International Journal of Algebra, Vol. 20, 2026, no. 1, 33 - 40
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2026.92004

Comparison of Ranks in Elliptic Curves

$y^2 = x^3 - Apqx$

Shin-Wook Kim

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

Abstract

Take elliptic curves E_{-pq} and E_{-2pq} as $y^2 = x^3 - pqx$ and $y^2 = x^3 - 2pqx$ with distinct odd primes p and q then, we will compare the ranks of curves according to each condition.

Mathematics Subject Classification: 14G05, 11A41

Keywords: Elliptic curve, distinct odd primes

1 Introduction

In [2], the author showed that rank of $y^2 = x^3 - pqx$ is at most 3 when p and q are different odd primes as $p \equiv 13(mod\ 16)$ and $q \equiv 13(mod\ 16)$. Usually in $E_{-pq}: y^2 = x^3 - pqx$ under the hypothesis that $p \equiv 1(mod\ 8)$ and $q \equiv 5(mod\ 16)$ or $p \equiv 1(mod\ 8)$ and $q \equiv 13(mod\ 16)$ rank can take at most 3. But the forms $p \equiv 13(mod\ 16)$ and $q \equiv 13(mod\ 16)$([2]) are same forms and there is no form $p \equiv 1(mod\ 8)$, thus it is noticeable that if we can find the rank 3 in E_{-pq}. In this article, we compute rank of $y^2 = x^3 - pqx$ when primes are $p \equiv 13(mod\ 16)$ and $q \equiv 13(mod\ 16)$ and compare the consequences with other curves.

Define E and $\bar{E}$ as elliptic curves $y^2 = x^3 + ax^2 + bx$ and $y^2 = x(x^2 - 2ax + a^2 - 4b)$ and take Γ and $\bar{\Gamma}$ as the set of rational points on E and $\bar{E}$ respectively.

The homomorphism α and $\bar{\alpha}$ are in [5] and [4] and relations equations $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ and $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ for Γ and $\bar{\Gamma}$ are in section 6 of chapter III in [5] and [4] respectively. Let (M, e, N) be a solution of above equations that were in [5] and [4].

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

The notations are defined as follows:

$w.i.u.v.w.1$: with integers u and v and w and

$$(u, v, w) = 1.$$

$w.i.A.B.C.D.F.G.H.I.J.K.L.R.S.1$: with integers A and B and C and D and F and G and H and I and J and K and L and R and S and $(A, B, C, D, F, G, H, I, J, K, L, R, S) = 1$.

$r^{\geq}4.4$: $2^r \geq \frac{4\cdot4}{4}$([4]).

$r4.4$: $2^r = \frac{4\cdot4}{4}$([4]).

$r4.2$: $2^r = \frac{4\cdot2}{4} = 2$([4]).

2 Ranks in Two curves

In section 2, we treat the ranks of curves. For curve E_{-pq} where primes are $p \equiv 13(mod\ 16)$ and $q \equiv 13(mod\ 16)$ there remained relating equations $2)N^2 = -M^4 + pqe^4$ and $3)N^2 = pM^4 - qe^4$ and $4)N^2 = -pM^4 + qe^4$ for Γ and $4)N^2 = pM^4 + 4qe^4$ and $6)N^2 = 4pM^4 + qe^4$ for $\bar{\Gamma}$ to compute the rank from [2]. For curve E'_{-pq} the remaining equations are $3)N^2 = pM^4 - qe^4$ for Γ and $5)N^2 = 2pM^4 + 2qe^4$ for $\bar{\Gamma}$ for treating the rank due to [3].

Theorem 2.1. Suppose that E_{-pq} satisfy that $p \equiv 13(mod\ 16)$ and $q \equiv 13(mod\ 16)$ and $p = 25t^4 + 4$ and $q = 9t^4 + 4$ with odd integer t and E'_{-pq} is an elliptic curve such that $p = 11u^4 + 9v^4 + w^4 + 18u^2v^2 + 6u^2w^2 + 6v^2w^2$ $w.i.u.v.w.1$, $p \equiv 3(mod\ 16)$ and $q = 7u^4 + 9v^4 + w^4 + 18u^2v^2 + 6u^2w^2 + 6v^2w^2$ $w.i.u.v.w.1$ and $q \equiv 15(mod\ 16)$ and E_{-2pq} is given as

