Far East Journal of Mathematical Sciences (FJMS)
Volume 74, Number 1, 2013, Pages 105-117
Published Online: March 2013
Available online at http://pphmj.com/journals/fjms.htm
Published by Pushpa Publishing House, Allahabad, INDIA

POSSIBLE MAXIMAL RANK OF ELLIPTIC CURVE OF THE FORM $y^2 = x^3 + pqx$

Shin-Wook Kim and Hwasin Park

Department of Mathematics
Chonbuk National University
Chonju, Chonbuk 561-756, Korea

Abstract

Let $y^2 = x^3 + pqx$ be an elliptic curve, where p and q are distinct odd primes such that $p \equiv 3 \pmod{16}$ and $q \equiv 11 \pmod{16}$. Then we treat the possible maximal rank of this curve.

1. Introduction

Suppose that $E_{pq} : y^2 = x^3 + pqx$ is an elliptic curve, where p, q are distinct odd primes. And let Γ be the set of rational points on E_{pq}. And by Mordell's theorem, Γ is finitely generated abelian group and also it is isomorphic to $E(Q)_{tors} \oplus Z^r$, where $E(Q)_{tors}$ is a torsion subgroup and r is the rank of an elliptic curve. Then the values of ranks in this form are from 0 to 4. Specially, the maximal rank of the elliptic curve is changed as the conditions of odd primes p and q. In this paper, we compute the possible maximal rank, where p and q are distinct odd primes such that $p \equiv$

2010 Mathematics Subject Classification: 11A41, 14H52.
Keywords and phrases: prime numbers, ranks of elliptic curves.
Submitted by K. K. Azad
Received December 23, 2012

$3 \pmod{16}$ and $q = 11 \pmod{16}$. Before considering the rank, we should assume several notations.

Let α be a homomorphism from Γ to $Q^{\times}/Q^{\times 2}$ which satisfies the following conditions:

$\alpha(P) = 1 \pmod{Q^{\times 2}}$ when $P = O$ (O is an infinity point),

$\alpha(P) = b \pmod{Q^{\times 2}}$ when $P = (0, 0)$,

$\alpha(P) = x \pmod{Q^{\times 2}}$ when $P = (x, y)(x \neq 0)$.

Also, $Q^{\times}$ denotes the set of nonzero rational numbers and it is a multiplicative group. And $Q^{\times 2}$ is the set of squares of elements of $Q^{\times}$.

Now suppose that $\overline{\Gamma}$ is the set of rational points on $\overline{E_{pq}} : y^2 = x(x^2 - 2ax + a^2 - 4b)$ and $\overline{\alpha}$ is a homomorphism from $\overline{\Gamma}$ to $Q^{\times}/Q^{\times 2}$ which satisfies the following:

$\overline{\alpha}(P) = 1 \pmod{Q^{\times 2}}$ when $P = \overline{O}$ (infinity point),

$\overline{\alpha}(P) = a^2 - 4b \pmod{Q^{\times 2}}$ when $P = (0, 0)$,

$\overline{\alpha}(P) = x \pmod{Q^{\times 2}}$ when $P = (x, y)(x \neq 0)$.

And $Q^{\times 2}$, $Q^{\times}$ follow the same notations in the above.

The more thing what we have to treat is an equation which is necessary in computing the rank. Here, we call the equation as relating equation. For Γ, $N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4$ is a relating equation, where b_1 and b_2 are divisors of b and $b_1 b_2 = b$ and b_1 is not congruent to 1, $b \pmod{Q^{\times 2}}$. And (M, e, N) is the solution of the above equation and it should be $M \neq 0$ and $(N, e) = (M, e) = (b_1, e) = (b_2, M) = (M, N) = 1$. Also, relating equation for $\overline{\Gamma}$ is $N^2 = b_1 M^4 - 2aM^2 e^2 + b_2 e^4$ which satisfies the conditions that

$b_1 b_2 = a^2 - 4b$ and b_1 is not congruent to 1, $a^2 - 4b \pmod{Q^{\times 2}}$. And (M, e, N) is also a solution of this equation and other conditions are the same as in the above. And the rank r satisfies $2^r = \frac{|\alpha(\Gamma)||\overline{\alpha}(\overline{\Gamma})|}{4}$.

