International Journal of Algebra, Vol. 12, 2018, no. 1, 15 - 23
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2018.71257

Mersenne Prime's Inducement

Shin-Wook Kim

Deokjin-gu, Songcheon 54823
101-703, I-Park Apt
Jeonju, Jeonbuk, Korea

Abstract

We appoint that $y^2 = x^3 - 2px$ and $y^2 = x^3 + 4px$ and $y^2 = x^3 + 8px$ are elliptic curves where p is a Mersenne prime number. Then, the rank of these curves will be calculated.

Mathematics Subject Classification: 11A41, 11G05

Keywords: Mersenne prime, Elliptic curve

1 Introduction

In [1], the rank of an elliptic curve of the form $y^2 = x^3 + pqx$ was considered and in [2], the authors showed that rank of elliptic curve $E_n : y^2 = x^3 - nx$ is at least 3 if an integer n is written as a sum of two biquadrates in two different ways and in addition if n is odd and the parity conjecture is true then, the rank of E_n is even and at least 4. In [3], the author treated ranks of elliptic curves $y^2 = x^3 \pm 4px$ with odd prime p. In [7], Walsh proved that rank of $E_{-2p} : y^2 = x^3 - 2px$ is 3 under the supposition that there are two positive rational points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on E_{-2p} and a positive rational point $P_3 = (x_3, y_3)$ on $E_{8p} : y^2 = x^3 + 8px$ with $x_i = d_i u_i^2 (1 \leq i \leq 3)$(each d_i is squarefree and $u_i \in Q$) and furthermore $(d_1, d_2) \in \{(-1, 2), (-1, -2), (-1, p), (2, -2), (2, p)\}$, $d_3 \in \{2, p\}$. In [4], the authors computed that rank of an elliptic curve $y^2 = x^3 - px$ where p is a Mersenne prime is 0 when $p = 3$ and 1 when $p > 3$. In this paper, we will investigate the ranks of elliptic curves $y^2 = x^3 - 2px$ and $y^2 = x^3 + 4px$ and $y^2 = x^3 + 8px$ where p is a Mersenne prime.

Before researching the ranks of elliptic curves, we must survey some notations in [6].

We take E as an elliptic curve $y^2 = x^3 + ax^2 + bx$ and suppose that Γ is the set of rational points on E. Then, by $Mordell's$ theorem Γ is a finitely generated abelian group and Γ is isomorphic to $E(Q)_{tors} \oplus Z^r$. Here, $E(Q)_{tors}$ denotes a torsion subgroup and r is the $Mordell\text{-}Weil$ rank. Assume that $Q^\times$ is the set of nonzero rational numbers then, it is a multiplicative group. Furthermore, $Q^{\times 2}$ is the subgroup of squares of elements of $Q^\times$.

Next, we make a supposition that α is a homomorphism from Γ to $Q^\times/Q^{\times 2}$ which satisfies that

$$\alpha(O) = 1(\text{mod } Q^{\times 2}),$$

$$\alpha(0,0) = b(\text{mod } Q^{\times 2}),$$

$$\alpha(x,y) = x(\text{mod } Q^{\times 2}).$$

In the above, O is infinity point and x is nonzero.

For Γ, we appoint that $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ is the relating equation and the coefficients b_1 and b_2 should be $b_1b_2 = b$ and $b_1 \not\equiv 1, b(\text{mod } Q^{\times 2})$. Assume that (M, e, N) is the integral solution of above relating equation then, neither M nor e is zero and there educed that $1 = (M, N) = (b_1, e) = (b_2, M) = (N, e) = (M, e)$.

In the next step, we needed to treat the curve $\overline{E} : y^2 = x(x^2-2ax+a^2-4b)$. Put $\overline{\Gamma}$ as the set of rational points on $\overline{E}$. Set $\overline{\alpha}$ as a homomorphism from $\overline{\Gamma}$ to $Q^\times/Q^{\times 2}$ where the followings are hold:

$$\overline{\alpha}(O) = 1(\text{mod } Q^{\times 2}),$$

$$\overline{\alpha}(0,0) = a^2 - 4b(\text{mod } Q^{\times 2}),$$

$$\overline{\alpha}(x,y) = x(\text{mod } Q^{\times 2}).$$

In the above, O is infinity point and $x \neq 0$.

