International Journal of Algebra, Vol. 20, 2026, no. 2, 61 - 69
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2026.92007

Rank in Elliptic Curve $y^2 = x^3 - pqsx$

Shin-Wook Kim

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

Abstract

Set E_{-pqs} as an elliptic curve $y^2 = x^3 - pqsx$ with different odd primes p and q and s then, we regard rank of this curve.

Mathematics Subject Classification: 11A41, 14H52

Keywords: Different odd primes, elliptic curve

1 Introduction

In [5], the author investigated that ranks of curves $y^2 = x^3 + 2pqx$ where different odd primes p and q and in [6] the rank of curve $y^2 = x^3 + pqx$ with distinct odd primes p and q is treated. In this article, we approach to rank of elliptic curve $y^2 = x^3 - pqsx$ with different odd primes p and q and s.

We assume that both E and $\bar{E}$ are elliptic curves $y^2 = x^3 + ax^2 + bx$ and $y^2 = x(x^2 - 2ax + a^2 - 4b)$ and take Γ and $\bar{\Gamma}$ are the sets of rational points on E and $\bar{E}$. Define $Q^\times$ as the set of non-zero rational numbers and $Q^{\times 2}$ as the subgroup of squares of elements of $Q^\times$. Denote homomorphism α and relating equation $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ for Γ be in section 5 of chapter III in [7]. Suppose that homomorphism $\bar{\alpha}$ and relating equation $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ for $\bar{\Gamma}$ are in [3]. We appoint that (M, e, N) is a solution of both above equations in in section 5 of chapter III in [7] and [3].

Next, there derived that $2^r = \frac{\#\alpha(\Gamma)\#\bar{\alpha}(\Gamma)}{4}$ with rank r of E.

2 In E_{-pqs}

In section 2, we access to rank of curve $y^2 = x^3 - pqsx$. The solvability of 1) for Γ and 1), 3) for $\bar{\Gamma}$ will not be mentioned. See [3] for it. The notations $w.i.h.i.j.k.l.1$ denotes that with integers h and i and j and k and l and $(h, i, j, k, l) = 1$ and $w.i.t.u.1$ is in [5] and LSV is in [2].

Theorem 2.1. If E_{-pqs}: $y^2 = x^3 - pqsx$ is defined as an elliptic curve with different odd primes p and q and s are $p \equiv 5(mod\ 16)$ and $q \equiv 5(mod\ 16)$ and $s \equiv 5(mod\ 16)$ and E_{-19p}: $y^2 = x^3 - 19px$ is appointed the curve where prime is such that $p = 19h^4 + 361i^2 + j^2 + k^2 + l^2 + 38ij + 38ik + 38il + 2jk + 2jl + 2kl\ w.i.h.i.j.k.l.1$ and $p \equiv 7(mod\ 16)$ and E_{-19p}': $y^2 = x^3 - 19px$ is assumed as the curve where prime is the form $p = 1539h^4 + i^2 + j^2 + k^2 + l^2 - 2ij + 2ik + 2il - 2jk - 2jl + 2kl\ w.i.h.i.j.k.l.1$ and $p \equiv 7(mod\ 16)$ and E_{7p}: $y^2 = x^3 + 7px$ is defined as an elliptic curve with prime as $p = 27t^4 - 4t^3u + 8tu^3 - 4u^4\ w.i.t.u.1$ and $p \equiv 3(mod\ 16)$ then, we conclude that

$$rank(E_{-(16k+5)(16k'+5)(16k''+5)}(Q)$$

$$\leq rank(E_{-19(9h^4+361i^2+\cdots\cdots+2kl)}(Q)) + rank(E_{-19(1539h^4+i^2+\cdots\cdots+2kl)}'(Q))$$

$$+rank(E_{7(27t^4-4t^3u+8tu^3-4u^4)}(Q)) + 2$$

where $rank(E_{-(16k+5)(16k'+5)(16k''+5)}(Q))$ denotes rank of E_{-pqs}.