2. Computing the Rank

In this section, we compute the rank of an elliptic curve by using the method which is in [3].

Theorem 2.1. *Let* $y^2 = x^3 + pqx$ *be an elliptic curve, where p, q are different odd primes of the form* $p \equiv 3 \pmod{16}$, $q \equiv 11 \pmod{16}$. *Then the possible maximal rank is* 2.

Proof. Put an elliptic curve E_{pq} as $y^2 = x^3 + pqx$ and the different odd prime numbers p, q are $p \equiv 3 \pmod{16}$, $q \equiv 11 \pmod{16}$. For computation, let $p = 16k + 3$ and $q = 16k' + 11$.

We know that the relating equations for Γ are the following:

(i) $N^2 = M^4 + (16 + 3)(16k' + 11)e^4$,

(ii) $N^2 = (16k + 3)M^4 + (16k' + 11)e^4$.

As we defined in the previous section, the value $\alpha(P)$ is $\alpha(P) = 1$, $(16k + 3)(16k' + 11) \pmod{Q^{\times 2}}$ if P is O (infinity point), $(0, 0)$, respectively, thus we do not have to treat the solvability of equation (i).

Suppose that equation (ii) has a solution. Then two congruence relations

$$N^2 \equiv (16k + 3)M^4 \pmod{q}, \quad N^2 \equiv (16k' + 11)e^4 \pmod{p}$$

must have solutions simultaneously. Instantly, it should be $\left(\frac{(16k + 3)M^4}{q}\right)$ $= \left(\frac{p}{q}\right) = 1$, $\left(\frac{(16k' + 11)e^4}{p}\right) = \left(\frac{q}{p}\right) = 1$. But the Legendre symbols of $\left(\frac{p}{q}\right)$

and $\left(\frac{q}{p}\right)$ are different, thus one of $\left(\frac{(16k+3)M^4}{q}\right)$ and $\left(\frac{(16k'+11)e^4}{p}\right)$ must be –1. Therefore, we get a contradiction.

Thus the number of $\alpha(\Gamma)$ is 2.

Since E_{pq} is $y^2 = x^3 + (16k+3)(16k'+11)x$, $\overline{E_{pq}}$ is the curve $y^2 = x^3 - 4(16k+3)(16k'+11)x$ and there are relating equations for $\overline{\Gamma}$:

(i) $N^2 = M^4 - 4(16k+3)(16k'+11)e^4$,

(ii) $N^2 = -M^4 + 4(16k+3)(16k'+11)e^4$,

(iii) $N^2 = 2M^4 - 2(16k+3)(16k'+11)e^4$,

(iv) $N^2 = -2M^4 + 2(16k+3)(16k'+11)e^4$,

(v) $N^2 = 4M^4 - (16k+3)(16k'+11)e^4$,

(vi) $N^2 = -4M^4 + (16k+3)(16k'+11)e^4$,

(vii) $N^2 = (16k+3)M^4 - 4(16k'+11)e^4$,

(viii) $N^2 = -(16k+3)M^4 + 4(16k'+11)e^4$,

(viv) $N^2 = 2(16k+3)M^4 - 2(16k'+11)e^4$,

(x) $N^2 = -2(16k+3)M^4 + 2(16k'+11)e^4$,

(xi) $N^2 = 4(16k+3)M^4 - (16k'+11)e^4$,

(xii) $N^2 = -4(16k+3)M^4 + (16k'+11)e^4$.

$\overline{\alpha}(P)$ in (i) are $\overline{\alpha}(P) = 1$, $-4(6k+3)(16k'+11) (\mathrm{mod}\, Q^{\times 2})$ but we already know that these were defined when P is an infinity point, $(0, 0)$,

respectively, in the previous section, hence checking the solvability is of no use.

By using the prime number p in reducing (ii), (iii) and (vi), we get the following results:

(ii) $N^2 \equiv -M^4 \pmod{p}, \left(\frac{-M^4}{p}\right) = -1,$

(iii) $N^2 \equiv 2M^4 \pmod{p}, \left(\frac{2M^4}{p}\right) = -1,$

(vi) $N^2 \equiv -4M^4 \pmod{p}, \left(\frac{-4M^4}{p}\right) = -1.$

Thus there cannot be a solution in (ii), (iii), (vi). And there is no solution in (v) because of $1 \equiv N^2 \equiv -33e^4 \equiv 3e^4 \equiv 3 \pmod{4}$.