$$p = 17A^2 + 2B^2 + 2C^2 + 2D^2 + 2F^2 + 2G^2 + 2H^2 + 2I^2 + 2J^2 + 2K^2 + 2L^2$$

$$+2R^2 + 2S^2 + 2BC + 2BD + 2BF + 2BG + 2BH + 2BI + 2BJ + 2BK + 2BL$$

$$+2BR + 2BS + 2CD + 2CF + 2CG + 2CH + 2CI + 2CJ + 2CK + 2CL + 2CR$$

$$+2CS + 2DF + 2DG + 2DH + 2DI + 2DJ + 2DK + 2DL + 2DR + 2DS + 2FG$$

$$+2FH + 2FI + 2FJ + 2FK + 2FL + 2FR + 2FS + 2GH + 2GI + 2B + 2C + 2$$

$$\cdot D + 2F + 2G + 2H + 2I + 2J + 2K + 2L\ w.i.A.B.C.D.F.G.H.I.J.K.L.R.S.$$

1 and $p \equiv 13(mod\ 16)$ and $q = 9A^2 + B^2 + C^2 + D^2 + F^2 + G^2 + H^2 + I^2 +$

$$J^2 + K^2 + L^2 + R^2 + S^2 + BC + BD + BF + BG + BH + BI + BJ + BK + BL +$$

$$BR + BS + CD + CF + CG + CH + CI + CJ + CK + CL + CR + CS + DF + DG$$

$$+DH + DI + DJ + DK + DL + DR + DS + FG + FH + FI + FJ + FK + FL + F$$

$$\cdot R + FS + GH + GI + B + C + D + F + G + H + I + J + K + L\ w.i.A.B.C.D.$$

$F.G.H.I.J.K.L.R.S.1$ and $q \equiv 7(mod\ 16)$ then, there comes that

$$rank(E_{-(25t^4+4)(9t^4+4)}(Q)) \geq$$

$$rank(E'_{-((11u^4+9v^4+\cdots\cdots+6u^2w^2+6v^2w^2)(7u^4+9v^4+\cdots\cdots+6u^2w^2+6v^2w^2))}(Q))$$

$$> rank(E_{-2(17A^2+2B^2+2C^2+\cdots\cdots+2J+2K+2L)(9A^2+B^2+C^2+\cdots\cdots+J+K+L)}(Q)).$$

Proo$f$. First, we consider rank of E_{-pq}.

There exist relating equations for Γ as $1)N^2 = M^4 - (25t^4 + 4)(9t^4 + 4)e^4$ and $2)N^2 = -M^4 + (25t^4 + 4)(9t^4 + 4)e^4$ and $3)N^2 = (25t^4 + 4)M^4 - (9t^4 + 4)e^4$ and $4)N^2 = -(25t^4 + 4)M^4 + (9t^4 + 4)e^4$.

Equation 2) is $N^2 = -M^4 + (225t^8 + 136t^4 + 16)e^4$.

The term $225t^8$ is a square and there is also a square 16 in coefficient of e^4.

Henceforth, we suppose these comprise the resultant then, there should be appeared the term

$$2 \cdot 15t^4 \cdot 4 = 120t^4.$$

In arithmetical value $-M^4 + 136t^4e^4$ take $e = 1$ then, we must obtain that

$$-M^4 + 136t^4 = 120t^4.$$

It implies that $M^4 = 16t^4$.
Thereby, we attain that $M = 2t$.
Furthermore, from the numeration

$$-M^4 + 225t^8 + 136t^4 + 16$$

$$= -(2t)^4 + 225t^8 + 136t^4 + 16$$

$$= 225t^8 + 120t^4 + 16$$

the value N is gotten as $N = 15t^4 + 4$.
Whence, the solution is derived as $(2t, 1, 15t^4 + 4)$.
Next, the triple $(1, 1, 4t^2)$ satisfies the solution of 3).
Consequently, we got solutions in two equations 2) and 3).
In conclusion, from the algebraic structure $-1 \cdot (25t^4 + 4) = -(25t^4 + 4) \in \alpha(\Gamma)(mod\ Q^{\times 2})$ the equation $4) N^2 = -(25t^4 + 4)M^4 + (9t^4 + 4)e^4$ also takes a solution.
On this account, we say that $\#\alpha(\Gamma) = 8$.
Next, it is trivial that $\#\bar{\alpha}(\bar{\Gamma}) \geq 2$.
For this reason, we conclude that $r^{\geq}4.4$.
Consequently, we get that

$$rank(E_{-(25t^4+4)(9t^4+4)}(Q)) \geq 2.$$

Second, we treat rank of $E_{-pq}{}'$.
Equations are given as

$3) N^2 = (11u^4 + 9v^4 + w^4 + 18u^2v^2 + 6u^2w^2 + 6v^2w^2)M^4 - (7u^4 + 9v^4 +$

$w^4 + 18u^2v^2 + 6u^2w^2 + 6v^2w^2)e^4$ for Γ and

$5) N^2 = 2(11u^4 + 9v^4 + w^4 + 18u^2v^2 + 6u^2w^2 + 6v^2w^2)M^4 + 2(7u^4 + 9v^4$

$+w^4 + 18u^2v^2 + 6u^2w^2 + 6v^2w^2)e^4$ for $\bar{\Gamma}$.