Proof. Define primes p and q and q as $p = 16k + 5$ and $q = 16k' + 5$ and $s = 16k'' + 5$ with integers k, k', k'' then, it comes several elating equations for Γ as follows:

$$1)N^2 = M^4 - (16k + 5)(16k' + 5)(16k'' + 5)e^4,$$

$$2)N^2 = -M^4 + (16k + 5)(16k' + 5)(16k'' + 5)e^4,$$

$$3)N^2 = (16k + 5)M^4 - (16k' + 5)(16k'' + 5)e^4,$$

$$4)N^2 = -(16k + 5)M^4 + (16k + 5)(16k'' + 5)e^4,$$

$$5)N^2 = (16k' + 5)M^4 - (16k + 5)(16k'' + 5)e^4,$$

$$6)N^2 = -(16k' + 5)M^4 + (16k + 5)(16k'' + 5)e^4,$$

$$7)N^2 = (16k'' + 5)M^4 - (16k + 5)(16k' + 5)e^4,$$

$$8) N^2 = -(16k'' + 5)M^4 + (16k + 5)(16k' + 5)e^4.$$

Reducing 2) by 16 implies that $0, 1, 4, 9 \equiv N^2 \equiv 15M^4 + 13e^4 \equiv 15, 13, 12(mod\ 16)$ and the sides are unmatched, thus there cannot be induced a solution in this equation.

In modulo 16 in 3), 5), 7) shows that $0, 1, 4, 9 \equiv N^2 \equiv 5M^4 + 7e^4 \equiv 5, 7, 12(mod\ 16)$. Thus, neither has a solution.

Next, cutting down on 4), 6), 8) by 16 then, we are confronted with $0, 1, 4, 9 \equiv N^2 \equiv 11M^4 + 9e^4(mod\ 16)$. Let $M = 2F + 1$, $e = 2G + 1$ with integers F and G then, there induced that $11M^4 + 9e^4 = 11(2F + 1)^4 + 9(2G + 1)^4 \equiv 4(mod\ 16)$. Hence, it can have a solution. Besides, we apply LSV([2]) to 4). If there exists a solution in 4) then, we are confronted with $N^2 \equiv -(16k + 5)M^4(mod\ q)$ and $N^2 \equiv -(16k + 5)M^4(mod\ s)$ and $N^2 \equiv (16k' + 5)(16k'' + 5)e^4(mod\ p)$ from cutting down on it by primes q, s, p. Thereby, we ought to have that $1 = \left(\frac{-(16k+5)M^4}{q}\right) = \left(\frac{p}{q}\right) \cdots (AA)$ and $1 = \left(\frac{-(16k+5)M^4}{s}\right) = \left(\frac{p}{s}\right) \cdots (BB)$ and $1 = \left(\frac{(16k'+5)(16k''+5)e^4}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{s}{p}\right) \cdots (CC)$. Between the primes p, q and p, s and q, s we gain the relation LSV and thus there should be given that $\left(\frac{q}{p}\right)\left(\frac{s}{p}\right) = 1 \cdot 1 = 1$ from (AA), (BB) and so (CC) became 1. Accordingly, a solution can be educed in equation 4), 6), 8).

Consequently, we obtain that $\#\alpha(\Gamma) \leq 16$.

Now from E_{-pqs} in the above the curve $\overline{E_{-pqs}}$ is given as $y^2 = x^3 + 4(16k + 5)(16k' + 5)(16k'' + 5)x$.

And we have relating equations for $\bar{\Gamma}$ as $1) N^2 = M^4 + 4(16k + 5)(16k' + 5)(16k'' + 5)e^4$ and $2) N^2 = 2M^4 + 2(16k + 5)(16k' + 5)(16k'' + 5)e^4$ and $3) N^2 = 4M^4 + (16k + 5)(16k' + 5)(16k'' + 5)e^4$ and $4) N^2 = (16k + 5)M^4 + 4(16k' + 5)(16k'' + 5)e^4$ and $5) N^2 = 2(16k + 5)M^4 + 2(16k' + 5)(16k'' + 5)e^4$ and $6) N^2 = 4(16k + 5)M^4 + (16k' + 5)(16k'' + 5)e^4$ and $7) N^2 = (16k' + 5)M^4 + 4(16k + 5)(16k'' + 5)e^4$ and $8) N^2 = 2(16k' + 5)M^4 + 2(16k + 5)(16k'' + 5)e^4$ and $9) N^2 = 4(16k' + 5)M^4 + (16k + 5)(16k'' + 5)e^4$ and $10) N^2 = (16k'' + 5)M^4 + 4(16k + 5)(16k' + 5)e^4$ and $11) N^2 = 2(16k'' + 5)M^4 + 2(16k + 5)(16k' + 5)e^4$ and $12) N^2 = 4(16k'' + 5)M^4 + (16k + 5)(16k' + 5)e^4$.

We cannot find a solution in 2) because from modulo s in it there comes that $N^2 \equiv 2M^4(mod\ s)$ but we also take $\left(\frac{2M^4}{s}\right) = -1$ and hence a contradiction is deduced.