For $\overline{\Gamma}$, let $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ be the relating equation where b_1 and b_2 satisfy that $b_1b_2 = a^2-4b$ and $b_1 \not\equiv 1, a^2-4b(\text{mod } Q^{\times 2})$. Take (M, e, N) as the integral solution of relating equation for $\overline{\Gamma}$. Then, $M \neq 0$ and $e \neq 0$ and there comes that $1 = (M, N) = (b_1, e) = (b_2, M) = (N, e) = (M, e)$.

In the last case, $2^r = \frac{\#\alpha(\Gamma)\#\overline{\alpha}(\overline{\Gamma})}{4}$ holds where r is the rank of an elliptic curve E.

2 Investigation

Now in this section, we calculate the ranks of $y^2 = x^3 - 2px$ and $y^2 = x^3 + 4px$ and $y^2 = x^3 + 8px$ by the method in [6].

Theorem 2.1 (1). *Define E_{-2p} as an elliptic curve $y^2 = x^3 - 2px$ where p is a Mersenne prime $p = 2^q - 1$(q is an odd prime) such that $q = 4t + 1$ with integer t as $t \geq 1$ then, the result $rank(E_{-2(2^q-1)}(Q)) = 1$ is induced.*

(2). *Designate E_{4p} as an elliptic curve $y^2 = x^3 + 4px$ which satisfies that p is a Mersenne prime $p = 2^q - 1$(q is a prime). Then, we conclude that $rank(E_{4(2^q-1)}(Q)) = 0$ if $p = 3$ and $rank(E_{4(2^q-1)}(Q)) = 1$ if p is such that $p > 3$ and an odd prime q as $q = 4t + 1$ with integer t as $t \geq 1$.*

(3). *Suppose that E_{8p} is an elliptic curve $y^2 = x^3 + 8px$ where p is a Mersenne prime $p = 2^q - 1$ with an odd prime q as $q = 4t + 1$(t is an integer) and $t \geq 1$. Then, we encounter to $rank(E_{8(2^q-1)}(Q)) = 1$.*

Proof. (1). Denote E_{-2p} as an elliptic curve $y^2 = x^3 - 2px$ where p is a Mersenne prime $p = 2^q - 1$ that satisfies an odd prime q is such that $q = 4t+1$ with integer t as $t \geq 1$. Then, the relating equations for Γ are as follows:

$$1)N^2 = M^4 - 2(2^q - 1)e^4,$$

$$2)N^2 = -M^4 + 2(2^q - 1)e^4,$$

$$3)N^2 = 2M^4 - (2^q - 1)e^4,$$

$$4)N^2 = -2M^4 + (2^q - 1)e^4.$$

The values $\alpha(P)$ in relating equation 1) are $\alpha(P) = 1, -2(2^q-1) (\mathrm{mod}\ Q^{\times 2})$ and it were considered already in previous section. Thus, it doesn't have to be treated the solvability of 1).

Two equations 2) and 4) cannot have a solution because reducing these by p leaves $2)N^2 \equiv -M^4 (\mathrm{mod}\ p)$ and $4)N^2 \equiv -2M^4 (\mathrm{mod}\ p)$ respectively but at the same time the results $2)(\frac{-M^4}{p}) = -1$ and $4)(\frac{-2M^4}{p}) = -1$ are induced, hence there happens a contradiction in each case.

In equation 3), put $M = 2^t$ and $e = 1$ then, we attain that $2(2^t)^4 - (2^q - 1) = 2^{4t+1} - 2^q + 1$. From assumption, q is $q = 4t + 1$ with integer $t(t \geq 1)$ and thus we face that $2^{4t+1} - 2^{4t+1} + 1 = 1$. Therefore $(2^t, 1, 1)$ is a solution of relating equation 3).

Accordingly, we obtain that $\#\alpha(\Gamma) = 4$.