The triple $(1, 1, 2u^2)$ satisfies the solution of 3).
In equation 5) replacing 1 into M and e then, we gain

$$22u^4 + 18v^4 + 2w^4 + 36u^2v^2 + 12u^2w^2 + 12v^2w^2$$

$$+14u^4 + 18v^4 + 2w^4 + 36u^2v^2 + 12u^2w^2 + 12v^2w^2$$

$$= 36u^4 + 36v^4 + 4w^4 + 72u^2v^2 + 24u^2w^2 + 24v^2w^2.$$

Therefore, we got the solution as $(1, 1, 6u^2 + 6v^2 + 2w^2)$.
To conclude, it is derived that $\#\alpha(\Gamma) = \#\bar{\alpha}(\bar{\Gamma}) = 4$.
And it follows that $r4.4$.
Accordingly, we gain

$$rank\left(E'_{-((11u^4+9v^4+\cdots\cdots+6u^2w^2+6v^2w^2)(7u^4+9v^4+\cdots\cdots+6u^2w^2+6v^2w^2)}(Q)\right) = 2.$$

Third, we compute rank of E_{-2pq}.
Take p and q as $p = 16k + 13$ and $q = 16k^{'} + 7$ with integers k and k'.
Equations for Γ are derived as $1)N^2 = M^4 - 2(16k + 13)(16k' + 7)e^4$ and $2)N^2 = -M^4 + 2(16k + 13)(16k' + 7)e^4$ and $3)N^2 = 2M^4 - (16k + 13)(16k' + 7)e^4$ and $4)N^2 = -2M^4 + (16k + 13)(16k' + 7)e^4$ and $5)N^2 = (16k + 13)M^4 - 2(16k' + 7)e^4$ and $6)N^2 = -(16k + 13)M^4 + 2(16k' + 7)e^4$ and $7)N^2 = 2(16k + 13)M^4 - (16k' + 7)e^4$ and $8)N^2 = -2(16k + 13)M^4 + (16k' + 7)e^4$.
From 2) to 4) no solution exists since reduction of these shows that $2)N^2 \equiv -M^4(mod\ q)$ and $3)N^2 \equiv 2M^4(mod\ p)$ and $4)N^2 \equiv -2M^4(mod\ q)$ but there also given that $2)\left(\frac{-M^4}{q}\right) = -1$ and $3)\left(\frac{2M^4}{p}\right) = -1$ and $4)\left(\frac{-2M^4}{q}\right) = -1$ and taking a pair in each case derives a contradiction.
In modulo 16 in equations 5) and 8) yields that $1, 9 \equiv N^2 \equiv 13M^4 + 2e^4 \equiv 15, 13(mod\ 16)$ and $1, 9 \equiv N^2 \equiv 6M^4 + 7e^4 \equiv 7, 13(mod\ 16)$ respectively, hence neither takes a solution.
Next, equation 6) is

$$N^2 = -(17A^2 + 2B^2 + 2C^2 + 2D^2 + 2F^2 + 2G^2 + 2H^2 + 2I^2 + 2J^2 + 2K^2 +$$

$$2L^2 + 2R^2 + 2S^2 + 2BC + 2BD + 2BF + 2BG + 2BH + 2BI + 2BJ + 2BK + 2$$

$$\cdot BL + 2BR + 2BS + 2CD + 2CF + 2CG + 2CH + 2CI + 2CJ + 2CK + 2CL +$$

$$2CR + 2CS + 2DF + 2DG + 2DH + 2DI + 2DJ + 2DK + 2DL + 2DR + 2DS +$$

$$2FG + 2FH + 2FI + 2FJ + 2FK + 2FL + 2FR + 2FS + 2GH + 2GI + 2B + 2$$

$$\cdot C + 2D + 2F + 2G + 2H + 2I + 2J + 2K + 2L)M^4 + 2(9A^2 + B^2 + C^2 + D^2$$

