International Journal of Algebra, Vol. 20, 2026, no. 1, 41 - 49
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2026.92005

Comparing Ranks of Elliptic Equations

$y^2 = x^3 \pm Ax$

Shin-Wook Kim

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

Abstract

Assign $E_{p(p-2)}$ as an elliptic curve $y^2 = x^3 + p(p-2)x$ with twin primes then, we shall treat the rank of this curve and if E_{-2p} is gotten as an elliptic curve $y^2 = x^3 - 2px$ then, we will calculate the rank and compare the results with previous curves.

Mathematics Subject Classification: 11A41, 11G05

Keywords: Twin primes, elliptic curve

1 Introduction

In curves $y^2 = x^3 \pm pqx$, generalized(systematized) ranks were gotten in two kinds of forms. First forms are $p = Hu^4 + Iu^2v^2 + Kv^4$ and $q = H'u^4 + I'^{u^2v^2} + K'^{v^4}$. From these, we can obtain systematized ranks 2 or at least 2 and rank 1 and rank correlated to 3. Second forms are appointing by $p, p-2$(twin primes) or $p, p-4$. From these, there deduced generalized rank 0 or 1. In [3], the author showed that rank of $y^2 = x^3 - p(p-4)x$ is 1 when p is $p \equiv 15(mod\ 16)$ and that of curve $y^2 = x^3 - p(p-4)x$ is 1 when $p \equiv 5(mod\ 16)$. In [6], the author verified that rank of curve $y^2 = x^3 - pqx$ is 2 where different primes p and q are given as $p \equiv 11(mod\ 16)$ and $q \equiv 7(mod\ 16)$ and $p = 25u^4 + 20u^2v^2 + 6v^4$ and $q = 25u^4 + 20u^2v^2 + 2v^4$. And the form $y^2 = x^3 - 2px$ is

meaningful as much as $E_{\pm pq}: y^2 = x^3 \pm pqx$. Even if maximal rank of it is less than $E_{\pm pq}$ it is noticeable since there derived many results of generalized rank 1 in this form. In this article, we shall investigate the rank of elliptic equation $y^2 = x^3 + p(p-2)x$ with twin primes as $p \equiv 15(mod\ 16)$ and after that we shall research the rank of elliptic equation $y^2 = x^3 - 2px$ where p is composed of more than three terms with three variables.

Above all, it must be considered notations in [2], [9].

Suppose that E is an elliptic curve $y^2 = x^3 + ax^2 + bx$.

Take Γ as the set of rational points on E.

On account of $Mordell's$ Theorem, Γ is a finitely generated abelian group.

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

Let $Q^{\times}$ be the set of non-zero rational numbers then, this is a multiplicative group.

We appoint that $Q^{\times 2}$ is the subgroup of squares of elements of $Q^{\times}$.

Set α as a homomorphism in section 5 of chapter III in [9] and $\bar{\alpha}$ as homomorphism in [2].

Denote $\bar{E}$ as the curve $y^2 = x(x^2 - 2ax + a^2 - 4b)$.

Assume that $\bar{\Gamma}$ is the set of rational points on $\bar{E}$.

Let $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ be an relating equation for Γ where $b_1$and b_2 are divisors of b as $b = b_1b_2$ with $b_1 \not\equiv 1$, $b(mod\ Q^{\times 2})$.

Assign $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ as relating equation for $\bar{\Gamma}$ where b_1 and b_2 are divisors of $a^2 - 4b$ such that $b_1b_2 = a^2 - 4b$ and $b_1 \not\equiv 1$, $a^2 - 4b(mod\ Q^{\times 2})$.

Take (M , e , N) as an integral solution of above relating equations with (M, N)=(M, e)=(N, e) =$(b_1, e) = (b_2, M)$ =1 and $M \neq 0$, $e \neq 0$.

Lastly, there is induced $2^r = \frac{\#\alpha(\Gamma)\#\bar{\alpha}(\Gamma)}{4}$ with rank r of curve E.

We define next notation:

$w.i.s.t.u.1$: with integers s and t and u and (s, t, u)= 1([8]).

2 Calculation in $E_{p(p-2)}$

It is characteristic that generalized ranks are deduced with the primes $p, p-2$ or $p, p-4 \cdots\cdots (X)$ in curves $E_{\pm pq}$. In forms $E_{\pm p}$, $E_{\pm 2p}$ there is only one prime in coefficient of x, therefore we cannot treat the cases $p, p-2$ or $p, p-4$. And in curve E_{2pq} there are the results but it were restricted to rank 0 with $p, p-2$ and $p, p-4$. In curve E_{-2pqs} there derived rank at most 1 but it were not kind of (X). Henceforth, generalized rank 0 or 1 with $p, p-2$ or $p, p-4$ were emerged specially in curves $E_{\pm pq}$(until now, it is left the possibility that there can be gotten in other forms). Now we calculate the rank of $E_{p(p-2)}: y^2 = x^3 + p(p-2)x$ with twin primes $p, p-2$. We will not treat the solvability of 1) for Γ and 1), 5) for $\bar{\Gamma}$.

