Math. J. Okayama Univ. **47** (2005), 81–84

ON GROUP STRUCTURES OF SOME SPECIAL ELLIPTIC CURVES

Takehiro KUDO and Kaoru MOTOSE

The purpose of this paper is to determine the structures of groups of rational points on elliptic curves of form $y^2 = x^3 - px$ where p is a Fermat or Mersenne prime.

Let E be an elliptic curve $y^2 = x^3 - px$ where p is a prime and let Γ be the set of rational points in E. Then Γ has an abelian group structure. Mordell-Weil theorem states that Γ is finitely generated. Thus we can set $\Gamma = \mathcal{F} \oplus \mathcal{T}$ where $\mathcal{F}$ and $\mathcal{T}$ are the free part and the torsion part of Γ, respectively.

Let β be a natural group homomorphism from $\mathbb{Q}^\times$ to $\overline{\mathbb{Q}^\times} = \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ and let α be the group homomorphism from Γ to $\overline{\mathbb{Q}^\times}$ defined by

$$\alpha(P) = \begin{cases} 1 & \text{for } P = O \\ \beta(-p) & \text{for } P = \mathbf{0} \\ \beta(x) & \text{for } x \neq 0 \end{cases}$$

where $P = (x, y) \in \Gamma$, $\mathbf{0} = (0, 0)$ is the origin and O is the point at infinity.

We consider an elliptic curve $\bar{E} : y^2 = x^3 + 4px$ corresponding to E and we similarly define $\bar{\alpha}$ from $\bar{\Gamma}$ to $\overline{\mathbb{Q}^\times}$, namely,

$$\bar{\alpha}(P) = \begin{cases} 1 & \text{for } P = O \\ \beta(p) & \text{for } P = \mathbf{0} \\ \beta(x) & \text{for } x \neq 0 \end{cases}$$

where $P = (x, y) \in \bar{\Gamma}$.

The rank r of the free part $\mathcal{F}$ of Γ is computed from the formula

$$2^r = \frac{|\alpha(\Gamma)||\bar{\alpha}(\bar{\Gamma})|}{4} \text{ (see [1, Corollary 7.5]).}$$

We see the following facts from [1, Theorem 7.6].

The group $\alpha(\Gamma)$ consists of $1, \beta(-p)$ and $\beta(d)$ for divisors d of $-p$ such that

$$dS^4 - \frac{p}{d}T^4 = U^2$$

has a solution of integers S, T and U satisfying

$$(\dagger) \qquad S \geq 1, T \geq 1 \text{ and } (S, \frac{p}{d}) = 1.$$

This paper was financially supported by Fund for the Promotion of International Scientific Research B-2, 2004, Aomori, Japan.

The group $\bar{\alpha}(\bar{\Gamma})$ consists of $1, \beta(4p)$ and $\beta(\bar{d})$ for *positive* divisors $\bar{d}$ of $4p$ such that

$$\bar{d}S^4 + \frac{4p}{\bar{d}}T^4 = U^2$$

has a solution of integers S, T and U satisfying

$$(\ddagger) \qquad S \geq 1, T \geq 1 \text{ and } (S, \frac{4p}{\bar{d}}) = 1.$$

The torsion part $\mathcal{T}$ clearly contains two points O and $\mathbf{0} = (0,0)$ of order 2. Lutz-Nagell theorem (see [1, Theorem 7.11]) states that x and y are integers and y^2 is a divisor of the discriminant $\Delta = 4p^3$ of $x^3 - px$ for $(x,y) \in \mathcal{T} \setminus \{O, \mathbf{0}\}$.

Using this, we have the next theorem.

Theorem 1. $\mathcal{T} = \{O, \mathbf{0}\}$.

Proof. Let $P = (x,y) \neq O,\ \mathbf{0}$ be an element such that x, y are integers and y^2 divides the discriminant $\Delta = 4p^3$ and so $y^2 = 1, 4, p^2, 4p^2$.
Using $y^2 = x(x^2 - p)$ we have solutions in each case.
In case $y^2 = 1$, we have $p = 2, x = -1$.
In case $y^2 = 4$, we have $p = 2, x = 2$ or $p = 5, x = -1$ or $p = 17, x = -4$.
If $y^2 = p^2$ or $4p^2$, then $x = pt$ follows from $y^2 + px = x^3$.
In case $y^2 = p^2$, we have $t = 1, x = p = 2, y^2 = 4$.
In case $y^2 = 4p^2$, we have $t = 1, x = p = 5, y^2 = 100$.

Summarizing these solutions, we have the next table with $2P = (x_2, y_2)$ where $x_2 = (\frac{3x^2-p}{2y})^2 - 2x$.

p	2	2	5	5	17
x	-1	2	-1	5	-4
y^2	1	4	4	100	4
x_2	2.25	2.25	2.25	2.25	68.0625

Thus we have $\mathcal{T} = \{O, \mathbf{0}\}$ since $2P$ has the infinite order. □

The next theorem is the purpose of this paper.