Next from E_{-2p}, $\overline{E_{-2p}}$ is the curve $y^2 = x^3 + 8px$ and so there are 4 relating equations for $\overline{\Gamma}$ as follows:

$$1)N^2 = M^4 + 8(2^q - 1)e^4,$$

$$2)N^2 = 2M^4 + 4(2^q - 1)e^4,$$

$$3)N^2 = 4M^4 + 2(2^q - 1)e^4,$$

$$4)N^2 = 8M^4 + (2^q - 1)e^4.$$

The values $\overline{\alpha}(P)$ in 1) are $\overline{\alpha}(P) = 1, 8(2^q - 1) \equiv 1, 2(2^q - 1)(\text{mod } Q^{\times 2})$ but these were already treated in the previous, hence we need not to check the solvability of it.

After reducing 2) by 4 then, we acquire that $0 \equiv N^2 \equiv 2M^4 \equiv 2(\text{mod } 4)$ and so there cannot exist a solution in 2).

From supposition $q = 4t + 1$ with integer t as $t \geq 1$, we attain that $q \geq 5$ and so the result $2^q \geq 32$ is induced. Accordingly, 2^q contains 32 as a factor of it, namely it can be expressed as $2^q = 32 \cdot \Upsilon = 4 \cdot 8\Upsilon$ with integer Υ. Thus, if we reduce relating equations 3) and 4) by 4 then, we obtain that $3)0 \equiv N^2 \equiv 2(2^q - 1)e^4 \equiv 2e^4 \equiv 2(\text{mod } 4)$ and $4)1 \equiv N^2 \equiv (2^q - 1)e^4 \equiv 3e^4 \equiv 3(\text{mod } 4)$ respectively. Since two sides are unmatched in above results, relating equations 3) and 4) cannot possess a solution.

Hence, we know that $\#\overline{\alpha}(\overline{\Gamma}) = 2$ and from the fact $2^r = \frac{4 \cdot 2}{4} = 2$, we say that $rank(E_{-2(2^q-1)}(Q)) = 1$.

(2). Assume that E_{4p} is an elliptic curve $y^2 = x^3 + 4px$ where p is a Mersenne prime $p = 2^q - 1$ with a prime q. Then, there comes the relating equations for Γ as $1)N^2 = M^4 + 4(2^q - 1)e^4$, $2)N^2 = 2M^4 + 2(2^q - 1)e^4$, $3)N^2 = 4M^4 + (2^q - 1)e^4$.

The values $\alpha(P)$ in relating equation 1) are $\alpha(P) = 1, 4(2^q - 1) \equiv 1, 2^q - 1(\text{mod } Q^{\times 2})$ and it were already treated, hence we can omit to investigate the solvability of 1).

Now for treating the rank of E_{4p}, we divide prime p by two cases.

First, suppose that $p = 2^q - 1 = 3$.

Then, equation 2) is $N^2 = 2M^4 + 2 \cdot 3e^4$. Reducing this by 3 educes $N^2 \equiv 2M^4(\text{mod } 3)$ but the value of $(\frac{2M^4}{3})$ is -1 and hence we face a contradiction, thus taking a solution is impossible in 2).

Next, equation 3) is $N^2 = 4M^4 + 3e^4$ and so reducing it by 4 leaves $1 \equiv N^2 \equiv 3e^4 \equiv 3(\text{mod } 4)$. Owing to unmatched relation in this result, possessing a solution is impossible in 3).

Consequently, we attain that $\#\alpha(\Gamma) = 2$ for $p = 2^q - 1 = 3$.

Second, suppose that prime p is gotten as $p = 2^q - 1 > 3$ where an odd prime q is given as $q = 4t + 1$ with integer $t(t \geq 1)$.

Because q is of the form $q = 4t + 1$ with integer $t(t \geq 1)$, substitute 1 into both M and e in equation 2), then we attain that $2+2(2^q-1) = 2+2\cdot 2^q-2 = 2 \cdot 2^{4t+1} = 2^{4t+2} = (2^{2t+1})^2$. Thus $(1, 1, 2^{2t+1})$ is a solution of equation 2).

