22. On the Rank of the Elliptic Curve $y^2 = x^3 + k$

By Shoichi KIHARA*)

Department of Mathematics, Hyogo University of Teacher Education (Communicated by Shokichi IYANAGA, M. J. A., March 12, 1987)

Let F be a finitely generated field over a prime field and $k \in F$. The F-points of the elliptic curve

$$E(k): y^2 = x^3 + k$$

form a finitely generated abelian group with respect to the well-known addition on E(k). The rank of this group will be also called the rank of the curve E(k) and denoted by r(k). In this note, we consider the case F = Q(p, q) where p, q are variables and give an example of the elliptic curve E(k) with $r(k) \ge 5$.

Let us first consider the case with the field F in general, and suppose $a, b, c, d \in F$. In our previous note [3], we showed that E(k) with

(1)
$$k = (a^6 + b^6 + c^6 - 2a^3b^3 - 2b^3c^3 - 2c^3a^3)/4$$

has 5 F-points $P_i = (x_i, y_i)$ $(i=1, \dots, 5)$

provided that

$$a^3 + d^3 = 2(b^3 + c^3).$$

In [3], we utilized the parametric solution

$$egin{aligned} a = 72t^4 \ b = 36t^3 - 1 \ c = 1 \ d = -72t^4 + 6t \end{aligned}$$

of (3) to show that there are infinitely many values of $t \in \mathbb{Z}$, for which E(k) has at least 20 coprime \mathbb{Z} -points.

Observe now that (3) has the following parametric solution

$$\begin{array}{c} a\!=\!-2p\!-\!2q\!+\!8(p^2\!-\!pq\!+\!q^2)^2\\ b\!=\!-1\!+\!4(p\!-\!2q)(p^2\!-\!pq\!+\!q^2)\\ c\!=\!1\!-\!4(p\!+\!q)(p^2\!-\!pq\!+\!q^2)\\ d\!=\!2p\!-\!4q\!-\!8(p^2\!-\!pq\!+\!q^2)^2 \end{array}$$

(cf. Hardy and Wright [2] p. 199). This solution gives (4) as a specialization p=t, q=-t.

^{*} Current address: 2186-1 Shimobun, Kinsei-cho, Kawanoe-shi, Ehime-ken, 799-01 Japan.

Return now to F = Q(p, q). Substituting (5) to (2), we obtain 5 F-points $P_i(x_i, y_i)$ ($i=1, \dots, 5$) on E(k) where k=k(p, q). Specializing p, q to 1, -1, we have 5 Q-points $P'_i(x'_i, y'_i)$ on E(k) with k=k(1, -1)=27286371721. This E(k) has no torsion (cf. Cassels [1] Theorem V).

The author owes the following idea to the kind communication of Dr. J.-F. Mestre to show the independency of $P'_i(x'_i, y'_i)$, $i=1, \dots, 5$, on this E(k), k=27286371721.

If $P_i(x_i', y_i')$, $i=1, \dots, 5$, were dependent, then there should be $m_i \in \mathbb{Z}$, $i=1, \dots, 5$, $(m_1, \dots, m_5) \neq (0, \dots, 0)$ such that

$$\sum_{i=1}^{5} m_i P'_i(x'_i, y'_i) = 0,$$

which should imply

(6)
$$\sum_{i=1}^{5} n_i P'_i(x'_i, y'_i) = 2P(x, y)$$

where $n_i=0, 1, (n_1, \dots, n_5)\neq (0, \dots, 0), x, y\in Q$. There are 31 possibilities for (n_1, \dots, n_5) , that is, $(0,0,0,0,1), \dots, (1,1,1,1,1)$. Corresponding sums on the left hand side of (6) will be denoted by $P(s_1, t_1), \dots, P(s_3, t_3)$. (The