And by reducing $\pmod{4}$ in equations (vii), (xii), then we face the results:

(vii) $1 \equiv N^2 \equiv 3M^4 \equiv 3 \pmod{4}$, (xii) $1 \equiv N^2 \equiv 3e^4 \equiv 3 \pmod{4}$.

Since both left and right hand sides do not match in the above cases, there is no solution in equations (vii), (xii).

Now we treat the solvability of equation (iv). Reducing this by $\pmod{q,\ p}$, then there induced the results $N^2 \equiv -2M^4 \pmod{q}$, $N^2 \equiv -2M^4 \pmod{p}$. And the Legendre symbols of $\left(\frac{-2M^4}{q}\right)$ and $\left(\frac{-2M^4}{p}\right)$ are 1. And so having a solution is possible in equation (iv). And for checking the solvability of relating equation, we use the method of reduction by integer. The case of 4, 8, 16 is relatively simple. Thus in here, we treat the case of 32. If we reduce (iv) by 32, then the left hand side is $N^2 \equiv 0, 4, 16 \pmod{32}$

and the right hand side is

$$-2M^4 + 2(16k+3)(16k'+11)e^4$$

$$\equiv 30M^4 + 2(16\cdot 11k + 48k' + 33)e^4$$

$$\equiv 30 + 2(16k + 16k' + 1)e^4 \equiv 30 + 2e^4 \equiv 30 + 2 \equiv 0 \pmod{32}.$$

Therefore, there can exist a solution in equation (iv). And in the next cases, we check the reduction only the case 32.

If we reduce equation (viii) by q and p, respectively, then we face the two congruence relations

$$N^2 \equiv -(16k+3)M^4 \pmod{q}, \quad N^2 \equiv 4(16k'+11)e^4 \pmod{p}.$$

And the two things should have solutions simultaneously. And it is possible that both values of

$$\left(\frac{-(16k+3)M^4}{q}\right) = -\left(\frac{p}{q}\right) \text{ and } \left(\frac{4(16k'+11)e^4}{p}\right) = \left(\frac{q}{p}\right)$$

can be 1 this is because the value of $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ is different. Thus having a solution in (viii) is possible. In addition, if we try to use the method of reduction by 32, then the left hand side is $N^2 \equiv 1, 9, 17, 25 \pmod{32}$ and the right hand side is

$$-(16k+3)M^4 + 4(16k'+11)e^4 \equiv 31(16k+3)M^4 + 12e^4$$

$$\equiv (16k+29)\cdot 17 + 12e^4$$

$$\equiv 16k + 13 + 12e^4 \pmod{32}.$$

Let k and e be odd numbers. Then $16k + 13 + 12e^4 \equiv 16 + 13 + 12 = 41 \equiv 9 \pmod{32}$ and so there can exist a solution in (viii).

Reducing (viv) by q and p leads to $N^2 \equiv 2(16k+3)M^4 \pmod{q}$, $N^2 \equiv -2(16k'+11)e^4 \pmod{p}$. And both of the Legendre symbols in $\left(\frac{2(16k+3)M^4}{q}\right) = -\left(\frac{p}{q}\right)$ and $\left(\frac{-2(16k'+11)M^4}{p}\right) = \left(\frac{q}{p}\right)$ can be 1 because of the fact that $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ and so there can be a solution in (viv). And if we reduce both sides of (viv) by $\pmod{32}$, then there induced the result as $0, 4, 16 \equiv N^2 \equiv 6M^4 + 10e^4 \equiv 6 + 10 = 16 \pmod{32}$. Hence, there can exist a solution in equation (viv).