Refer to [6] for this and LDV, LSV are in [5] and $r2.4$ in [7].

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 $p \equiv 15(mod\ 16)$ then, we gain $rank(E_{p(p-2)}(Q)) = 1$.

Proo$f$. Take $p = 16k + 15$ with integer k.
Then, there derived relating equations for Γ as follows:

$1)N^2 = M^4 + (16k+15)(16k+13)e^4$
$2)N^2 = (16k+15)M^4 + (16k+13)e^4$

In modulo 16 in equation 2) gives that $0, 1, 4, 9 \equiv N^2 \equiv 15M^4 + 13e^4 \equiv 12, 13, 15(mod\ 16)$ and the sides are unmatched. We can show its insolvability by other method. Equation 2) is given as $2)N^2 = pM^4 + (p-2)e^4$, henceforth cutting down this by p showes that $N^2 \equiv -2e^4(mod\ p)$ but there also educed $\left(\frac{-2e^4}{p}\right) = -1$ and these cannot coexist and hence we also have a contradiction.
Resultantly, we reach that #α(Γ) = 2.
Next, there is the curve $\overline{E_{-pq}}$ as $y^2 = x^3 - 4(16k+15)(16k'+13)x$.
Whence, we take relating equations for $\bar{\Gamma}$ as follows:

$1)N^2 = M^4 - 4(16k+15)(16k+13)e^4$
$2)N^2 = -M^4 + 4(16k+15)(16k+13)e^4$
$3)N^2 = 2M^4 - 2(16k+15)(16k+13)e^4$
$4)N^2 = -2M^4 + 2(16k+15)(16k+13)e^4$
$5)N^2 = 4M^4 - (16k+15)(16k+13)e^4$
$6)N^2 = -4M^4 + (16k+15)(16k+13)e^4$
$7)N^2 = (16k+15)M^4 - 4(16k+13)e^4$
$8)N^2 = -(16k+15)M^4 + 4(16k+13)e^4$
$9)N^2 = 2(16k+15)M^4 - 2(16k+13)e^4$
$10)N^2 = -2(16k+15)M^4 + 2(16k+13)e^4$
$11)N^2 = 4(16k+15)M^4 - (16k+13)e^4$
$12)N^2 = -4(16k+15)M^4 + (16k+13)e^4$

In modulo 16 in relating equation 2) yields that $1,\ 9 \equiv N^2 \equiv 15M^4 + 156e^4 \equiv 15 + 12e^4 \equiv 15, 11(mod\ 16)$ and two sides do not match, thereby it cannot take a solution.
Cutting down on 3) and 4) by $p-2$ gives that $3)N^2 \equiv 2M^4(mod\ p-2)$ and $4)N^2 \equiv -2M^4(mod\ p-2)$ but we also confront to $3)\left(\frac{2M^4}{p-2}\right) = -1$, $4)\left(\frac{-2M^4}{p-2}\right) = -1$ and thus a contradiction is gotten in both cases.

In the next step, reducing equation 6) by prime p induces that $N^2 \equiv -4M^4(mod\ p)$ but simultaneously we are confronted with $\left(\frac{-4M^4}{p}\right) = -1$ and these cannot exist together, thus we get a contradiction.

Cutting down on relating equation 7) by 16 derives the congruence $1,\ 9 \equiv N^2 \equiv 15 + 12e^4 \equiv 15, 11(mod\ 16)$ and the sides are unmatched, thereby we gain a contradiction.

Reducing equation 8) by p derives that $N^2 \equiv -8e^4(mod\ p)$ but we also have $\left(\frac{-8e^4}{p}\right) = -1$ and these cannot coexist, therefore a contradiction is deduced.

Equation 9) is 9)$N^2 = 2pM^4 - 2(p-2)e^4$ and it takes a solution (1, 1, 2).

In modulo 32 in relating equation 10) shows that $0,\ 4,\ 16 \equiv N^2 \equiv 2M^4 + 26e^4 \equiv 28(mod\ 32)$ and this is unmatched congruence.

In modulo 16 in relating equation 11) deduces that $1, 9 \equiv N^2 \equiv 12M^4 + 3e^4 \equiv 15, 3(mod\ 16)$ and we obtain unmatched relation.