In modulo 16 in 4), 7), 10) deduces that $1, 9 \equiv N^2 \equiv 5 + 4e^4(mod\ 16)$. Take e as $e = 2L + 1$ with integer L then, we gain the relation as $5 + 4e^4 = 5 + 4(2L + 1)^4 \equiv 9(mod\ 16)$. Accordingly, we can expect an appearance of solution. And we apply LSV ([2]) to this equation. If there exists a solution in equation 4) then, it comes that $N^2 \equiv (16k + 5)M^4(mod\ q)$ and $N^2 \equiv (16k + 5)M^4(mod\ s)$ and $N^2 \equiv 4(16k' + 5)(16k'' + 11)e^4(mod\ p)$ in modulo q and s and p respec-

tively. Therefore, it should be given that $1 = \left(\frac{(16k+5)M^4}{q}\right) = \left(\frac{p}{q}\right) \cdots (AA)$ and $1 = \left(\frac{(16k+5)M^4}{s}\right) = \left(\frac{p}{s}\right) \cdots (BB)$ and $1 = \left(\frac{4(16k'+5)(16k''+5)e^4}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{s}{p}\right) \cdots (CC)$. Between the primes p, q and p, s and q, s we obtain the relation LSV and thus it must be induced that $\left(\frac{q}{p}\right)\left(\frac{s}{p}\right) = 1 \cdot 1 = 1$ from (AA), (BB) and thus (CC) is induced as 1. Wherefore, a solution can be derived in equation 4), 7), 10).

Cutting down on 5), 8), 11) by 32 yields that $0, 4, 16 \equiv N^2 \equiv 10M^4 + 18e^4 = 2 \equiv 28(mod\ 32)$ and two sides are unmatched.

From modulo 16 in 6), 9), 12) we get that $1, 9 \equiv N^2 \equiv 4M^4 + 9(mod\ 16)$. Take M as $M = 2L$ with integer L then, we gain the relation as $4M^4 + 9 \equiv 9(mod\ 16)$. Accordingly, we can expect an appearance of solution. And we apply LSV ([2]) to this equation. If there exists a solution in equation 6) then, it comes that $N^2 \equiv 4(16k+5)M^4(mod\ q)$ and $N^2 \equiv 4(16k+5)M^4(mod\ s)$ and $N^2 \equiv (16k'+5)(16k''+5)e^4(mod\ p)$ in modulo q and s and p respectively. Therefore, it should be given that $1 = \left(\frac{4(16k+5)M^4}{q}\right) = \left(\frac{p}{q}\right) \cdots (AA)$ and $1 = \left(\frac{4(16k+5)M^4}{s}\right) = \left(\frac{p}{s}\right) \cdots (BB)$ and $1 = \left(\frac{(16k'+5)(16k''+5)e^4}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{s}{p}\right) \cdots (CC)$. Between the primes p, q and p, s and q, s there derived that LSV and thus it must be induced that $\left(\frac{q}{p}\right)\left(\frac{s}{p}\right) = 1 \cdot 1 = 1$ from (AA), (BB) and thus (CC) is induced as 1. Wherefore, a solution can be derived in equation 6), 9), 12).

In sum, we got relating equations that can take a solution are given as follows:

$$4) N^2 = (16k+5)M^4 + 4(16k'+5)(16k''+5)e^4 \text{ and}$$

$$6) N^2 = 4(16k+5)M^4 + (16k'+5)(16k''+5)e^4 \text{ and}$$

$$7) N^2 = (16k'+5)M^4 + 4(16k+5)(16k''+5)e^4 \text{ and}$$

$$9) N^2 = 4(16k'+5)M^4 + (16k+5)(16k''+5)e^4 \text{ and}$$

$$10) N^2 = (16k''+5)M^4 + 4(16k+5)(16k'+5)e^4 \text{ and}$$

$$12) N^2 = 4(16k''+5)M^4 + (16k+5)(16k'+5)e^4.$$

Consequentially, we are faced with $\#\bar{\alpha}(\bar{\Gamma}) \leq 8$.

On that account, we gain $2^r \leq \frac{16 \cdot 8}{4} = 32$.

For that reason, it shows that

$$rank(E_{-(16k+5)(16k'+5)(16k''+5)}(Q)) \leq 5 \cdots \cdots (1).$$

Next, we research the rank of curve E_{-19p}.