By reducing equation (x) $\pmod{q,\ p}$, we face two induced results

$$N^2 \equiv -2(16k+3)M^4 \pmod{q} \quad \text{and} \quad N^2 \equiv 2(16k'+11)e^4 \pmod{p}.$$

These two congruence relations must have a solution together. And Legendre symbols of $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ are not the same, thus both $\left(\frac{-2(16k+3)M^4}{q}\right)$ and $\left(\frac{2(16k'+11)e^4}{p}\right)$ can be 1, hence a solution can exist. Furthermore, reducing (x) by 32 leaves the result as

$$0, 4, 16 \equiv N^2 = -2(16k+3)M^4 + 2(16k'+11)e^4$$

$$\equiv -6M^4 + 22e^4 \equiv 26M^4 + 22e^4 \pmod{32}.$$

Since M and e are odd numbers,

$$26M^4 + 22e^4 \equiv 26 \cdot 17 + 22 \equiv 26 + 22 \equiv 16 \pmod{32},$$

thus (x) can have a solution.

If we reduce (xi) by q, p, respectively, then the induced two congruence relations are $N^2 \equiv 4(16k+3)M^4 \pmod{q}$, $N^2 \equiv -(16k'+11)e^4 \pmod{p}$

and both should have a solution simultaneously. Namely,

$$\left(\frac{4(16k+3)M^4}{q}\right)\left(\frac{p}{q}\right) \text{ and } \left(\frac{-(16k'+11)e^4}{p}\right) = -\left(\frac{q}{p}\right)$$

should be 1 and this is possible because of $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Furthermore, after reducing (xi) by 32, we face the result as

$$1, 9, 17, 25 \equiv N^2 \equiv 12M^4 + 31(16k'+11)e^4 \pmod{32}.$$

If k' is an even, then $12M^4 + (16k'+21)e^4 \equiv 12M^4 + 21e^4 \pmod{32}$ and let M be an odd and $e = 1$. Then induced congruence relation is $12M^4 + 21e^4 \equiv 12 + 21 \equiv 1 \pmod{32}$, therefore having a solution is possible in equation (xi).

In conclusion, if we rewrite the relating equations which can have a solution are the following:

(i) $N^2 = M^4 - 4(16k+3)(16k'+11)e^4$,

(iv) $N^2 = -2M^4 + 2(16k+3)(16k'+11)e^4$,

(viii) $N^2 = -(16k+3)M^4 + 4(16k'+11)e^4$,

(viv) $N^2 = 2(16k+3)M^4 - 2(16k'+11)e^4$,

(x) $N^2 = -2(16k+3)M^4 + 2(16k'+11)e^4$,

(xi) $N^2 = 4(16k+3)M^4 - (16k'+11)e^4$.

Now the possible maximal number of relating equations which can have a solution is 4. We should consider about this.

If all equations of the above have a solution, then $2(16k+3) \in \overline{\alpha}(\overline{\Gamma}) \pmod{Q^{\times 2}}$ and $-2(16k+3) \in \overline{\alpha}(\overline{\Gamma}) \pmod{Q^{\times 2}}$ ($2(16k+3)$ correspond

to (viv), $-2(16k+3)$ corresponds to (x)) and so $-1 \in \overline{\alpha}(\overline{\Gamma}) (\mathrm{mod}\, Q^{\times 2})$ because $\overline{\alpha}(\overline{\Gamma})$ is a subgroup of $Q^{\times}/Q^{\times 2}$. But as we saw in the above, equation (ii) $N^2 = -M^4 + 4(16k+3)(16k'+11)e^4$ cannot have a solution, thus we arrive at a contradiction. Therefore, there cannot happen the case that all 6 relating equations in the above have solutions. Similarly, it is impossible that 5 relating equations have solutions simultaneously. For example, assume that equations (i), (iv), (viii), (viv), (x) have solutions. Then $-(16k+3) \in \overline{\alpha}(\overline{\Gamma}) (\mathrm{mod}\, Q^{\times 2})$ and $-2(16k+3) \in \overline{\alpha}(\overline{\Gamma}) (\mathrm{mod}\, Q^{\times 2})(-(16k+3)$ correspond to (viii) and $-2(16k+3)$ corresponds to (x)) and so $2 \in \overline{\alpha}(\overline{\Gamma}) (\mathrm{mod}\, Q^{\times 2})$. But equation (iii) $N^2 = 2M^4 - (16k+3)(16k'+11)e^4$ has no solution and so we face a contradiction. Other cases can also be proved like this method.