Equation 12) is $N^2 = -4pM^4 + (p-2)e^4$. Cutting down on this by p gives that $N^2 \equiv -2e^4(mod\ p)$ but it is induced that $\left(\frac{-2e^4}{p}\right) = -1$. Whence, there educed a contradiction, hence no solution exists in this equation.

For equations 10) and 11) we also can verify its insolvability by other method.

Next, if a solution exists in relating equation 10) then, we are faced with the congruences $N^2 \equiv -2(16k+15)M^4(mod\ p-2)$ and $N^2 \equiv 2(16k+13)e^4(mod\ p)$ respectively by reduction of it by $p-2$ and p. Wherefore, we attain that

$$1 = \left(\frac{-2(16k+15)M^4}{p-2}\right) = -\left(\frac{p}{p-2}\right) \text{ and}$$

$$1 = \left(\frac{2(16k+13)e^4}{p}\right) = \left(\frac{p-2}{p}\right).$$

LDV is deduced but there comes LSV between p and $p-2$ and so a contradiction is derived.

If a solution exists in 11) then, we acquire the relations $N^2 \equiv 4(16k+15)M^4(mod\ p-2)$ and $N^2 \equiv -(16k+13)e^4(mod\ p)$ respectively from cutting down on it by $p-2$ and p. Thereby, we reach that $1 = \left(\frac{4(16k+15)M^4}{p-2}\right) = \left(\frac{p}{p-2}\right)$ and $1 = \left(\frac{-(16k+13)e^4}{p}\right) = -\left(\frac{p-2}{p}\right)$. There derived LDV but we take LSV between p and $p-2$ and thus a contradiction is educed.

On that account, we obtain that $\#\bar{\alpha}(\bar{\Gamma}) = 4$.

For this reason, $rank(E_{p(p-2)}(Q)) = 1$ is educed owing to $r2.4$. □

Case for equation 10) in the above using by LDV, LSV insolvability was verified. But it was also given twin primes $p, p-2$ in this equation, hence after cutting down on it by prime p there derived $N^2 \equiv -4e^4(mod\ p)$ and simultaneously it is

induced $\left(\frac{-4e^4}{p}\right) = -1$, whence a contradiction is educed.

3 In Curve E_{-2p}

There derived many results of generalized rank 1 in form E_{-2p}. It is characteristic of this curve. The form of prime p should be $p \equiv 11, 3, 13, 5(mod\ 16)$. In section 3, we manage the rank of $E_{-2p}: y^2 = x^3 - 2px$ where p has three variables and 6 terms.

Theorem 3.1. (1). If prime p is $p = 38s^4 + 100t^4 + u^4 - 120s^2t^2 + 12s^2u^2 - 20t^2u^2\ w.i.s.t.u.1$ and $p \equiv 11(mod\ 16)$ in E_{-2p} then, it shows that

$$rank(E_{-2(38s^4+100t^4+u^4-120s^2t^2+12s^2u^2-20t^2u^2)}(Q)) = rank(E_{p(p-2)}(Q)).$$

(2). Suppose that p is a prime such that $p = 402s^4 + 4t^4 + u^4 - 80s^2t^2 - 40s^2u^2 + 4t^2u^2\ w.i.s.t.u.1$ and $p \equiv 3(mod\ 16)$ in E_{-2p} then, the result

$$rank(E_{-2(402s^4+4t^4+u^4-80s^2t^2-40s^2u^2+4t^2u^2)}(Q)) = rank(E_{p(p-2)}(Q))$$

is educed.

(3). Define prime p as the form $p = 486s^4 + 324t^4 + u^4 + 792s^2t^2 - 44s^2u^2 - 36t^2u^2\ w.i.s.t.u.1$ and $p \equiv 3(mod\ 16)$ in curve E_{-2p} then, it induces that

$$rank(E_{-2(486s^4+324t^4+u^4+792s^2t^2-44s^2u^2-36t^2u^2)}(Q)) = rank(E_{p(p-2)}(Q)).$$

(4). Assign prime p as the form $p = 146s^4 + t^4 + 9u^4 + 24s^2t^2 + 72s^2u^2 + 6t^2u^2\ w.i.s.t.u.1$ and $p \equiv 3(mod\ 16)$ in E_{-2p} then, it gives that

$$rank(E_{-2(146s^4+t^4+9u^4+24s^2t^2+72s^2u^2+6t^2u^2)}(Q)) = rank(E_{p(p-2)}(Q)).$$

Proo$f$. (1). Due to [4], there is remained relating equation for Γ that is necessary to look into the solvability of

$4)N^2 = -2M^4 + (38s^4 + 100t^4 + u^4 - 120s^2t^2 + 12s^2u^2 - 20t^2u^2)e^4$ for Γ.