Put prime p as $p = 16k + 7$ with integer k then, following relating equations for Γ are given:

$1)N^2 = M^4 - 19(16k + 7)e^4$
$2)N^2 = -M^4 + 19(16k + 7)e^4$
$3)N^2 = 19M^4 - (16k + 7)e^4$
$4)N^2 = -19M^4 + (16k + 7)e^4$

In modulo p in 2) implies that $N^2 \equiv -M^4 (mod\ p)$ but there induced that $\left(\frac{-M^4}{p}\right) = -1$, thus a contradiction is given.

Next, equation 4) is

$$4)N^2 = -19M^4 + (19h^4 + 361i^2 + j^2 + k^2 + l^2 + 38ij + 38ik + 38il + 2jk$$

$$+2jl + 2kl)e^4 \text{ for } \Gamma.$$

Substitute h and 1 into both M and e then, there derived that

$$-19h^4 + 19h^4 + 361i^2 + j^2 + k^2 + l^2 + 38ij + 38ik + 38il + 2jk$$

$$+2jl + 2kl$$

$$= 361i^2 + j^2 + k^2 + l^2 + 38ij + 38ik + 38il + 2jk$$

$$+2jl + 2kl.$$

Whence, we took solution as $(h, 1, 19i + j + k + l)$.

Now we assign equation 3) takes a solution then, we acquire that $19 \cdot (-19) \equiv -1 \in \alpha(\Gamma)(mod\ Q^{\times 2})$ but it is impossible that equation $2)N^2 = -M^4 + 19(16k + 7)e^4$ has a solution, thus a contradiction is gotten.

As a result, it is deduced the conclusion #α(Γ) = 4.

Now $\overline{E_{-19p}}$ is given as $y^2 = x^3 + 76(16k + 7)x$.

Whence, we attain relating equations for $\bar{\Gamma}$:

$1)N^2 = M^4 + 76(16k + 7)e^4$

$2)N^2 = 2M^4 + 38(16k + 7)e^4$

$3)N^2 = 4M^4 + 19(16k + 7)e^4$

$4)N^2 = 19M^4 + 4(16k + 7)e^4$

$5)N^2 = 38M^4 + 2(16k + 7)e^4$

$$\boxed{6)N^2 = 76M^4 + (16k + 7)e^4}$$

In modulo 16 in equation 2) gives that $0, 4 \equiv N^2 \equiv 2M^4 + 42e^4 \equiv 12(mod\ 16)$.
Reducing equation 4) by 8 implies that $1 \equiv N^2 \equiv 3M^4 + 4e^4 \equiv 3, 7(mod\ 8)$.
We obtain that $5)0, 4, 16 \equiv N^2 \equiv 6M^4 + 14e^4 \equiv 20(mod\ 32)$ and $6)1 \equiv N^2 \equiv 3(mod\ 4)$ after reducing 5) and 6) by 32 and 4.
Thereby, we gain the conclusion $\#\bar{\alpha}(\bar{\Gamma}) = 2$.
To conclude, we acquire the result as

$$rank(E_{-19(9h^4+361i^2+\cdots\cdots+2kl)}(Q)) = 1 \cdots \cdots (2\ ).$$

In the next step, from the above E_{-19p} it is sufficient that we find the solution of equation

$$4)N^2 = -19M^4 + (1539h^4 + i^2 + j^2 + k^2 + l^2 - 2ij + 2ik + 2il - 2jk - 2jl$$

$$+2kl)e^4 \text{ for } \Gamma.$$

In coefficient of e^4 there are squares i^2 and j^2 and k^2 and l^2.
There are non-square terms $-2ij$ and $2ik$ and $2il$ and $-2jk$ and $-2jl$ and $2kl$.
Therefore, if we chose $i - j + k + l$ then, squaring of it induces

$$i^2 + j^2 + k^2 + l^2 - 2ij + 2ik + 2il - 2jk - 2jl\ + 2kl.$$

Henceforth, if the term $1539h^4$ is crossed out then, we obtain our objective.
Now we observe that

$$-19M^4 + 1539h^4e^4.$$

Set e as 1 then, our aim is $-19M^4 + 1539h^4 = 0$.
Whence, it must be given that

$$19M^4 = 1539h^4.$$

On this account, we gain $M^4 = 81h^4$.
Thereby, we attain that $M = 3h$.
We obtained our aim.
Accordingly, the solution is deduced as

$$(3h, 1, i - j + k + l).$$

Thus, it follows that $\#\alpha(\Gamma) = 4$.
Accordingly, we acquire that

$$rank(E_{-19(1539h^4+i^2+\cdots\cdots+2kl)}{}'(Q)) = 1 \cdots\cdots (3\,).$$

From [4] if we find the solution of

$$11)N^2 = 28M^4 - (27t^4 - 4t^3u + 8tu^3 - 4u^4)e^4 \text{ for } \Gamma \text{ then,}$$

treating the rank of curve is completed.

