70. *Examples of Elliptic Curves over Q with Rank ≥ 17*

By Koh-ichi NAGAO*)

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1992)

Abstract: We construct some elliptic curves over Q with *rank* ≥ 17.

Recently, Mestre [1,2,3] constructed large rank elliptic curves. We summarize his results in the following three propositions.

Proposition 1 ([1]). *Let $\mathfrak{E}$ be the curve over rational function field $Q(T)$ of the form*

$$Y^2 = (429T^2 + 55260)X^4 - (5434T^2 + 1239000)X^3 + (-3432T^4 - 2451T^2 + 1222156)X^2 + (21736T^4 - 3637984T^2 + 134780352)X + 6864T^6 - 1074992T^4 + 53200096T^2 - 758849264.$$

Then $Q(T)$-rank of $\mathfrak{E}$ is ≥ 11.

Proposition 2 ([2]). *Let $\mathfrak{E}'$ be the curve over $Q(T')$ ($Q(T')$ also means rational function field) which is obtained by specializing $\mathfrak{E}$ to $T = (3T'^2 - 478T' + 1287)/(T'^2 - 429)$. Then $Q(T')$-rank of $\mathfrak{E}'$ is ≥ 12.*

Proposition 3 ([3]). *Let C be the curve defined over Q which is obtained by specializing $\mathfrak{E}'$ to $T' = 77$. Then Q-rank of C is ≥ 15.*

Let N be a fixed positive integer. For an elliptic curve E defined over Q, we define ([4])

$$S = S(N) = \sum (2 + a_p)\log p/(p + 1 - a_p)$$
$$S' = S'(N) = \sum - a_p \log p$$

where $a_p = p + 1 - \# E(F_p)$ and p moves over prime numbers satisfying $p \leq N$. We experimentally know that elliptic curves whose S and S' are sufficiently large have large ranks ([4]).

For a rational number t, let E_t be an elliptic curve defined over Q which is obtained by specializing $\mathfrak{E}$ to $T = t$. We consider the family of elliptic curves $\{E_{t_1/t_2}\}$ where (t_1, t_2) moves over coprime integers satisfying $1 \leq t_1 \leq 1000$ and $1 \leq t_2 \leq 100$. By selecting the curves in this family satisfying $S_{401} > 39$, $S_{1009} > 54$, and, $S'_{1009} > 17000$, we obtain four curves $E_{967/59}$, $E_{866/35}$, $E_{542/49}$, and, $E_{537/71}$.

Theorem. (1) *Q-rank of $E_{537/71}$ is ≥ 17.*
(2) *Q-rank of $E_{866/35}$ is ≥ 17.*

Proof of (1). $E_{537/71}$ is Q-isomorphic to the following minimal Weiestrass curve of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where

$a_1 = 1$
$a_2 = 0$
$a_3 = 0$
$a_4 = -189578248336247618824782543 1$

*) Shiga Polytecnic college, 1414 Hurukawa cho, Oh-mihachiman shi 523, Japan.

$a_6 = 42810746555185028468846212199762991367145$

and the following p_i $(1 \leq i \leq 17)$ are independent points of this curve.

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]

There is calculation system **PARI** which is useful for number theory calculation and which runs on ordinary work stations. By using PARI, we have that the conductor of this curve is

$2*3*5*11*13^2*31*71*32059793*$
$69880275538796967770686936178147450273527$

and that the determinant of matrix $(\langle p_i, p_j \rangle_{1 \leq i,j \leq 17})$, where $\langle\, , \rangle$ means canonical height pairing, is 14813374499818820.0325557329... . Since, above determinant is non zero, we have that $p_i (1 \leq i \leq 17)$ are independent points of this curve.

(2) Similarly, $E_{866/35}$ is Q-isomorphic to the minimal Weiestrass curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where

$a_1 = 0$

$a_2 = 1$

$a_3 = 0$

$a_4 = - 18478018087690013395692891145$

$a_6 = 966788754934919721471057668405679651084743$

and the following $p_1, p_2, \ldots, p_{17}$ are independent points of this curve.

p_1 = [987132393978079331954/12581209,
44155864801840452651790531875/44625548323]

$p_2 =$ [6360438106451911/81, 8324089271233969805OO/729]
$p_3 =$ [13270945713669554/169, 2555271033060881176965/2197]
$p_4 =$ [857729078027047559/10609,
399120995547426717209614 20/1092727]
$p_5 =$ [79430124839906, 1461592070515O940175]
$p_6 =$ [46O7314783851323, − 312597047325749802318252]
$p_7 =$ [2573692194283109/4, − 1278625225116535500169 35/8]
$p_8 =$ [17056161852252119/49, − 207819300589092229558950O/343]
$p_9 =$ [4301027702330981171/52441,
− 6563660393068113939767163OO/12008989]
$p_{10} =$ [81650469905306, − 4896106126515152587 5]
$p_{11} =$ [145150467371853905O9/187489,
13237740834430354843171725OO/81182737]
$p_{12} =$ [95102457210723860443 1/12243001,
5280745632869191414409339475OO/42838260499]
$p_{13} =$ [632503187469855989 81/811801,
64026337245755911907973015OO/731432701]
$p_{14} =$ [383087327491229/4, − 219902090967735371 6955/8]
$p_{15} =$ [1738525538929581791/22201,
931090303390915874O238180/3307949]
$p_{16} =$ [443811832334711, − 895450573635895122846O]
$p_{17} =$ [40256051740112549O9/27889,
− 5324653812843602019420280500/4657463]

We have that the determinant of matrix associated to height pairing is 4806705005919007.180831854947... and that the conductor of this curve is $2^7 * 3 * 5 * 7 * 11 * 13 * 17 * 19 * 831851 * 276884796725521287156064626403852388034812821$.

Remark. We see in the same way that the *Q-rank* of $E_{542/49}$, $E_{967/59}$ are $\geq 16, 14$ respectively.

References

[1] J.-F. Mestre: Courbes elliptiques de rang ≥ 11 sur $Q(T)$. C. R. Acad. Sci. Paris, ser. 1, **313**, 139–142 (1991).
[2] ——: Courbes elliptiques de rang ≥ 12 sur $Q(T)$. ibid., ser. 1, **313**, 171–174 (1991).
[3] ——: Un exemple de courbes elliptiques sur Q de rang ≥ 15. ibid., ser. 1, **314**, 453–455 (1992).
[4] ——: Construction d'une courbes elliptiques de rang ≥ 12. ibid., ser. 1, **295**, 643–644 (1982).