International Journal of Algebra, Vol. 20, 2026, no. 2, 51 - 59
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2026.92006

Results in Ranks of Elliptic Equations

$y^2 = x^3 - Ax$

Shin-Wook Kim

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

This article is distributed under the Creative Commons by-nc-nd Attribution License.
Copyright © 2026 Hikari Ltd.

Abstract

Take $E_{-p(p-2)}$ as an elliptic curve $y^2 = x^3 - p(p-2)x$ with twin primes p and $p-2$ then, we shall investigate the rank of it. Denote E_{-2p} and E_{-4p} as elliptic curves $y^2 = x^3 - 2px$ and $y^2 = x^3 - 4px$ then, we will research the ranks and compare the results with previous curve.

Mathematics Subject Classification: 11A41, 14G05

Keywords: Twin primes, elliptic curves

1 Introduction

If prime p is given as the form $p = As^4 + Bt^4 + Cu^4 + Ds^2t^2 + Fs^2u^2 + Gt^2u^2 \cdots\cdots (X)$ then, there derived much results of generalized rank 1 in $E_{-2p}: y^2 = x^3 - 2px$. In curve $E_{-4p}: y^2 = x^3 - 4px$ there deduced generalized rank 1 when p is $p = At^4 + Bt^3u + Ctu^3 + Dt^2u^2 + Fu^4 \cdots\cdots (Z)$ often. The forms (X) and (Z) are not usual forms in E_{-2p} and E_{-4p}. These forms make extension of generalized ranks 1 in E_{-2p} and E_{-4p}. Main form in E_{-2p} that induces rank 1 is $p = Hu^4 + Iu^2v^2 + Kv^4 \cdots\cdots (S)$. In E_{-2p} there are various forms of $p(\neq (X), (Z))$ which yields rank 1. The number of terms in (X) is 6 and there are three variables. But there exists prime p with 14 variables and 105 terms

in E_{-2p} with rank 1([9]). All primes p are the comprised of terms for squares. Meanwhile in curve E_{-4p}, (Z) is as little different from (X). There are non-square terms Bt^3u and Ctu^3. This difference in components of p is correlated to relating equations. Anyway, (X) and (Z) are appeared (except $p = Hu^4 + Iu^2v^2 + Kv^4$) in E_{-2p} and E_{-4p} respectively. In this article, we shall research the ranks of $y^2 = x^3 - 2px$ and $y^2 = x^3 - 4px$ where p is (X) and (Z). First, we calculate the rank of $E_{-p(p-2)}$: $y^2 = x^3 - p(p-2)x$.

It is necessary to treat notations in [6], [10].

We appoint that E is an elliptic curve $y^2 = x^3 + ax^2 + bx$ and Γ is the set of rational points on E.

Then, the set Γ is a finitely generated abelian group.

There comes the structure $\Gamma \cong E(Q)_{tors} \oplus Z^r$ with torsion subgroup $E(Q)_{tors}$ and $Mordell's - Weil$ rank r .

Take $Q^\times$ as the set of non-zero rational numbers then, this is a multiplicative group. Assign $Q^{\times 2}$ as the subgroup of squares of elements of $Q^\times$.

Let α and $\bar{\alpha}$ be a homomorphism in [10] and [6].

Denote $\bar{E}$ as the curve $y^2 = x(x^2 - 2ax + a^2 - 4b)$ and $\bar{\Gamma}$ as the set of rational points on $\bar{E}$.

Take α as a homomorphism in section 5 of chapter III in [10] and $\bar{\alpha}$ in homomorphism in [6].

Assign $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ as relating equation for Γ which satisfies conditions in section 6 of chapter III in [10].

Put $\bar{E}$ as the curve $y^2 = x(x^2 - 2ax + a^2 - 4b)$ and $\bar{\Gamma}$ as the set of rational points on $\bar{E}$.

We assume that $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ is relating equation for $\bar{\Gamma}$ that satisfies the conditions in [6].