Table

$\begin{array}{c ccccccccccccccccccccccccccccccccccc$							
2	j	$(n_1$	n_2	n_3	n_4	$n_5)$	s_j
3 (0 0 0 1 1) 11939977/4356 4 (0 0 1 0 0) 35 5 (0 0 1 0 1) 10699472 6 (0 0 1 1 0) 432644/25 7 (0 0 1 1 0 10 2624 8 (0 1 0 0 0 72 9 (0 1 0 1 0 2562 11 (0 1 0 1 0 2562 11 (0 1 0 0 79726934 1 13 (0 1 1 0 0 79726934 1 13 (0 1 1 1 0 1 823948/361 15 (0 1 1 1 0 7937164610/2948089 1 16 (1 0 0 0 0 2520 17 (1 0	1	(0	0	0	0	1)	-66
4 (0 0 1 0 0) 35 5 (0 0 1 0 1) 10699472 6 (0 0 1 1 0) 432644/25 7 (0 0 1 1 0 10 0 0 8 (0 1 0 0 1) -28565/4761 10 (0 1 0 1 0 2562 11 (0 1 0 1 0 95316900/5329 12 (0 1 1 0 0 79726934 13 (0 1 1 0 0 79726934 13 (0 1 1 0 0 -1079097439/37210000 14 (0 1 1 1 0 -823948/361 15 (0 1 1 1 7937164610/2948089 16 (1 0 0 0 2520 17 (1 0 0 1 1 <td>2</td> <td>(0</td> <td>0</td> <td>0</td> <td>1</td> <td>0)</td> <td>-2310</td>	2	(0	0	0	1	0)	-2310
5 (0 0 1 0 1) 10699472 6 (0 0 1 1 0) 432644/25 7 (0 0 1 1 1) -510896329/214369 8 (0 1 0 0 1 -28565/4761 10 (0 1 0 1 0 2562 11 (0 1 0 1 1 95316900/5329 12 (0 1 1 0 79726934 -1079097439/37210000 14 (0 1 1 0 -823948/361 -1079097439/37210000 14 (0 1 1 0 -823948/361 -1079097439/37210000 14 (0 1 1 1 7937164610/2948089 -6520 16 (1 0 0 0 2520 17 (1 0 0 1 15697248613788/4214809 18 (1	3	(0	0	0	1	1)	11939977/4356
6	4	(0	0	1	0	0)	35
7 (0 0 1 1 1) -510896329/214369 8 (0 1 0 0 0) 72 9 (0 1 0 0 1) -28565/4761 10 (0 1 0 1 0) 2562 11 (0 1 0 1 1) 95316900/5329 12 (0 1 1 0 0) 79726934 13 (0 1 1 0 1) -1079097439/37210000 14 (0 1 1 1 0 1 -1079097439/37210000 14 (0 1 1 1 0 1 -1079097439/37210000 14 (0 1 1 0 1 -823948/361 15 (0 1 1 1 7937164610/2948089 16 (1 0 0 0 0 17 (1 0 0 1 0 18 (1 0 0 1 <td>5</td> <td>(0</td> <td>0</td> <td>1</td> <td>0</td> <td>1)</td> <td>10699472</td>	5	(0	0	1	0	1)	10699472
8 (0 1 0 0 0 72 9 (0 1 0 0 1) -28565/4761 10 (0 1 0 1 0) 2562 11 (0 1 0 1 1) 95316900/5329 12 (0 1 1 0 0) 79726934 13 (0 1 1 0 1) -1079097439/37210000 14 (0 1 1 1 0) -823948/361 15 (0 1 1 1 0 -823948/361 15 (0 1 1 1 7937164610/2948089 16 (1 0 0 0 2520 17 (1 0 0 0 1 18 (1 0 0 1 500815/4761 19 (1 0 0 1 15697248613788/4214809 20 (1 0 1 0 1 21 (1	6	(0	0	1	1	0)	432644/25
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	7	(0	0	1	1	1)	-510896329/214369
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	8	(0	1	0	0	0)	72
11 (0 1 0 1 1) 95316900/5329 12 (0 1 1 0 0) 79726934 13 (0 1 1 0 1) -1079097439/37210000 14 (0 1 1 1 0) -823948/361 15 (0 1 1 1 7937164610/2948089 16 (1 0 0 0 0 17 (1 0 0 0 1 18 (1 0 0 1 0 19 (1 0 0 1 15697248613788/4214809 20 (1 0 1 0 0 500126/25 21 (1 0 1 0 19463029784/8128201 22 (1 0 1 1 19463029784/8128201 23 (1 0 1 1 30997065966482/150326022961 24 (1 1 0 0 1 1846807/5184 25 (1	9	(0	1	0	0	1)	-28565/4761
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	10	(0	1	0	1	· 0)	2562
13 (0 1 1 0 1) -1079097439/37210000 14 (0 1 1 1 0) -823948/361 15 (0 1 1 1 7937164610/2948089 16 (1 0 0 0 0 17 (1 0 0 0 1 18 (1 0 0 1 0 19 (1 0 0 1 15697248613788/4214809 20 (1 0 1 0 500126/25 21 (1 0 1 0 500126/25 21 (1 0 1 0 19463029784/8128201 22 (1 0 1 1 30997065966482/150326022961 24 (1 1 0 0 0 -11846807/5184 25 (1 1 0 1 16224276635070/839782441 26 (1 1	11	(0	1	0	1	1)	95316900/5329
14 (0 1 1 1 0) -823948/361 15 (0 1 1 1 7937164610/2948089 16 (1 0 0 0 0 2520 17 (1 0 0 0 1 -404792178/185761 18 (1 0 0 1 0 500815/4761 19 (1 0 0 1 15697248613788/4214809 20 (1 0 1 0 0 500126/25 21 (1 0 1 0 19463029784/8128201 22 (1 0 1 1 0 -65205175/465124 23 (1 0 1 1 30997065966482/150326022961 24 (1 1 0 0 0 -11846807/5184 25 (1 1 0 1 0 99077034 27 (1 1 0 1 1 -1413382713911/14249196900 28 (1 1 1 0 </td <td>12</td> <td>(0</td> <td>1</td> <td>1</td> <td>0</td> <td>0)</td> <td>79726934</td>	12	(0	1	1	0	0)	79726934
15 (0 1 1 1) 7937164610/2948089 16 (1 0 0 0 0 2520 17 (1 0 0 1) -404792178/185761 18 (1 0 0 1 500815/4761 19 (1 0 0 1 15697248613788/4214809 20 (1 0 1 0 500126/25 21 (1 0 1 19463029784/8128201 22 (1 0 1 19463029784/8128201 23 (1 0 1 1 30997065966482/150326022961 24 (1 1 0 0 -11846807/5184 25 (1 1 0 1 16224276635070/839782441 26 (1 1 0 1 -1413382713911/14249196900 28 (1 1 1 0 4278112427/1666681 29 (1 1 1	13	(0	1	1	0	1)	-1079097439/37210000
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	14	(0	1	1	1	0)	-823948/361
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	15	(0	1	1	1	1)	7937164610/2948089
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	16	(1	0	0	0	0)	2520
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	17	(1	0	0		1)	-404792178/185761
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	18	(1	0	0	1	0)	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	19	(1	0	0	1	1)	15697248613788/4214809
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	20	(1	0	1	0	0)	500126/25
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	21	(1	0		0	1)	19463029784/8128201
24 (1 1 0 0 0) -11846807/5184 25 (1 1 0 0 1) 16224276635070/839782441 26 (1 1 0 1 0) 99077034 27 (1 1 0 1 1) -1413382713911/14249196900 28 (1 1 1 0 0) 4278112427/1666681 29 (1 1 1 0 1) -1281072003164320/580176226249	22	(1	0		1	0)	-65205175/465124
25	23	(1				1)	30997065966482/150326022961
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	24	(1	1	-	-		-11846807/5184
27 (1 1 0 1 1) —1413382713911/14249196900 28 (1 1 1 0 0) 4278112427/1666681 29 (1 1 1 0 1) —1281072003164320/580176226249	25	(1		0		1)	·
28 (1 1 1 0 0) 4278112427/1666681 29 (1 1 1 0 1) -1281072003164320/580176226249	26	(1	1	0	1	0)	99077034
29 (1 1 1 0 1) —1281072003164320/580176226249	27		1	0	1	1)	-1413382713911/14249196900
	28		1	1	0	0)	4278112427/1666681
30 (1 1 1 1 0) 482128052/7070281	29	(1	1	1	0	1)	-1281072003164320/580176226249
	30	(1					· ·
31 (1 1 1 1 1) 10879673506835735/1794962689	31	(1	1	1	1	1)	10879673506835735/1794962689