$$+F^2 + G^2 + H^2 + I^2 + J^2 + K^2 + L^2 + R^2 + S^2 + BC + BD + BF + BG + BH$$

$$+BI + BJ + BK + BL + BR + BS + CD + CF + CG + CH + CI + CJ + CK + C$$

$\cdot L + CR + CS + DF + DG + DH + DI + DJ + DK + DL + DR + DS + FG + F$

$\cdot H + FI + FJ + FK + FL + FR + FS + GH + GI + B + C + D + F + G + H + I$

$+J + K + L)e^4.$

Substitute 1 into M and e derives the result

$-(17A^2 + 2B^2 + 2C^2 + 2D^2 + 2F^2 + 2G^2 + 2H^2 + 2I^2 + 2J^2 + 2K^2 + 2L^2 +$

$2R^2 + 2S^2 + 2BC + 2BD + 2BF + 2BG + 2BH + 2BI + 2BJ + 2BK + 2BL +$

$2BR + 2BS + 2CD + 2CF + 2CG + 2CH + 2CI + 2CJ + 2CK + 2CL + 2CR +$

$2CS + 2DF + 2DG + 2DH + 2DI + 2DJ + 2DK + 2DL + 2DR + 2DS + 2FG +$

$2FH + 2FI + 2FJ + 2FK + 2FL + 2FR + 2FS + 2GH + 2GI + 2B + 2C + 2D$

$+2F + 2G + 2H + 2I + 2J + 2K + 2L) + 2(9A^2 + B^2 + C^2 + D^2 + F^2 + G^2 +$

$H^2 + I^2 + J^2 + K^2 + L^2 + R^2 + S^2 + BC + BD + BF + BG + BH + BI + BJ +$

$BK + BL + BR + BS + CD + CF + CG + CH + CI + CJ + CK + CL + CR + CS$

$+DF + DG + DH + DI + DJ + DK + DL + DR + DS + FG + FH + FI + FJ +$

$+FK + FL + FR + FS + GH + GI + B + C + D + F + G + H + I + J + K + L)$

$= -17A^2 + 18A^2 = A^2.$

On this account, we take the solution as $(1, 1, A)$.

Lastly, assume that 7) has a solution then, we obtain that $2(16k + 13)\big(-(16k' + 13)\big) \equiv -2 \in \alpha(\Gamma)(mod\ Q^{\times 2})$ but equation 4) cannot take a solution, thus a contradiction is induced and so no solution exists in equation 7).

Therefore, we have $\#\alpha(\Gamma) = 4$.

Next, we gain the curve $\overline{E_{-2pq}}$ as $y^2 = x^3 + 8(16k + 13)(16k' + 7)x$.

Hence, it follows the equations for $\bar{\Gamma}$ as $1)N^2 = M^4 + 8(16k + 13)(16k' + 7)e^4$ and $2)N^2 = 2M^4 + 4(16k + 13)(16k' + 7)e^4$ and $3)N^2 = 4M^4 + 2(16k + 13)(16k' + 7)e^4$ and $4)N^2 = 8M^4 + (16k + 13)(16k' + 7)e^4$ and $5)N^2 = (16k + 13)M^4 + 8(16k' + 7)e^4$ and $6)N^2 = 2(16k + 13)M^4 + 4(16k' + 7)e^4$ and $7)N^2 = 4(16k + 13)M^4 + 2(16k' + 7)e^4$ and $8)N^2 = 8(16k + 13)M^4 + (16k' + 7)e^4$.

Cutting down on equations from 2) to 8) by 4 and 8 yields that $2)0 \equiv N^2 \equiv 2M^4 \equiv 2(mod\ 4)$ and $3)0 \equiv N^2 \equiv 26 \cdot 7e^4 \equiv 2(mod\ 4)$ and $4)1 \equiv N^2 \equiv$

$91e^4 \equiv 3(mod\ 8)$ and $5)1 \equiv N^2 \equiv 13M^4 \equiv 5(mod\ 8)$ and $6)0 \equiv N^2 \equiv 26M^4 \equiv 2(mod\ 4)$ and $7)0 \equiv N^2 \equiv 14e^4 \equiv 2(mod\ 4)$ and $8)1 \equiv N^2 \equiv 7e^4 \equiv 7(mod\ 8)$ and the sides are unmatched in all relations.

Whence, it implies that $r4.2$.