Next, reducing equation 3) by 4 then, we are confronted with $1 \equiv N^2 \equiv (2^q - 1)e^4 \equiv -e^4 (\text{mod } 4)$ this is because we know that $q \geq 5$ from the supposition $q = 4t + 1$ with integer $t(t \geq 1)$, hence the result $2^q \geq 32$ is given, thus 2^q contains 32 as a factor of it and so the expression $2^q = 32 \cdot \Upsilon_1 = 4 \cdot 8\Upsilon_1$ with integer Υ_1 is produced and thus in the process of calculation of reduction by 4, the number 2^q is eliminated. Now if we do more computation then, it is $-e^4 \equiv 3e^4 \equiv 3(\text{mod } 4)$. Because both RHS and LHS don't match, we arrive at a contradiction. Accordingly, relating equation 3) cannot take a solution.

Thereby, we say that $\#\alpha(\Gamma) = 4$ for $p = 2^q - 1 > 3$.

Next from E_{4p}, $\overline{E_{4p}}$ is the curve $y^2 = x^3 - 16(2^q - 1)x$ and so we gain relating equations for $\overline{\Gamma}$ as follows:

$$1)N^2 = M^4 - 16(2^q - 1)e^4,\ 2)N^2 = -M^4 + 16(2^q - 1)e^4,$$

$$3)N^2 = 2M^4 - 8(2^q - 1)e^4,\ 4)N^2 = -2M^4 + 8(2^q - 1)e^4,$$

$$5)N^2 = 4M^4 - 4(2^q - 1)e^4,\ 6)N^2 = -4M^4 + 4(2^q - 1)e^4,$$

$$7)N^2 = 8M^4 - 2(2^q - 1)e^4,\ 8)N^2 = -8M^4 + 2(2^q - 1)e^4,$$

$$9)N^2 = 16M^4 - (2^q - 1)e^4,\ 10)N^2 = -16M^4 + (2^q - 1)e^4.$$

The values $\overline{\alpha}(P)$ in 1) and 9) are the same as $\overline{\alpha}(P) = 1, -16(2^q - 1) \equiv 1, -(2^q - 1)(\text{mod } Q^{\times 2})$. These were defined in the previous section already, thus we can omit to consider the solvability of equations 1) and 9).

If equations 2) and 3) and 4) are reduced by 4 then, there derived that $2)1 \equiv N^2 \equiv -M^4 \equiv 3M^4 \equiv 3(\text{mod } 4)$ and $3), 4)0 \equiv N^2 \equiv 2M^4 \equiv 2(\text{mod } 4)$ respectively and two sides don't match in these results, hence taking a solution is impossible in these equations.

Equation 6) cannot possess a solution since reducing this by prime p yields that $6)N^2 \equiv -4M^4(\text{mod } p)$ but we also acquire that $(\frac{-4M^4}{p}) = -1$ and thus there induced a contradiction.

If we reduce equation 10) by prime p then, we are faced with $N^2 \equiv -16M^4(\text{mod } p)$ but at the same time we know that $(\frac{-16M^4}{p}) = -1$. These two facts cannot exist simultaneously and thus a contradiction happens. Hence, there is no solution in 10).

In respect of equation 5), if we take $p = 3$ then, 5) is $N^2 = 4M^4 - 4 \cdot 3e^4$. If we reduce this relating equation by 16 then, deduced relation is $0, 4 \equiv N^2 \equiv 4M^4 - 12e^4 \equiv 4M^4 + 4e^4 \equiv 4 + 4 = 8(\text{mod } 16)$ and this is unmatched result and so there comes a contradiction. Therefore, taking a solution is impossible. Next, suppose that $p = 2^q - 1 > 3$ where an odd prime q is gotten as $q = 4t+1$

with integer $t(t \geq 1)$. Then, we acquire that $q \geq 5$ and so there educed that $2^q \geq 32$ and hence 2^q can be rewritten as $2^q = 32 \cdot \bigotimes$ with integer $\bigotimes$. Thus, $-4 \cdot 2^q$ is expressed as $-4 \cdot 2^q = -4 \cdot 32 \cdot \bigotimes = 32 \cdot (-4) \cdot \bigotimes$. Consequently, if we reduce relating equation 5) by 16 then, we obtain the relation $0, 4 \equiv N^2 \equiv 4M^4 + 4e^4 \equiv 4 + 4 = 8(\text{mod } 16)$. Thus, both sides do not match in this arithmetical result and so we gain a contradiction. Consequentially, there cannot exist a solution in equation 5).