Above all, the terms $100t^4$ and u^4 are appeared in coefficient of e^4.

Wherefore, we can expect that there will be appeared the square of polynomial that is comprised of s, t, u.

Now it is essential to find the square form for the term s^4.

Next, we confront to arithmetical value

$$-2M^4 + 38s^4e^4.$$

On that account, take $e = 1$ and $M = s$ then, we gain $36s^4$.
There are remained the terms

$$-120s^2t^2, 12s^2u^2, -20t^2u^2.$$

Two terms for s^2t^2 and t^2u^2 are negative and there is common term t^2.
Therefore, we select components of N as $6s^2$ and $-10t^2$ and u^2.
The term $-120s^2t^2$ are induced from $6s^2$ and $-10t^2$.
The term $12s^2u^2$ is gotten from $6s^2, u^2$.
We obtain $-20t^2u^2$ due to $-10t^2, u^2$.
Consequentially, we attain the value N as

$$6s^2 - 10t^2 + u^2.$$

On this account, the solution of equation 4) is derived as $(s, 1, 6s^2 - 10t^2 + u^2)$.
It yields the conclusion $\#\alpha(\Gamma) = 4$.
For that reason, the consequence

$$rank(E_{-2(38s^4+100t^4+u^4-120s^2t^2+12s^2u^2-20t^2u^2)}(Q)) = 1$$

is derived.
Now by lemma 2.1, we complete the proof.
(2). If there is given the solution of equation

$$4)N^2 = -2M^4 + (402s^4 + 4t^4 + u^4 - 80s^2t^2 - 40s^2u^2 + 4t^2u^2)e^4 \text{ for } \Gamma$$

then, it is sufficient to calculate the rank of curve on account of [4].
Two squares $4t^4$ and u^4 are shown in coefficient of e^4.
Henceforth, there exists a potentiality that form of square will be appeared after determining the integers M, e.
It needs to search the form of square correlated to s^4.
We should consider numerical value $-2M^4 + 402s^4e^4$.
For that reason, we appoint that $e = 1$ and $M = s$ then, it is given that $400s^4$.
Next, we confront to $-80s^2t^2, -40s^2u^2, 4t^2u^2$.
The value of two terms for s^2t^2 and s^2u^2 are negative.
We take the components of N as $20s^2$ and $-2t^2$ and $-u^2$.
Now due to $20s^2, -2t^2$ there derived $-80s^2t^2$.
By $20s^2$ and $-u^2$ we acquire that $-40s^2u^2$.
From $-2t^2$ and $-u^2$ there comes $4t^2u^2$.

Henceforth, the integer N is induced as $20s^2 - 2t^2 - u^2$.
Thereby, we attain the solution of 4) as

$$(s, 1, 20s^2 - 2t^2 - u^2).$$

It shows that $\#\alpha(\Gamma) = 4$.
Consequently, there comes

$$rank(E_{-2(402s^4+4t^4+u^4-80s^2t^2-40s^2u^2+4t^2u^2)}(Q)) = 1.$$

Next form lemma 2.1, the proof is accomplished.

(3). If we find the solution of equation 4)$N^2 = -2M^4 + (486s^4 + 324t^4 + u^4 + 792s^2t^2 - 44s^2u^2 - 36t^2u^2)e^4$ for Γ then, it is enough to compute the rank of curve from [4]. The squares $324t^4$ and u^4 are found in coefficient of e^4. Therefore, there is a possibility of appearance of polynomial's square with variables s, t, u. Accordingly, we ought to look for the square related to s^4. There is left $-2M^4 + 486s^4e^4$. Henceforth, assign $e = 1$ and $M = s$ then, we took $484s^4$. In the next step, we are faced with $792s^2t^2$, $-44s^2u^2, -36t^2u^2$. The symbols of terms for s^2u^2 and t^2u^2 are both negative. Since there is common value u^2 in these terms we decide the components of N as $22s^2$ and $18t^2$ and $-u^2$. There induced $792s^2t^2$ from $22s^2$, $18t^2$. There educed $-44s^2u^2$ from $22s^2$, $-u^2$. We obtain $-36t^2u^2$ from $18t^2$, $-u^2$. Accordingly, we gain the value N as $22s^2 + 18t^2 - u^2$. It follows that $(s, 1, 22s^2 + 18t^2 - u^2)$ as a solution of equation 4). Hence, there deduced the conclusion $\#\alpha(\Gamma) = 4$. Lastly, we confront to $rank(E_{-2(486s^4+324t^4+u^4+792s^2t^2-44s^2u^2-36t^2u^2)}(Q)) = 1$. By lemma 2.1, the proof is done.