Whereas, the case that 4 relating equations have solutions is possible. Theses cases are (i), (iv), (viii), (viv) and (i), (iv), (x), (xi). There is no matter in closeness of multiplication of $\overline{\alpha}(\overline{\Gamma})$ in these two cases. Accordingly, the maximal number of $\overline{\alpha}(\overline{\Gamma})$ is 8 and thus from $2^r = \frac{2 \cdot 8}{4} = 4$, the possible maximal rank of E_{pq} is 2. □

In [1], the authors suggested the special condition that $p \equiv 1 \pmod 8$ and q is different from p and the form of $q = p^2 + 24p + 400$ and there are rational numbers X, Y such that $Y^2 = 2X^4 - 2pq$ for an elliptic curve $y^2 = x^3 + pqx$ has a rank 4 which is a maximal rank in the form. Similarly, in [2], there is a particular condition that $2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4$, where p is a prime and u, v are integers for having a maximal rank 3 in form $y^2 = x^3 - 2px$. The ranks 4 and 3 are not only ranks, respectively, in those forms, but under those conditions, they are the only ranks in each case and it is the maximal value. But here, the conditions $p \equiv 3 \pmod{16}$ and $q \equiv 11 \pmod{16}$ are not detail as the conditions in [1] and [2], thus there can

be other values of ranks but we only concentrate to the maximal rank 2 here and this is the reason why the author uses the word possible maximal rank.

And we need to consider the residue $17 \pmod{32}$. It is natural that 1, 9, 25 is residue $\bmod 32$. But case of 17 requires the computation.

First, put an odd integer N as $N = 4k + 1$ with integer k. Then we get $N^2 = 16k^2 + 8k + 1$.

(1) If k is an odd $(k = 2k' + 1$ and $k' \in Z)$, then

$$N^2 = 16(4k'^2 + 4k' + 1) + 8(2k' + 1) + 1 \equiv 16 + 16k' + 9 = 16k' + 25 \pmod{32}.$$

When k' is $k' = 2a + 1$ $(a \in Z)$,

$$16k' + 25 = 16(2a + 1) + 25 \equiv 16 + 25 \equiv 9 \pmod{32}.$$

And when k' is $k' = 2a$ (a is an integer), then $16k' + 25 \equiv 25 \pmod{32}$.

(2) If k is an even $(k = 2k'$ with integer $k')$, then $N^2 = 16 \cdot 4k'^2 + 8 \cdot 2k' + 1 \equiv 16k' + 1 \pmod{32}$. When $k' = 2a + 1$ (a is an integer), then $16k' + 1 \equiv 16(2a + 1) + 1 \equiv 17 \pmod{32}$. And when $k' = 2a$ (a is an integer), then $16k' + 1 \equiv 1 \pmod{32}$.

At last, $N^2 \equiv 1, 9, 17, 25 \pmod{32}$.

Second, let $N = 4k + 3$ (k is an integer). Then $N^2 = 16k^2 + 24k + 9$.

(1) If k is an odd $(k = 2k' + 1$ with k' is an integer), then

$$N^2 = 16(4k'^2 + 4k' + 1) + 24(2k' + 1) + 9 \equiv 16 + 16k' + 33$$

$$\equiv 16k' + 17 \pmod{32}.$$

When $k' = 2a + 1$ (a is an integer), then $16k' + 17 \equiv 16 + 17 \equiv 1 \pmod{32}$. And when $k' = 2a$ (a is an integer), then $16k' + 17 \equiv 17 \pmod{32}$.

(2) If k is an even ($k = 2k'$ with k' is an integer), then $N^2 = 16 \cdot 4k'^2 + 24 \cdot 2k' + 9 \equiv 16k' + 9 \pmod{32}$. When $k' = 2a + 1$ (a is an integer), then $16k' + 9 = 16(2a + 1) + 9 \equiv 25 \pmod{32}$. And when $k' = 2a$ (a is an integer), then $16k' + 9 \equiv 9 \pmod{32}$.

Henceforth, we get that $N^2 \equiv 1, 9, 17, 25 \pmod{32}$.

Therefore, if an odd integer N is reduced by 32, then the induced thing is $N^2 \equiv 1, 9, 17, 25 \pmod{32}$. And thus 17 can be the residue mod 32.

If we compute the above process by setting $N = 2k + 1$, then $N^2 = 4k^2 + 4k + 1$ and by dividing k as odd, even and doing detail computation, then the same result is induced.

