66. An Example of Elliptic Curve over Q with Rank ≥ 20

By Koh-ichi NAGAO

Shiga Polytechnic College*)

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1993)

Abstract: We construct an elliptic curve over Q with rank ≥ 20.

Mestre [1] (resp. [2]) constructed elliptic curves over $Q(T)$ with $Q(T)$-rank ≥ 11 (resp. with $Q(T)$-rank ≥ 12). In the families of elliptic curves over Q, which are obtained by specialization of above curves, Mestre [3] found an elliptic curve over Q with Q-rank ≥ 15. In choosing appropriate elliptic curves in these families, author [4] (resp. Tunnel (cf. [5]), resp. Fermiger [5]) found two elliptic curves with Q-rank ≥ 17 (resp. one curve with Q-rank ≥ 18, resp. two curves with Q-rank ≥ 19). In this paper, we show by the same method but using a computational device mentioned later that there is an elliptic curve over Q with Q-rank ≥ 20.

§1. Mestre's construction of elliptic curve over $Q(T)$ with $Q(T)$-rank $\geq$ 11. Let $\alpha_i \in Z$ $(i = 1,2,3,4,5,6)$, and put $q(X) = \Pi_{i=1}^{6} (X - \alpha_i)$, $p(X) = q(X - T) * q(X + T) \in Q(T)[X]$. Then there are $g(x)$, $r(X) \in Q(T)[X]$ with $\deg g = 6$, $\deg r \leq 5$ such that $p = g^2 - r$. Then the curve $Y^2 = r(X)$ contains 12 $Q(T)$-rational points $P_1, \ldots, P_{12}$ where

$$P_i = (T + \alpha_i, g(T + \alpha_i)),\ P_{i+6} = (-T + \alpha_i, g(-T + \alpha_i)),\ _{1 \leq i \leq 6}.$$

Let c_5 be the coefficient of X^5 of $r(X)$.

In case $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) = (-17, -16, 10, 11, 14, 17)$, we have $c_5 = 0$ and on the elliptic curve $Y^2 = r(X)$, $P_1, \ldots, P_{11}$ are independent $Q(T)$-rational points. (Group structure is given with P_{12} at origin.)

For any 6-ple of $A = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) \in Z^6$ with $c_5 = 0$, we obtain as above an elliptic curve $\varepsilon_A : Y^2 = r(X)$ over $Q(T)$. For $t \in Q$, we denote with $E_t = E_{A,t}$ the elliptic curve over Q obtained from ε_A by specialization $T \to t$.

§2. Construction of our curve. For an elliptic curve E over Q, and a prime number p, we put $a_p = a_p(E) = p + 1 - \# E(F_p)$. For a fixed integer N, we put furthermore $S(N) = S(N, E) = \sum(-a_p + 2)/(p + 1 - a_p)$ and $S'(N) = S'(N, E) = (\sum - a_p * log(p))/N$ where p runs over good primes satisfying $p \leq N$. It is experimentally known (cf. [6]) that high rank curves are found among curves with large $S(N)$, $S'(N)$.

Now let $A = (95,71,66,58,13,0)$. Then we have $c_5 = 0$. We search in the family of curves

$$\{E_{t_1/t_2} (= E_{A,t_1/t_2}) \mid 1 \leq t_1 \leq 3000,\ 1 \leq t_2 \leq 300,\ t_1\, t_2 \textit{ are co-prime}\},$$

curves satisfying

$S(401) \geq 31.5$, $S'(401) \geq 11$, $S(1987) \geq 61$, $S'(1987) \geq 16$,

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

$S(3001) \geq 71$, $S'(3001) \geq 16$, $S(4003) \geq 75$, $S'(4003) \geq 16$, $S(5297) \geq 80$, $S'(5297) \geq 17$, $S(6581) \geq 84$, and $S'(6581) \geq 17$, and find $E_{349/48}$ and $E_{619/195}$, for the latter of which we could show that the Q-rank ≥ 20. Thus we have

Theorem. *The Q-rank of $E_{619/195}$ is ≥ 20.*

In fact $E_{619/195}$ is Q-isomorphic to the minimal Weiestrass model

$$y^2 + xy = x^3 - 431092980766333677958362095891166x + 5156283555366643659035652799871176909391533088196$$

whose conductor is

$$2*3*5*7*13*17*19*29*53*1759*539449*1884347 *78324820513*38888278938650095324808499814402930189 1.$$

On this curve the following $P_1, \ldots, P_{20}$ are independent points.