Let (M, e, N) be a solution of above equations in [10], [6] respectively.

We have that $2^r = \frac{\#\alpha(\Gamma)\#\bar{\alpha}(\Gamma)}{4}$ where r is rank of E.

Take the notations as follows:

$r4.2$: $2^r = \frac{4\cdot 2}{4} = 2$([7]).

$w.i.s.t.u.1$: with integers s and t and u and

$(s, t, u) = 1$([8]).

$w.i.t.u.1$: with integers t and u and $(t, u) = 1$.

2 In Equation $E_{-p(p-2)}$

Primes (X) in equation E_{-2p} has 6 terms in it. Usually, this number is not large but in computation of rank in E_{-2p}, it is not small number. There deduced prime p

that has 3 terms often in E_{-2p} with rank 1, thus compared with it the number of terms 6 is not small. In equation E_{-4p}, 5 terms in (Z) is also not little numbers of terms. Now, we investigate rank of E_{-2p} and E_{-4p} where p is the form as (X) and (Z). We shall omit to say about solvability of relating equation 1) for Γ and equations 1), 5) for $\bar{\Gamma}$. For this, see [6] and the notations LDV, LSV are in [5].

Lemma 2.1. Denote $E_{-p(p-2)}$ as an elliptic equation $y^2 = x^3 - p(p-2)x$ with twin primes p and $p-2$ as $p \equiv 7(mod\ 16)$ then, we gain the result $rank(E_{-p(p-2)}(Q)) = 0$.

Proo$f$. Assign $p = 16k + 7$ with integer k.
Then, we took relating equations for Γ as follows:

$1) N^2 = M^4 - (16k+7)(16k+5)e^4$
$2) N^2 = -M^4 + (16k+7)(16k+5)e^4$
$3) N^2 = (16k+7)M^4 - (16k+5)e^4$
$4) N^2 = -(16k+7)M^4 + (16k+5)e^4$

Cutting down on equation 2) by 16 shows that $0, 1, 4, 9 \equiv N^2 \equiv 15M^4 + 35e^4 \equiv 3, 2, 15(mod\ 16)$, thus a contradiction is derived.
Let equation 3) possess a solution then, we are faced with the congruences $N^2 \equiv (16k+7)M^4(mod\ p-2)$ and $N^2 \equiv -(16k+5)e^4(mod\ p)$ respectively on account of reduction of it by $p-2$ and p respectively. On this account, we ought to reach that

$$1 = \left(\frac{(16k+7)M^4}{p-2}\right) = \left(\frac{p}{p-2}\right) \text{ and}$$

$$1 = \left(\frac{-(16k+5)e^4}{p}\right) = -\left(\frac{p-2}{p}\right).$$

We have LDV in the above and it is unmatched to relation LSV between p and $p-2$. It gives a contradiction.
Relating equation 4) is also the form $N^2 = -pM^4 + (p-2)e^4$ and thus if we reduce this by p then, we arrive at that $N^2 \equiv -2e^4(mod\ p)$ but there comes $\left(\frac{-2e^4}{p}\right) = -1$. Accordingly, this equation cannot take a solution.
Consequently, it yields the conclusion #α(Γ) = 2.
In the next step, $\overline{E_{-pq}}$ is deduced as $y^2 = x^3 + 4(16k+7)(16k+5)x$.
This submits several relating equations for $\bar{\Gamma}$ as follows:

$1) N^2 = M^4 + 4(16k+7)(16k+5)e^4$
$2) N^2 = 2M^4 + 2(16k+7)(16k+5)e^4$
$3) N^2 = 4M^4 + (16k+7)(16k+5)e^4$

$4)N^2 = (16k+7)M^4 + 4(16k+5)e^4$
$5)N^2 = 2(16k+7)M^4 + 2(16k+5)e^4$
$6)N^2 = 4(16k+7)M^4 + (16k+5)e^4$

Reducing equation 2) by $p-2$ educes the relation $N^2 \equiv 2M^4(mod\ p-2)$ and there deduced $\left(\frac{2M^4}{p-2}\right) = -1$.