Accordingly, there comes that

$$rank(E_{-2(17A^2+2B^2+2C^2+\cdots\cdots+2J+2K+2L)(9A^2+B^2+C^2+\cdots\cdots+J+K+L)}(Q)) = 1.$$

Finally, we completed the proof. □

In above the rank of E_{-pq} is gotten as at least 2. In previous section, we mentioned that whether the rank is 3 when $p \equiv 13(mod\ 16)$ and $q \equiv 13(mod\ 16)$ or not. The conclusion is not 3. There is left the probability that rank is 3 if there is found the solution in relating equation $4)N^2 = pM^4 + 4qe^4$ or $6)N^2 = 4pM^4 + qe^4$ for $\bar{\Gamma}$([2]). But under the condition that $p = 25t^4 + 4$ and $q = 9t^4 + 4$ with odd integer t searching the solution is not simple. Thus, we only can conclude that $\#\bar{\alpha}(\bar{\Gamma}) \geq 2$ and this induces rank at least 2. This is the kernel of rank of elliptic curve in form $y^2 = x^3 + Ax$. The noticeable thing in above E_{-pq} is the forms of primes $p = At^4 + B$ and $q = Ct^4 + D$. Usually at least rank 2 is gotten in the forms $p = Hu^4 + Iu^2v^2 + Kv^4$, $p = H'u^4 + I'u^2v^2 + K'v^4$. That is, the numbers of terms are at least 3 in primes but here we got the consequence where numbers of terms are 2. This can be correlated to the same forms of primes p and q as $p \equiv 13(mod\ 16)$ and $q \equiv 13(mod\ 16)$. But we cannot conclude certainly.

Remark 2.2. In [2], the author suggested example of rank at most 3 in curve $E_{-pq}(p \equiv 13(mod\ 16)$ and $q \equiv 13(mod\ 16))$ as $y^2 = x^3 - 29 \cdot 13x$. This is the minimal case where p and q can take. But we could not conclude that the rank is 3 in E_{-pq}. Thus, the author used 'at most'. But by giving additional conditions as $p = 25t^4 + 4$ and $q = 9t^4 + 4$ with odd integer t even if the consequence was not 3 but we get a conclusion that rank is at least 2. And in next section we will mention that the examples are gotten where primes are larger than 29 and 13.

Remark 2.3. In E_{-2pq} in the above, the primes are little different from general forms. In curve E_{-2pq} if the rank is 1 then, usually primes are gotten as $p = Hu^4 + Iu^2v^2 + Kv^4$, $p = H'u^4 + I'u^2v^2 + K'v^4$. And even though the terms are increased there maintained the regularity. Namely, there are the variables repeated. But above forms is different. The variables are $A, B, C, D, F, G, H, I, J, K, L, R, S$ and there are the parts which were not repeated. For examples, in terms we note that $2GH + 2GI$ in p and $GH + GI$ in q. In usual pattern there also should be appeared $2GJ + 2GK + 2GL + 2GR + 2GS$ in p and $GJ + GK + GL + GR + GS$ in q but these are delisted. Similarly, there are $2B + 2C + 2D + 2F + 2G + 2H + 2I + 2J + 2K + 2L$ in p and $B + C + D + F + G + H + I + J + K + L$ in q

but the numerical values $2A$, $2R + 2S$ and $A, R + S$ are delisted. Consequently, we can say that generalized rank 1 in E_{-2pq} can be educed in various forms(that is, we need not notice only the forms $p = Hu^4 + Iu^2v^2 + Kv^4$, $p = H'u^4 + I'u^2v^2 + K'v^4$).

3 Examples

The examples of theorem 2.1(1) to (3) are educed as follows(From [1] we can check primality):

(p, q, t): (2029, 733, 3), (60029, 21613, 7), (714029, 257053, 13).

(p, q, u, v, w): (227, 223, 1, 1, 3), (188483, 129919, 11, 3, 3).

$(p, q, A, B, C, D, F, G, H, I, J, K, L, R, S)$:

(25981, 13751, 39, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1),

(209581, 110951, 111, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1).

In E_{-2pq} in the above, if we take $(A, B, C, D, F, G, H, I, J, K, L, R, S)$ as (45, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) then, primes p, q are given as 34549 and 18287 but the forms are $p \equiv 5(mod\ 16)$ and $q \equiv 15(mod\ 16)$.

References

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

[2] S. W. Kim, Change of possible maximal ranks in elliptic curves, *Jeonbuk National University,* 21.02.2014, 1-42.

[3] 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

[4] 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

[5] 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