It is rewritten as

$$N^2 = 28M^4 + (-27t^4 + 4t^3u - 8tu^3 + 4u^4)e^4.$$

The existence of square in coefficient of e^4 makes it possible to inducement of square in resultant.

In arithmetical value $28M^4 - 27t^4e^4$ we take $e = 1$.

In considering the terms $4t^3u$ and $-8tu^3$ we pursue the relation

$$28M^4 - 27t^4 = t^4$$

holds.

Thus, the value $M = t$ is gotten.

Now we are confronted with

$$t^4 + 4t^3u - 8tu^3 + 4u^4.$$

It can be written as

$$t^4 + 4t^2u^2 + 4u^4 + 4t^3u - 8tu^3 - 4t^2u^2.$$

This is square of $t^2 + 2tu - 2u^2$.

Accordingly, the solution is given as

$$(t, 1, t^2 + 2tu - 2u^2).$$

Hence, we get that $\#\bar{\alpha}(\bar{\Gamma}) = 4$.

On that account, we say that

$$rank(E_{7(27t^4-4t^3u+8tu^3-4u^4)}(Q)) = 1 \cdots\cdots (4\,).$$

Thus, from (1) and (2) and (3) and (4) we accomplished the proof. □

In curve E_{-19p}: $y^2 = x^3 - 19px$ primes are gotten as $p = 19h^4 + 361i^2 + j^2 + k^2 + l^2 + 38ij + 38ik + 38il + 2jk + 2jl + 2kl$ and $p = 1539h^4 + i^2 + j^2 + k^2 + l^2 - 2ij + 2ik + 2il - 2jk - 2jl + 2kl$. These are not the form $p =$

$Hu^4 + Iu^2v^2 + Kv^4 \cdots\cdots (5)$. When, generalized rank is given as 1 in curve $y^2 = x^3 \pm Apx$ then, prime is usually given as $p = Hu^4 + Iu^2v^2 + Kv^4$. But we also can get rank 1 where prime is other forms$(\neq (5))$.

Remark 2.2. In above curve E_{-pqs}: $y^2 = x^3 - pqsx$ the rank r is induced as $r \leq 5$. The only condition is $p \equiv 5(mod\ 16)$ and $q \equiv 5(mod\ 16)$ and $s \equiv 5(mod\ 16)$. There is a probability that if some other condition is added then, range of rank can be decreased.

3 Example

In section 3, we consider some examples. Primality was done by in [1].
For curve E_{-pqs} finding the examples is not simple treatment.
Here, we treat examples of E_{-19p} and E_{7p}.
Examples are induced as follows:

(p, h, i, j, k, l): (503, 1, 1, 1, 1, 1), (46103, 7, 1, 1, 1, 1).

(p, h, i, j, k, l): (1543, 1, 1, 1, 1, 1), (961879, 5, 1, 1, 1, 1).

(p, t, u): (62467, 7, 5), (171827, 9, 7).

References

[1] C. Caldwell, http://primes.utm.edu/curios/includes/primetest.php.

[2] S. W. Kim, Different odd primes in curve $y^2 = x^3 - pqx$, *Far East J. Math. Sci. (FJMS),* **107** (2018), 155-165. https://doi.org/10.17654/ms107010155

[3] S. W. Kim, Various forms in components of primes, *Int. J. of Algebra,* **13** (2019), 59-72. https://doi.org/10.12988/ija.2019.913

[4] S. W. Kim, Ranks in some elliptic curves $y^2 = x^3 \pm Apx$, *JP J. of Algebra, Number Theory and Applications,* **51** (2021), 223-248. https://doi.org/10.17654/nt051020223

[5] S. W. Kim, Ranks in elliptic curves of the forms $y^2 = x^3 + Ax^2 + Bx$, *Int. J. of Algebra,* **16** (2022), 109-218. https://doi.org/10.12988/ija.2022.91726

[6] S. W. Kim, Calculation of rank in elliptic curve $y^2 = x^3 + pqx$, *Int. J. of Algebra,* **19** (2025), 69-77. https://doi.org/10.12988/ija.2025.91957

[7] J. H. Silverman and J. Tate, *Rational points on elliptic curves,* Springer, New York, (1992). https://doi.org/10.1007/978-1-4757-4252-7

Received: January 1, 2026; Published: January 31, 2026