In modulo 4 in equation 3) induces unmatched congruence $1 \equiv N^2 \equiv 35e^4 \equiv 3(mod\ 4)$.

Cutting down on equations 4) by 4 gives that $1 \equiv N^2 \equiv 7M^4 \equiv 3(mod\ 4)$ and this is unmatched relation.

Let equation 5) have a solution then, we gain $N^2 \equiv 2(16k+7)M^4(mod\ p-2)$ and $N^2 \equiv 2(16k+5)e^4(mod\ p)$ in modulo $p-2$ and p respectively. Thereby, we must obtain next things:

$$1 = \left(\frac{2(16k+7)M^4}{p-2}\right) = -\left(\frac{p}{p-2}\right) \text{ and}$$

$$1 = \left(\frac{2(16k+5)e^4}{p}\right) = \left(\frac{p-2}{p}\right).$$

There educed LDV in the above and this is unmatched to LSV that is relation between p and $p-2$.

Relating equation 6) is also gotten as $6)N^2 = 4pM^4 + (p-2)e^4$. In modulo p implies that $N^2 \equiv -2e^4(mod\ p)$ but we also acquire that $\left(\frac{-2e^4}{p}\right) = -1$.

Consequentially, it is derived that $\#\bar{\alpha}(\bar{\Gamma}) = 2$.

For this reason, there comes that $r2.2$.

Henceforth, $rank(E_{-p(p-2)}(Q)) = 0$ is given. □

In above relating equations $4)N^2 = -pM^4 + (p-2)e^4$, $6)N^2 = 4pM^4 + (p-2)e^4$ for Γ and $\bar{\Gamma}$ are noticeable because it affects to rank 0 severely. Other equations are possible to anticipate the solvability. But these are little different. If there is appointed as $p = 16k+7$, $q = 16k'+5$, namely if there doesn't exist twin relations $p, p-2$ between p and q then, we confront to the congruences $4)0, 1, 4, 9 \equiv N^2 \equiv 9M^4 + 5e^4(mod\ 16)$ and $6)1, 9 \equiv N^2 \equiv 12M^4 + 5e^4(mod\ 16)$ and so there can be deduced solutions in these equations but the correlation $p, p-2$ are given. Therefore, we can attain a contradiction from cutting down on it by p as $4)N^2 \equiv -2e^4(mod\ p)$ and $6)N^2 \equiv -2e^4(mod\ p)$. Since the relation $p, p-2$ eliminates the numerical value pe^4 in the process of numeration in modulo p as a result p and $p-2$ determines the rank in $E_{-p(p-2)}$. Above equation is kind of E_{-pq}. The number of relating equations for $\bar{\Gamma}$ is 6. Meanwhile in form of curve E_{pq}, even though there are two relating equations for Γ but there exist 12 relating equations for $\bar{\Gamma}$. Hence, compared with E_{-pq} it needs more attention. In [2], the

author showed that rank of $y^2 = x^3 - p(p-4)x$ is 2 under the hypothesis $p \equiv 3(mod\ 8)$ and $p - 2 = t^2$ and in $E_{\mp pq}$ there are the result of rank 1. Not rank of 3, 4 but there appeared generalized rank 0, 1, 2.

Remark 2.2 If we mention about equation $5)N^2 = 2pM^4 + 2(p-2)e^4$ for $\bar{\Gamma}$ in the above then, doing modulo 16 in it also submits a contradiction from $0, 4 \equiv N^2 \equiv 14M^4 + 10e^4 \equiv 8(mod\ 16)$. By reduction of 32 its insolvability also can be verified.