Next, for two relating equations 7) and 8) assume that $p = 2^q - 1 = 3$. Then, those equations are 7)$N^2 = 8M^4 - 2 \cdot 3e^4$ and 8)$N^2 = -8M^4 + 2 \cdot 3e^4$ respectively. If it were reduced by 16 then, educed calculations are 7)$0, 4 \equiv N^2 \equiv 8M^4 + 10e^4 \equiv 8 + 10 = 18 \equiv 2(\text{mod } 16)$ and 8)$0, 4 \equiv N^2 \equiv -8M^4 + 6e^4 \equiv 8M^4 + 6e^4 \equiv 8 + 6 = 14(\text{mod } 16)$ respectively. Because unmatched relations are produced in two cases, we arrive at a contradiction in each case. For that reason, there cannot exist a solution in equations 7) and 8). Next, suppose that $p = 2^q - 1 > 3$ where an odd prime q is gotten as $q = 4t + 1$ with integer t as $t \geq 1$. Henceforth, we attain that $q \geq 5$ and so the result $2^q \geq 32$ is derived. Thus, there exists 32 as a factor of 2^q. For this reason, the number 2^q can be expressed as $2^q = 32 \cdot \bigotimes_1$ with integer $\bigotimes_1$. And so as a part of coefficient of e^4, both $-2 \cdot 2^q$ and $2 \cdot 2^q$ can be rewritten as $-2 \cdot 2^q = -2 \cdot 32 \cdot \bigotimes_1 = 32 \cdot (-2) \cdot \bigotimes_1$ and $2 \cdot 2^q = 2 \cdot 32 \cdot \bigotimes_1 = 32 \cdot 2 \cdot \bigotimes_1$ respectively. On that account, reducing two equations 7) and 8) by 32 yields that 7)$0, 4, 16 \equiv N^2 \equiv 8M^4 + 2e^4 \equiv 8 + 2 = 10(\text{mod } 32)$ and 8)$0, 4, 16 \equiv 24M^4 - 2e^4 \equiv 24M^4 + 30e^4 \equiv 24 + 30 = 54 \equiv 22(\text{mod } 32)$. Since both LHS and RHS are unmatched in these results, there happens a contradiction in each case. On this account, there cannot exist a solution in these two equations.

For this reason, we meet that $\#\overline{\alpha}(\overline{\Gamma}) = 2$.

In conclusion, if $p = 3$ then, the result $2^r = \frac{2 \cdot 2}{4} = 1$ is given and so we face that $rank(E_{4(2^q-1)}(Q)) = 0$.

And if a prime p is $p = 2^q - 1 > 3$ where an odd prime q as $q = 4t + 1$ with integer $t(t \geq 1)$ then, there comes that $2^r = \frac{4 \cdot 2}{4} = 2$ and so we conclude that $rank(E_{4(2^q-1)}(Q)) = 1$.

(3). Assume that E_{8p} is an elliptic curve $y^2 = x^3 + 8px$ where p is a Mersenne prime $p = 2^q - 1$ such that an odd prime q as $q = 4t + 1$ with integer $t(t \geq 1)$. As we did in 2.1(1), it is clear that $\#\alpha(\Gamma) = 2$.(In 2.1(1), $\#\overline{\alpha}(\overline{\Gamma}) = 2$ was induced in E_{-2p}. The curve E_{8p} treated here is $\overline{E_{-2p}}$ in 2.1(1) and thus the value $\#\overline{\alpha}(\overline{\Gamma})$ is $\#\alpha(\Gamma)$ in here.)

Next from E_{8p}, the curve $\overline{E_{8p}}$ is gotten as $y^2 = x^3 - 32(2^q - 1)x$. Then, there are 12 relating equations for $\overline{\Gamma}$ as follows:

$$1)N^2 = M^4 - 32(2^q - 1)e^4,\ 2)N^2 = -M^4 + 32(2^q - 1)e^4,$$

$$3)N^2 = 2M^4 - 16(2^q - 1)e^4,\ 4)N^2 = -2M^4 + 16(2^q - 1)e^4,$$

$$5)N^2 = 4M^4 - 8(2^q - 1)e^4,\ 6)N^2 = -4M^4 + 8(2^q - 1)e^4,$$

$$7)N^2 = 8M^4 - 4(2^q - 1)e^4,\ 8)N^2 = -8M^4 + 4(2^q - 1)e^4,$$

$$9)N^2 = 16M^4 - 2(2^q - 1)e^4,\ 10)N^2 = -16M^4 + 2(2^q - 1)e^4,$$

$$11)N^2 = 32M^4 - (2^q - 1)e^4,\ 12)N^2 = -32M^4 + (2^q - 1)e^4.$$

The values $\overline{\alpha}(P)$ in relating equation 1) are $\overline{\alpha}(P) = 1, -32(2^q - 1) \equiv 1, -2(2^q - 1) (\mathrm{mod}\ Q^{\times 2})$ but in section 1 it were defined already, thus we can omit to check the solvability of 1) here.

If we use 4 in reducing relating equations from 2) to 4) then, we are confronted with $2)1 \equiv N^2 \equiv -M^4 \equiv 3M^4 \equiv 3 (\mathrm{mod}\ 4)$ and $3), 4)0 \equiv N^2 \equiv 2M^4 \equiv 2 (\mathrm{mod}\ 4)$ respectively. Two sides are unmatched in these numerations and so there cannot exist a solution in these three equations.

Reducing four relating equations from 5) to 8) by 32 leads to $5)0, 4, 16 \equiv N^2 \equiv 4M^4 + 8e^4 (\mathrm{mod}\ 32)$, $6)0, 4, 16 \equiv N^2 \equiv -4M^4 - 8e^4 \equiv 28M^4 + 24e^4 (\mathrm{mod}\ 32)$, $7)0, 4, 16 \equiv N^2 \equiv 8M^4 + 4e^4 (\mathrm{mod}\ 32)$, $8)0, 4, 16 \equiv N^2 \equiv -8M^4 - 4e^4 \equiv 24M^4 + 28e^4 (\mathrm{mod}\ 32)$ respectively. We must consider about these congruences. From assumption $q = 4t + 1$(q is an odd prime and t is an integer with $t \geq 1$), we know that $q \geq 5$ and hence we gain the fact that $2^q \geq 32$. Therefore, the number 2^q is expressed as $2^q = 32 \cdot \bigotimes_2$ with integer $\bigotimes_2$ and so the numbers $-8 \cdot 2^q$ and $8 \cdot 2^q$ and $-4 \cdot 2^q$ and $4 \cdot 2^q$ can be expressed as $-8 \cdot 2^q = -8 \cdot 32 \cdot \bigotimes_2 = 32 \cdot (-8) \cdot \bigotimes_2$ and $8 \cdot 2^q = 8 \cdot 32 \cdot \bigotimes_2 = 32 \cdot 8 \cdot \bigotimes_2$ and $-4 \cdot 2^q = -4 \cdot 32 \cdot \bigotimes_2 = 32 \cdot (-4) \cdot \bigotimes_2$ and $4 \cdot 2^q = 4 \cdot 32 \cdot \bigotimes_2 = 32 \cdot 4 \cdot \bigotimes_2$ respectively. Thus, in process of calculation of reduction by 32 in relating equations 5) and 6) and 7) and 8), four numbers $-8 \cdot 2^q$ and $8 \cdot 2^q$ and $-4 \cdot 2^q$ and $4 \cdot 2^q$ are canceled. Now, the remanent arithmetical values are $5)4M^4 + 8e^4 (\mathrm{mod}\ 32)$, $6)28M^4 + 24e^4 (\mathrm{mod}\ 32)$, $7)8M^4 + 4e^4 (\mathrm{mod}\ 32)$, $8)24M^4 + 28e^4 (\mathrm{mod}\ 32)$ respectively. If we do more calculation then, we acquire the relations $5)4M^4 + 8e^4 \equiv 4 + 8 = 12 (\mathrm{mod}\ 32)$ and $6)28M^4 + 24e^4 \equiv 28 + 24 = 52 \equiv 20 (\mathrm{mod}\ 32)$ and $7)8M^4 + 4e^4 \equiv 8 + 4 = 12 (\mathrm{mod}\ 32)$ and $8)24M^4 + 28e^4 \equiv 52 \equiv 20 (\mathrm{mod}\ 32)$ respectively. Two sides do not match in each case and hence no solution exists in relating equations from 5) to 8).