$P_1 = [11176771052208428265 24/37249,$
$\quad 3153047947718548901150587231643 4/7189057]$

$P_2 = [38095017214360176, 663463890748267533423286 2]$

$P_3 = [128263157005359747/4,$
$\quad 3943883738880797593764991 5/8]$

$P_4 = [1735413707212417277 64/4489,$
$\quad 204581311349257832170977498540 6/300763]$

$P_5 = [114037038978699019879860444/2903808769,$
$\quad 1093029826650184196976652135696199191086/156477543135103]$

$P_6 = [10257968319668962556557698 0/3236130769,$
$\quad 8894059315207553492547830918835552613 98/184093771056103]$

$P_7 = [5205906656889497350 68/11881,$
$\quad 108653651654847592740058182154 50/1295029]$

$P_8 = [201537570874848579/4, 84414630327852273660698571/8]$

$P_9 = [8566017671075667672/169,$
$\quad 2340866321116566203164824767 4/2197]$

$P_{10} = [848108116495076 76, 240546959795967044447053 62]$

$P_{11} = [-21830796739843140, 2040388505636168283880914]$

$P_{12} = [-2234086367006310516/121,$
$\quad 3476314228926730107073128678/1331]$

$P_{13} = [-398890292913112314601476/47513449,$
$\quad 93691572538281697461686196213358943 4/327510203957]$

$P_{14} = [-388503783119847409 00/5041,$
$\quad 10136471367585467909913817882 54/357911]$

$P_{15} = [410916153652874282067804/58874929,$
$\quad 7124833440519895938250643194029123 54/451747330217]$

$P_{16} = [303086976097371000762351 6/266375041,$
$\quad 5708794986061809828924957672204713682/4347507044161]$

$P_{17} = [56681238039560590 68/361,$
$\quad 103076389847314019042818890 30/6859]$

$P_{18} = [-580936108517972743204832 4/267289801,$
$\quad 901827975235853363156896624255334773 8/4369920956549]$

$P_{19} = [-256381598399113962133604/10169721,$

1315536690951996543879087852628778/32431240269]

$P_{20} =$ [479228870284501996956/167281,

135888316201098799476616096547298/68417929].

By using calculation system PARI, we have that the determinant of the matrix $(\langle P_i, P_j \rangle)_{1 \leq i,j \leq 20}$ associated to canonical height is 2975173777358668583558.164104. Since this determinant is non-zero, we see that $P_1, \ldots, P_{20}$ are independent points.

3. Computational device. Let $A = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) \in Z^6$ be a 6-ple with $c_5 = 0$. This having been found, we should search for $t \in Q$ such that $S(N) = S(N, E_{A,t})$, and $S'(N) = S'(N, E_{A,t})$ have large values. For this purpose, we have to calculate $\# E_{A,t}(F_p)$. Now, notice that $\# E_{A,t}(F_p) = \# E_{A,s}(F_p)$ for $t, s \in Q$, $s \equiv t \pmod{p}$. Then, to caluculate $\# E_{A,t}(F_p)$, we have only to calculate it for $t = 0, 1, \ldots, p-1$ and save the values in the computer. With this device, we could considerably accelerate our computation.

4. Examples of the other high rank curves. The Q-ranks of the three elliptic curves $E_{A,t}$ with the following three values of A, t have been shown to be at least 19.

1. $A = (34, 31, 28, 27, 1, 0)$, $t = 7582/623$
2. $A = (34, 31, 28, 27, 1, 0)$, $t = 6441/59$
3. $A = (50, 42, 37, 29, 4, 0)$, $t = 8429/52$.

References

[1] J.-F. Mestre: Courbes elliptiques de rang≥ 11 sur $Q(T)$. C. R. Acad. Sci, Paris, **313**, ser. 1, 139–142 (1991).

[2] ——: Courbes elliptiques de rang ≥ 12 sur $Q(T)$. ibid., **313**, ser. 1, 171–174 (1991).

[3] ——: Un exemple de courbes elliptiques sur Q de rang ≥ 15. ibid., **314**, ser. 1, 453–455 (1992).

[4] K. Nagao: Examples of elliptic curves over Q with rank ≥ 17. Proc. Japan Acad., **68** A, 287–289 (1992).

[5] S. Fermiger: Un exemple de courbe elliptique definie sur Q de rang ≥ 19. C. R. Acad Sci, Paris, **315**, ser. 1, 719–722 (1992).

[6] J.-F. Mestre: Construction de courbes elliptiques sur Q de rang ≥ 12. ibid., **295**, ser. 1, 643–644 (1982).