3 In Equations E_{-2p} and E_{-4p}

In this section, we will compute rank of elliptic equations E_{-2p} and E_{-4p} where prime p is the form $p = As^4 + Bt^4 + Cu^4 + Ds^2t^2 + Fs^2u^2 + Gt^2u^2$ and $p = At^4 + Bt^3u + Ctu^3 + Dt^2u^2 + Fu^4$.

Theorem 3.1. (1). Suppose that prime p is $p = 1286s^4 + 16t^4 + u^4 - 48s^2t^2 - 12s^2u^2 + 8t^2u^2\ w.i.s.t.u.1$ and $p \equiv 3(mod\ 16)$ in E_{-2p} then, it is derived that

$$rank(E_{-2(1286s^4+16t^4+u^4-48s^2t^2-12s^2u^2+8t^2u^2)}(Q)) > rank(E_{-p(p-2)}(Q)).$$

(2). If prime p is assumed as $p = 328t^4 - 16t^3u - 16tu^3 - 804t^2u^2 + 533u^4$ $w.i.t.u.1$ and $p \equiv 5(mod\ 16)$ in E_{-4p} then, we obtain that

$$rank(E_{-4(328t^4-16t^3u-16tu^3-804t^2u^2+533u^4)}(Q)) > rank(E_{-p(p-2)}(Q)).$$

Proo$f$. (1). There is left relating equation

$4)N^2 = -2M^4 + (1286s^4 + 16t^4 + u^4 - 48s^2t^2 - 12s^2u^2 + 8t^2u^2)e^4$ for Γ

from [3].

In coefficient of e^4 there are squares $16t^4$ and u^4.

It is essential to find square term for s^4.

In arithmetical value $-2M^4 + 1286s^4e^4$ take $e = 1$ then, we gain $-2M^4 + 1286s^4 \cdots\cdots (\neg/)$.

We note to terms $-48s^2t^2$, $-12s^2u^2$, $8t^2u^2$.

Since there are terms $16t^4$ and u^4 the term $8t^2u^2$ can be deduced.

Next, it is given $-48s^2t^2 = -2 \cdot 4 \cdot 6s^2t^2$ and $-12s^2u^2 = -2 \cdot 6s^2u^2$.

Wherefore, it needs to be shown the term $36s^4$ after selecting the value M in $(\neg/)$.

Now we confront to

$$-2M^4 + 1286s^4 = 36s^4.$$

Then, we take that $2M^4 = 1250s^4$.
It yields that $M = 5s$.
Thus, the pair $(e, M) = (1, 5s)$ satisfies the part of solution.
Now from the numeration

$$-2(5s)^4 + 1286s^4 + 16t^4 + u^4 - 48s^2t^2 - 12s^2u^2 + 8t^2u^2$$

$$= -1250s^4 + 1286s^4 + 16t^4 + u^4 - 48s^2t^2 - 12s^2u^2 + 8t^2u^2$$

$$= 36s^4 + 16t^4 + u^4 - 48s^2t^2 - 12s^2u^2 + 8t^2u^2$$

there comes $N = 6s^2 - 4t^2 - u^2$.
Eventually, there derived the solution of above equation as a triple

$$(5s, 1, 6s^2 - 4t^2 - u^2).$$

And hence we acquire the conclusion #α(Γ) = 4 and $r4.2$.
This gives the result

$$rank(E_{-2(1286s^4+16t^4+u^4-48s^2t^2-12s^2u^2+8t^2u^2)}(Q)) = 1.$$

Due to lemma 2.1, the proof is accomplished.
(2). It requires to find the solution of following equation for Γ from [4]:

$$6)N^2 = -4M^4 + (328t^4 - 16t^3u - 16tu^3 - 804t^2u^2 + 533u^4)e^4 .$$

In numerical values

$$-4M^4 + 328t^4e^4 \text{ and } -4M^4 + 533u^4e^4$$

set e as 1 then, we acquire that

$$-4M^4 + 328t^4 \text{ and } -4M^4 + 533u^4.$$

Therefore, in looking for the value M if it possesses variables t and u then, there can be gotten the terms $324t^4$ and $529u^4$.
Now there is given $-16t^3u$ and $-16tu^3$.
If M is assigned as the form $at - bu$ with positive integers a, b then, due to degree 4 of M^4, it is possible that terms for t^3u and tu^3 are deduced.
Let $M = t - u$ and $e = 1$ then, there derived that

$$-16t^3u - 16tu^3 + 16t^3u + 16tu^3.$$

Thus, the terms t^3u and tu^3 are erased.
In the next step, we see that

$$-24t^2u^2 - 804t^2u^2 = -828t^2u^2.$$

From the numeration

$$-4t^4 + 328t^4 = 324t^4 \text{ and } -4u^4 + 533u^4 = 529u^4$$

the terms $324t^4$, $529u^4$, $-828t^2u^2$ are shown.
Hence, we get that

$$324t^4 - 828t^2u^2 + 529u^4.$$

And it follows that

$$N = 18t^2 - 23u^2.$$

For that reason, the triple

$$(t - u, 1, 18t^2 - 23u^2)$$

is derived as the solution of above equation.
Accordingly, next conclusions are given:

$$\#\alpha(\Gamma) = 4 \text{ and } r4.2.$$

Wherefore, we are confronted with following result:

$$rank(E_{-4(328t^4-16t^3u-16tu^3-804t^2u^2+533u^4)}(Q)) = 1.$$

From lemma 2.1, we finish the proof. □

In above prime $p = 1286s^4 + 16t^4 + u^4 - 48s^2t^2 - 12s^2u^2 + 8t^2u^2$ in E_{-2p} the coefficient of s^4 is 1286 and this is not a square term. Thus, in calculation with $-2M^4$ if there comes square coefficient then, it is sufficient. Hence, we only treat the numerical value $-2M^4 + 1286s^4$. Whereas in E_{-4p}, relating equation is gotten as $6)N^2 = -4M^4 + pe^4$. The coefficient of M^4 is -4, whence for taking a square in resultant in computation $-4(at - bu)^4 + Bt^3u + Ctu^3$, there must be eliminated the terms Bt^3u and Ctu^3. This is difference in regarding rank of E_{-2p} and E_{-4p}.

4 Examples

In this section, we shall submit examples of previous calculations. From [1], primality is checked.

The examples from lemma 2.1 are followings:

$(p, p-2)$: (7, 5), (103, 101), (1063, 1061), (1303, 1301),

(1879, 1877), (2311, 2309), (3463, 3461).

Next things are examples of theorems 3.1(1) and (2):

(p, s, t, u): (102931, 3, 1, 3), (103651, 3, 1, 1).

(p, t, u): (70549, 4, 1), (2547253, 10, 3).

References

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

[2] S. W. Kim, Relation of primes in rank of elliptic curve, *Far East J. Math. Sci. (FJMS),* **102** (2017), 995-1006. https://doi.org/10.17654/ms102050995

[3] S. W. Kim, Crucial function of prime's form, *Int. J. of Algebra,* **10** (2016), 283 - 290. https://doi.org/10.12988/ija.2016.6428

[4] S. W. Kim, Ranks of elliptic curves $y^2 = x^3 \pm 4px$, *Int. J. of Algebra,* **9** (2015), 205-211. https://doi.org/10.12988/ija.2015.5421

[5] 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

[6] 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

[7] S. W. Kim, Enumeration in ranks of various elliptic curves $y^2 = x^3 \pm Ax$, *Int. J. of Algebra,* **14** (2020), 139-162. https://doi.org/10.12988/ija.2020.91250

[8] 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

[9] S. W. Kim, Compositions of primes in elliptic curves $y^2 = x^3 - 2px$, *Int. J. of Algebra,* **17** (2023), 105-112. https://doi.org/10.12988/ija.2023.91743

[10] 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