Using 4 in reducing relating equation 9) then, we obtain that $0 \equiv N^2 \equiv -2 \cdot (-1)e^4 \equiv 2e^4 \equiv 2 (\mathrm{mod}\ 4)$ this is because $-2 \cdot 2^q$ is eliminated in the process of calculation by reduction of 4 as a similar reason to above equations from 5) to 8). Since two sides are unmatched in the above, taking a solution is impossible in 9).

Reducing 10) and 12) by prime p shows that $10)N^2 \equiv -16M^4 (\mathrm{mod}\ p)$ and $12)N^2 \equiv -32M^4 (\mathrm{mod}\ p)$ respectively, but at the same time we attain that $10)(\frac{-16M^4}{p}) = -1$, $12)(\frac{-32M^4}{p}) = -1$. For that reason, there induced a contradiction in two cases and thus above two relating equations cannot have a solution.

Finally, equation 11) is $N^2 = 2^5M^4-(2^q-1)e^4 = 2^5M^4-(2^{4t+1}-1)e^4$ from assumption and thus replacing 2^{t-1} and 1 into M and e respectively yields that $2^5 \cdot (2^{t-1})^4 - (2^{4t+1}-1) = 1$. Hence, $(2^{t-1}, 1, 1)$ is a solution of equation 11).

Eventually, we obtain that $\#\overline{\alpha}(\overline{\Gamma}) = 4$ and so we gain $2^r = \frac{2\cdot 4}{4} = 2$.

Therefore, the conclusion $rank(E_{8(2^q-1)}(Q)) = 1$ is given. □

3 Examples

The examples of Mersenne primes $p = 2^q - 1$ in theorem 2.1(1), (2)($p > 3$), (3) are as follows(We can check the primality in Tables 2.1 of chapter 2 in [5] and [8]):

2^5-1, $2^{13}-1$, $2^{17}-1$, $2^{61}-1$, $2^{89}-1$, $2^{521}-1$, $2^{2281}-1$, $2^{3217}-1$,

$2^{4253}-1$, $2^{9689}-1$, $2^{9941}-1$, $2^{11213}-1$, $2^{19937}-1$, $2^{21701}-1$, $2^{23209}-1$,

$2^{44497}-1$, $2^{132049}-1$, $2^{859433}-1$, $2^{1398269}-1$, $2^{2976221}-1$, $2^{3021377}-1$,

$2^{6972593}-1$, $2^{13466917}-1$, $2^{30402457}-1$, $2^{32582657}-1$, $2^{42643801}-1$,

$2^{43112609}-1$, $2^{57885161}-1$, $2^{74207281}-1$.

References

[1] A. J. Hollier, B. K. Spearman, Q. Yang, Elliptic curves $y^2 = x^3 + pqx$ with maximal rank, *Int. Math. Forum,* **5** (2010), 1105-1110.

[2] F. A. Izadi, F. Khoshnam and K. Nabardi, Sums of two biquadrates and elliptic curves of rank ≥ 4, *Math. J. Okayama Univ.,* **56** (2014), 51-63.

[3] S. W. Kim, Considering in rank of $y^2 = x^3 \pm 4px$, *Far East J. Math. Sci. (FJMS),* **96** (2015), 899-911.
https://doi.org/10.17654/fjmsapr2015_899_911

[4] T. Kudo and K. Motose, On group structures of some special elliptic curves, *Math J. Okayama Univ.,* **47** (2005), 81-84.

[5] F. Lemmermeyer, *Reciprocity Laws*, Springer, 2000.
https://doi.org/10.1007/978-3-662-12893-0

[6] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer New York, 1992. http://dx.doi.org/10.1007/978-1-4757-4252-7

[7] P. G. Walsh, Maximal ranks and integer points on a family of elliptic curves II, *Rocky Mountain J. of Math.,* **41** (2011), 311-317. https://doi.org/10.1216/rmj-2011-41-1-311

[8] http://www.mersenne.org/primes/

Received: December 23, 2017; Published: January 15, 2018