values of s_1, \dots, s_{31} are given in the Table.) Then the relation (6) should again imply that

$$x^4-4s_1x^3-8kx-4ks_1=0, j=1,\dots,31,$$

has a rational solution, because of the duplication formula. The author verified that this is not the case by using the computer algebra system mu-Math on NEC "PC9801" computer. This implies

Theorem. The rank of the elliptic curve E(k) with k=k(p, q), where k(p, q) is the polynomial of degree 24 in p, q obtained by substituting (5) in (1), is at least five.

As our curve E(k) used in [3] was nothing but a specialization E(k(t, -t)) of E(k(p, q)), we obtain the following corollary in virtue of Theorem 20.3 in [4].

Corollary. There are infinitely many E(k) with $k \in \mathbb{Z}$ with $r(k) \geq 5$ and with at least 20 coprime integral points.

Acknowledgements. The author wishes to express his hearty thanks to Professors S. Iyanaga M. J. A., J. P. Serre, H. Yanagihara, Dr. J.-F. Mestre and Dr. S. Nakano for their help and suggestion.

References

- [1] J. W. S. Cassels: The rational solutions of the diophantine equation $Y^2=X^3-D$. Acta Math., **82**, 243-273 (1950).
- [2] G. H. Hardy and E. M. Wright: An introduction to the theory of numbers. The Clarendon Press, Oxford (1979).
- [3] S. Kihara: On coprime integral solutions of $y^2=x^3+k$. Proc. Japan Acad., 63A, 13-16 (1987).
- [4] J. H. Silverman: The arithmetic of elliptic curves. Graduate Texts in Math., vol. 106, Springer-Verlag, New York (1986).