $S_{1009} > 54$, 及び, $S'_{1009} > 17000$, を満たすものを選ぶことにより　我々は曲線 $E_{967/59}$, $E_{866/35}$, $E_{542/49}$, 及び $E_{537/71}$を得る。

Theorem
(1)$E_{537/71}$ の　Q-$rank$は$\geq$ 17 である。
(2)$E_{866/35}$ の　Q-$rank$は$\geq$ 17 である。
(3)$E_{542/49}$ の　Q-$rank$は$\geq$ 16 である。
(4)$E_{967/59}$ の　Q-$rank$は$\geq$ 14 である。

2.Sと S'

Mestre は [4] において、$S = S_N(E)$ の大きな楕円曲線は経験的に rank が大きいことを利

用し、Sの大きな楕円曲線を集めることによってrankの高い楕円曲線を構成した。Sはその各項 $(2+a_p)\log p/(p+1-a_p)$ の値が p が十分大きくなると、0 に近ずく為、p が大きな素数をとるときの$\#E(F_p)$ の値を　そのrank に十分反映しているとはいえない。ここでは、以下 Sの改良であるところの S'について述べる。
楕円曲線 Eに対して
$L_E(s)=\prod_{p|cond}(1-a_p p^{-s})^{-1}*\prod_{p\not| cond}(1-a_p p^{-s}+p^{1-2s})^{-1}$
をそのL関数という。

ここで、$a_p=\begin{cases} p+1-\#E(F_p) & if\ good\ reduction \\ 0 & if\ additive\ reduction \\ 1 & if\ split\ multiplicative\ reduction \\ -1 & if\ nonsplit\ multiplicative\ reduction \end{cases}$ である。以下簡単のため、有限項$\prod_{p|cond}$の部分を除いた
$\prod_{p\not| cond}(1-a_p p^{-s}+p^{1-2s})^{-1}$ を Eの L 関数ということにする。
L_Eは複素平面全体に mermorphic　function として解析接続でき (Hasse conjecture)、$s=1$ での L_Eの零点の位数が Eの rank である (Birch Swinerton-Dyer conjecture) と予想されている。$\alpha_p, \overline{\alpha_p}$ を

$$(1-a_p p^{-s}+p^{1-2s})=(1-\alpha_p p^{-s})(1-\overline{\alpha_p}p^{-s})$$

で表される複素数とする。

また $B(p,m)=\alpha_p^m+\overline{\alpha_p}^m$ とする。形式的に
$L'/L=\sum_{p;prime}\sum_{m\geq 1}-B(p,m)\ \log(p)p^{-ms}$ と書けている。(右辺は　$\Re(s)>3/2$　で収束)
Birch Swinerton-Dyer 予想より Eの rank は $res_{s=1}L'/L(s)$ となる。
Proposition (tauber type theorem)
$f(s)$ を $\sum a_n n^{-s}$ と書かれる　$\Re(s)>1$ で収束する Dirichlet 級数とする。$A_N=(\sum_{n\leq N}a_n)/N$ が　ある値 κ に収束するとき $res_{s=1}f(s)=\kappa$ が成り立つ。

$f(s)=L'/L(s)$　の場合を考える。$\Re(s)>1$ での収束や　A_N の収束は期待できないが、A_N の値が rank に近いものと予想できる。
実際　$A_N=(\sum_{p;prime\ m\geq 1\ p^m\leq N}-B(p,m)\log(p))/N$
であり　その $m=1$ の部分和 $(\sum_{p;prime\ p\leq n}-a_p\log(p))/N\ =\ S'_N/N$ の大きい楕円曲線を選ぶことによって我々は rank の高い楕円曲線を構成した。

3. 有理数の独立性について
次の proposition によって、$Y^2=aX^4+bX^3+cX^2+dX+e$ の形をした楕円曲線を Weiestrass form に直すことができる。
Proposition
E を完全体 k上定義され定義式が $Y^2=aX^4+bX^3+cX^2+dX+e$ で与えられた楕円曲線とする。
また、E'を定義式が $T^2=S^3+cS^2+(bd-4ae)S+(ad^2+b^2e-4ace)$ で与えられた楕円曲線とする。

E,E' は変数変換
$S=(2*e^2+dX-2\sqrt{e}Y)/X^2$ 、$T=(2*(S^2-4ea)X-2dS-4eb)/4e$ で表される写像
ψ: $E\rightarrow E'$ によって $k(\sqrt{e})$-同型である。
又　Eが k-有理点 P_0をもつとき Eから E'への写像$\phi(P)=\psi(P)-\psi(P_0)$ は k上定義され
　Eと E'はψによって k-同型となる。