3. Considering Examples

In this section, we consider an example of an elliptic curve which is related to previous section's theorem. We omit to say about the solution of relating equation (i) for Γ, $\overline{\Gamma}$.

Example 3.1. Suppose that $y^2 = x^3 + 3 \cdot 11x$ is an elliptic curve. Then it is clear that $\#\alpha(\Gamma) = 2$ and the relating equations for $\overline{\Gamma}$ what we have to treat are the following:

(i) $N^2 = M^4 - 4 \cdot 3 \cdot 11e^4$, (iv) $N^2 = -2M^4 + 2 \cdot 3 \cdot 11e^4$,

(viii) $N^2 = -3M^4 + 4 \cdot 11e^4$, (viv) $N^2 = 6M^4 - 22e^4$,

(x) $N^2 = -6M^4 + 22e^4$, (xi) $N^2 = 4 \cdot 3M^4 - 11e^4$.

Equations (iv), (x), (xi) have solutions $(1, 1, 8)$, $(1, 1, 4)$, $(1, 1, 1)$, respectively. And (viii), (viv) have no solution. This is because if (viii) has a solution, then $-3 \cdot -6 \equiv 2 \in \overline{\alpha}(\overline{\Gamma}) \pmod{Q^{\times 2}}$. But as we know, equation (iii) $N^2 = 2M^4 - 2 \cdot 3 \cdot 11e^4$ has no solution, thus we arrive at a contradiction.

If (viv) has a solution, then $6 \cdot (-6) \equiv -1 \in \overline{\alpha}(\overline{\Gamma}) (\mathrm{mod}\, Q^{\times 2})$. But it is impossible having a solution in (ii) $N^2 = -M^4 + 4(16k + 3)(16k' + 11)e^4$.

Accordingly, the number of $\overline{\alpha}(\overline{\Gamma})$ is 8 and so the rank is 2.

Example 3.2. If we consider the rank of an elliptic curve $y^2 = x^3 + 19 \cdot 11x$, then we get easily that $\#\alpha(\Gamma) = 2$. And relating equations for $\overline{\Gamma}$ which we should consider are the following:

(i) $N^2 = M^4 - 4 \cdot 19 \cdot 11e^4$, (iv) $N^2 = -2M^4 + 2 \cdot 19 \cdot 11e^4$,

(viii) $N^2 = -19M^4 + 44e^4$, (viv) $N^2 = 2 \cdot 19M^4 - 2 \cdot 11e^4$,

(x) $N^2 = -2 \cdot 19M^4 + 2 \cdot 11e^4$, (xi) $N^2 = 4 \cdot 19M^4 - 11e^4$.

And equations (iv), (viii), (viv) has a solution $(3, 1, 16)$, $(1, 1, 5)$, $(1, 1, 4)$, respectively. And two equations (x) and (xi) have no solutions and we can show this by similar method as in Example 3.1. Thereby, the rank of $y^2 = x^3 + 19 \cdot 11x$ is 2.

Example 3.1 is the case of (i), (iv), (x), (xi) and Example 3.2 is that of (i), (iv), (viii), (viv) in the proof of Theorem 2.1.

Remark 3.3. As we saw in the above examples, according to the curve, the relating equation's solvability is different. In Example 3.1, equations (viii) and (viv) have no solution and in case of Example 3.2, (x) and (xi) have no solution.

Remark 3.4. Even though, there are induced same residues in both sides of relating equations ((viv) of Example 3.1 and (x) of Example 3.2) after reducing any number, they cannot have a solution, because as we saw in Theorem 2.1, if there exists a solution, then from closedness of operation in group $\overline{\alpha}(\overline{\Gamma})$, a contradiction happens. We can find similar phenomenon in relating equation $N^2 = 17M^4 - 4e^4$ in elliptic curve $y^2 = x^3 + 17x$ whose rank is 0 ([2, p. 98]).

References

[1] Angela J. Hollier, Blair K. Spearman and Qiduan Yang, Elliptic curves $y^2 = x^3 + pqx$ with maximal rank, Int. Math. Forum 5(23) (2010), 1105-1110.

[2] Blair K. Spearman, On the group structure of elliptic curves $y^2 = x^3 - pqx$, Int. J. Algebra 1(5) (2007), 247-250.

[3] J. H. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer, New York, 1985.