Theorem 2. *Let p be Fermat primes or Mersenne primes. Then we have*

(1) *In case $p = 2^{2^n} + 1$ is a Fermat prime,*

$$\Gamma \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \textit{for } p = 3 \\ \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \textit{for } p = 5 \\ \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \textit{for } p > 5. \end{cases}$$

(2) *In case $p = 2^q - 1$ is a Mersenne prime where q is prime,*

$$\Gamma \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{for } p = 3 \\ \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{for } p > 3. \end{cases}$$

Proof. We already proved $\mathcal{T} = \{O, \mathbf{0}\}$ in Theorem 1.

(1) First we assume $p = 2^{2^n} + 1$ is a Fermat prime.

In case $p = 3$, we have $\left(\frac{-1}{p}\right) = -1$ and so the equation $-S^4 + pT^4 = U^2$ has no integral solutions satisfying conditions (†). Thus $\alpha(\Gamma)$ contains neither $\beta(-1)$ nor $\beta(p)$ since $\alpha(\Gamma)$ is a subgroup of $\overline{\mathbb{Q}^\times}$.

In case $p > 3$, the equation $-S^4 + pT^4 = U^2$ has a solution $S = T = 1$ and $U = 2^{2^{n-1}}$ for $n \geq 1$. Thus $\alpha(\Gamma)$ contains $\beta(-1)$ and also $\beta(p)$ since $\alpha(\Gamma)$ is a subgroup of $\overline{\mathbb{Q}^\times}$. Hence we have

$$\alpha(\Gamma) = \begin{cases} \{1, \beta(-p)\} & \text{for } p = 3 \\ \{\beta(\pm 1), \beta(\pm p)\} & \text{for } p > 3. \end{cases}$$

If the equation $2S^4 + 2pT^4 = U^2$ has a solution satisfying conditions (‡), then $\left(\frac{2}{p}\right) = 1$, contrary to $\left(\frac{2}{p}\right) = -1$ for $p = 3$ or 5. Thus $\bar{\alpha}(\bar{\Gamma})$ contains neither $\beta(2)$ nor $\beta(2p)$ for $p = 3$ or 5 since $\bar{\alpha}(\bar{\Gamma})$ is a subgroup of $\overline{\mathbb{Q}^\times}$.

In case $p > 5$, we set $a = 2^{2^{n-2}}$. Then $p = a^4 + 1$ and $2S^4 + 2pT^4 = U^2$ has the next solutions satisfying conditions (‡).

$$S = a \pm 1,\ T = 1 \text{ and } U = 2(a^2 \pm a + 1).$$

Thus $\bar{\alpha}(\bar{\Gamma})$ contains 2 and also $2p$ since $\bar{\alpha}(\bar{\Gamma})$ is a subgroup of $\overline{\mathbb{Q}^\times}$.

Hence we have the next because $\beta(4) = 1$ and $\beta(4p) = \beta(p)$.

$$\bar{\alpha}(\bar{\Gamma}) = \begin{cases} \{1, \beta(p)\} & \text{for } p = 3, 5 \\ \{1, \beta(2), \beta(p), \beta(2p)\} & \text{for } p > 5. \end{cases}$$

The rank r of $\mathcal{F}$ follows from the formula

$$2^r = \frac{|\alpha(\Gamma)||\bar{\alpha}(\bar{\Gamma})|}{4}.$$

Thus we have

$$r = \begin{cases} 0 & \text{for } p = 3 \\ 1 & \text{for } p = 5 \\ 2 & \text{for } p > 5. \end{cases}$$

(2) Next we assume $p = 2^q - 1$ is a Mersenne prime.

In case $p = 3$, we already see $r = 0$ in (1). Thus we assume q is odd. The equation $-S^4 + pT^4 = U^2$ has no integral solutions satisfying conditions (†) from $\left(\frac{-1}{p}\right) = -1$. Thus $\alpha(\Gamma) = \{1, \beta(-p)\}$.

The equation $2S^4 + 2pT^4 = U^2$ has an integral solution $S = T = 1$ and $U = 2^{\frac{q+1}{2}}$ because q is an odd prime. Thus $\bar{\alpha}(\bar{\Gamma})$ contains $\beta(2), \beta(2p)$ and so $\bar{\alpha}(\bar{\Gamma}) = \{1, \beta(2), \beta(p), \beta(2p)\}$. Hence $r = 1$ follows from

$$2^r = \frac{|\alpha(\Gamma)||\bar{\alpha}(\bar{\Gamma})|}{4} = 2.$$

$\square$

References

[1] J.S. Chahal, *Topics in number theory*, Kluwer Academic/Plenum Publisher, 1988.

Takehiro Kudo
An undergraduate on Jan., 2005
A graduate on Mar., 2005 from
Department of Mathematical system Sciences
Faculty of Science and Technology
Hirosaki University
Hirosaki 036-8561, Japan

Kaoru Motose
Department of Mathematical System Science
Faculty of Science and Technology
Hirosaki University
Hirosaki 036-8561, Japan
e-mail address: skm@cc.hirosaki-u.ac.jp

(*Received January 28, 2005*)