一般のワークステイション上で動く PDS 数式処理ソフトＰＡＲＩによって Weiestrass Form で表されている　楕円曲線の minimal weiestrass model を求めることができる。
また　その有理点 Pに対して canonical height の値 $h(P)$ を任意精度で求めることができる。実際、$E_{537/71}$ は conductor が
$2*3*5*11*13^2*31*71*32059793*$
　　　69880275538796967770686936178147450273527
である次の minimal Weiestrass curve $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$
$a_1=1$
$a_2=0$
$a_3=0$
$a_4=-1895782483362476188247825431$
$a_6=42810746555185028468846212199762991367145$
と Q-同型で　その上の有理点
$p_1=[9529946590244278/81, 877339317930179132982349/729]$
$p_2=[20121870453749702/169, 2695230693436703340441017/2197]$
$p_3=[832895565844694, -24005332929074426761579]$
$p_4=[170323128927446, -2158931233727022802795]$
$p_5=[2705247588331766/49, -111897080628880491318877/343]$
$p_6=[42800399533958, -200188548806606122939]$
$p_7=[911893195333944758/22801, -605810297183101189471167469/3442951]$
$p_8=[826902562282742/49, -42873975604122721153117/343]$
$p_9=[1381131197535594758/32041, 1163925394071743348949284359/5735339]$
$p_{10}=[232185357760483651238/4923961,$
　　$2637393845318100394599410665999/10926269459]$
$p_{11}=[75026691547561127/1444, 15957698316628635168731107/54872]$
$p_{12}=[55048888392278, 324451948662567802901]$
$p_{13}=[56063905437398, 335773236821174910101]$
$p_{14}=[222469439971613318/3721, 85887675571396806667576841/226981]$
$p_{15}=[892018268333445638/961, 841577165574425466532140971/29791]$
$p_{16}=[1087869867462051014/29929, -766682063863902139838061287/5177717]$
$p_{17}=[1403950398237398, 52580177817811779812501]$
に対して canonical height pairing の作る行列 $(<p_i,p_j>_{1\leq i,j\leq 17})$ の行列式は,
14813374499818820.0325557329.... であると計算できる。
この行列式が零でないことより、$p_i(1\leq i\leq 17)$ は独立な有理点であることがわかる。

又、$E_{866/35}$ は conductor が
$2^7 * 3 * 5 * 7 * 11 * 13 * 17 * 19 * 831851*$
$27688479672552128715606462640385238803481282 1.$

である次の minimal Weiestrass curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

$a_1 = 0$
$a_2 = 1$
$a_3 = 0$
$a_4 = -1847801808769001339569289 1145$
$a_6 = 96678875493491972147105766840567965108 4743$

と Q-同型で　その上の有理点

$p_1 = [987132393978079331954/12581209,$
$441558648018404526517905318 75/44625548323]$
$p_2 = [6360438106451911/81, 832408927123396980500/729]$
$p_3 = [13270945713669554/169, 2555271033060881176965/2197]$
$p_4 = [857729078027047559/10609, 3991209955474267172096 1420/1092727]$
$p_5 = [79430124839906, 1461592070515094017 5]$
$p_6 = [4607314783851323, -31259704732574980231 8252]$
$p_7 = [2573692194283109/4, -127862522511653550016935/8]$
$p_8 = [17056161852252119/49, -2078193005890922295589500/343]$
$p_9 = [430102770233098117 1/52441,$
$- 656366039306811393976716300/12008989]$
$p_{10} = [81650469905306, -489610612651515258 75]$
$p_{11} = [145150467371853905 09/187489,$
$132377408344303548431717 2500/81182737]$
$p_{12} = [951024572107238604431/12243001,$
$528074563286919141440933947500/42838260499]$
$p_{13} = [632503187469855989 81/811801,$
$640263372457559119079730 1500/731432701]$
$p_{14} = [383087327491229/4, -2199020909677353716955/8]$
$p_{15} = [17385255389295817 91/22201, 931090303390915874023818 0/3307949]$
$p_{16} = [443811832334711, -8954505736358951228460]$
$p_{17} = [402560517401125490 9/27889,$
$- 532465381284360201942028 0500/4657463]$

に対して canonical height pairing の作る行列 $(< p_i, p_j >_{1 \leq i,j \leq 17})$ の行列式は,
4806705005919007.180831854947.... である。この行列式が零でないことより、$p_i (1 \leq i \leq 17)$ は独立な有理点であることがわかる。

Referrences

[1] J-F Mestre ,Courbes elliptiques de rang ≥ 11 sur $Q(T)$,

C.R.acad.Sci, Paris,313 ser 1,1991,139pp-142pp.
[2] J-F Mestre ,Courbes elliptiques de rang ≥ 12 sur $Q(T)$,
C.R.acad.Sci, Paris,313 ser 1,1991,171pp-174pp.
[3] J-F Mestre ,Un exemple de courbes elliptiques sur Q de rang ≥ 15,
C.R.acad.Sci, Paris,314 ser 1,1992,453pp-455pp.
[4] J-F Mestre ,Construction d' une courbes elliptiques de rang ≥ 12,
C.R.acad.Sci, Paris,295 ser 1,1982,643pp-644pp.
[5] Koh-ichi Nagao , Examples of elliptic curves over Q with rank ≥ 17 ,
Proc. Japan Aacd. 68 ser. A 199 287pp-289pp

KOH-ICHI NAGAO
SHIGA POLYTECNIC COLLEGE
1414 HURUKAWA CHO OH-MIHACHIMAN SHI 523 JAPAN