(4). The equation for Γ that is needed to find the solution is 4)$N^2 = -2M^4 + (146s^4 + t^4 + 9u^4 + 24s^2t^2 + 72s^2u^2 + 6t^2u^2)e^4$ because of [4]. Squares t^4 and $9u^4$ are emerged in coefficient of e^4. Whence, a probability for being shown the polynomial's square exists. Thereby, it is necessary to search the square involved to s^4. It is remained $-2M^4 + 146s^4e^4$. Denote $e = 1$ and $M = s$ then, there educed that $144s^4$. Now we confront to $24s^2t^2, 72s^2u^2, 6t^2u^2$. The value of terms for s^2u^2 and t^2u^2 are positive. Because there exists a common thing u^2 in these terms, we determine the components of N as $12s^2$ and t^2 and $3u^2$. We gain $24s^2t^2$ from $12s^2$ and t^2. We take $72s^2u^2$ from $12s^2$ and $3u^2$. There derived $6t^2u^2$ from t^2 and $3u^2$. It leads to N as $12s^2 + t^2 + 3u^2$. Hence, we obtain the triple $(s, 1, 12s^2 + t^2 + 3u^2)$ as a solution of equation 4). Wherefore, we reach that $\#\alpha(\Gamma) = 4$. For this reason, there comes the result as $rank(E_{-2(146s^4+t^4+9u^4+24s^2t^2+72s^2u^2+6t^2u^2)}(Q)) = 1$. Owing to lemma 2.1, the proof is completed. □

Prime numbers p were the forms $p = As^4 + Bt^4 + Cu^4 + Ds^2t^2 + Fs^2u^2 + Gt^2u^2 \cdots\cdots (LL)$ in above results. The terms for s^2t^2, s^2u^2, t^2u^2 are positive or

negative. Only the case of (4) three terms are all positive. Since the resultant must be square the terms for s^4 and t^4 and u^4 are all positive and there is changed in symbols for terms s^2t^2, s^2u^2, t^2u^2. In case of $p = Hu^4 + Iu^2v^2 + Kv^4$ with rank 1, it is similar that square terms for u^4, v^4 are positive meanwhile there is negative term in u^2v^2. And the numbers of places in coefficients of terms are from 1 to 3 in the above. Compared with other primes $p = Hu^4 + Iu^2v^2 + Kv^4$ the bigness is smaller. In this form there appeared the coefficient H that has more than 10 places$\cdots\cdots(SS)$ but in (LL), it is difficult to search as kind of form of (SS) in relative.

Remark 3.2. Above primes p were $p = As^4 + Bt^4 + Cu^4 + Ds^2t^2 + Fs^2u^2 + Gt^2u^2 \cdots\cdots (LL)$. Compared with the form $p = Hu^4 + Iu^2v^2 + Kv^4 \cdots\cdots (Y)$, there emerged less examples in form (LL). It is result of computation. And in bigness, case of (LL) is smaller than (Y). In seemingly, the case of (LL) has more terms and thus the bigness of numbers in examples seems to be larger than case of (Y). But it isn't. As we will treat in next section, in form (LL) it is difficult to find the numbers with more than 5 places. In (Y) we can search the numbers of primes in examples with more than 10 places.

4 Examples

In section 4, we will preset examples of preceding results. Primality is checked in [1].

The examples of lemma 2.1 are the next things:

$(p, p-2)$:(31, 29), (271, 269), (463, 461), (1231, 1229), (1279, 1277),

(1951, 1949), (1999, 1997), (2143, 2141).

Examples from theorem 3.1(1) to (4) are followings:

(p, s, t, u):(11, 1, 1, 1), (2971, 3, 1, 3), (15787, 3, 1, 9).

(p, s, t, u):(26083, 3, 3, 1), (2135971, 9, 9, 1).

(p, s, t, u):(1523, 1, 1, 1), (36643, 3, 1, 5).

(p, s, t, u):(1091, 1, 3, 2), (11027, 1, 9, 2).

References

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

[2] J. A. Johnstone and B. K. Spearman, Congruent number elliptic curves with rank at least three, *Canad. Math. Bull,* **53** (2010), 661 – 666. https://doi.org/10.4153/cmb-2010-071-3

[3] 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

[4] 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

[5] S. W. Kim, Different odd primes in curve $y^2 = x^3 - pqx$, *Far East J. Math. Sci. (FJMS),* **107** (1), (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] 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 30, 2026