

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

Shin-Wook Kim

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

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

Abstract

Elliptic curve $y^2 = x^3 - px$ can take ranks from 0 to 2. It means maximal rank is 2. But finding it is not simple treatment. In this article, we approach to rank 2 in curve $y^2 = x^3 - px$.

Mathematics Subject Classification: 11A41, 11G05

Keywords: Prime, elliptic curve

1 Introduction

Maximal rank of curve $y^2 = x^3 - px$ is 2. Thus, there can be deduced rank 0 and 1. When prime is such that $p \equiv 11(mod 16)$ then, rank is 0([3]). And there derived many results of rank 1 of the form $p = Hu^4 + Iv^2v^2 + Kv^4$ where prime is $p \equiv 5(mod 16)$ ([4], [6]). For getting maximal rank prime should be $p \equiv 1(mod 8)$. From [11] and [2] we can obtain rank 2 where primes are gotten as $p = u^4 + v^4 \dots \dots (GG)$ for some integers u and v and $p = e^2 + 1$, $e = 41t^2 + 58t + 41$, $t \neq -1 \dots \dots (NN)$ with prime p and integers e , t . Taking rank 2 in form $y^2 = x^3 - px$ is not simple. In [5] when curve is $y^2 = x^3 - pqx$ there derived rank 2 where primes are $p = 4u^4 + 20u^2v^2 + 27v^4$ and $q = 4u^4 + 20u^2v^2 + 23v^4$ w.i.u.v.1, $p \equiv 3(mod 16)$ and $q \equiv 15(mod 16)$ and in [6] there also induced rank 2 in $y^2 = x^3 - pqx$ where primes p and q are $p = 4u^4 - 20u^2v^2 + 27v^4$ and $q = 4u^4 - 20u^2v^2 + 23v^4$ w.i.u.v.1 $\dots \dots (WW)$ and $p \equiv 11(mod 16)$ and $q \equiv 7(mod 16)$. Our concern is getting maximal rank 2 in elliptic curve $E_{-p}: y^2 = x^3 - px$ where prime is different from (GG) and (NN) .

We try to apply the form (WW) to E_{-p} . The relating equations that should be regarded the solvability are $2)N^2 = -M^4 + pe^4$ for Γ and $2)N^2 = 2M^4 + 2pe^4$ for $\bar{\Gamma}$. We choose prime as $p = 17u^4 + 16u^2v^2 + 4v^4$ then, equation 2) for Γ has a solution $(u, 1, 4u^2 + 2v^2)$ whereas for $\bar{\Gamma}$ we confront to $2M^4 + 2(17u^4 + 16u^2v^2 + 4v^4) = 2M^4 + 34u^4 + 32u^2v^2 + 8v^4$ under the assumption that $e = 1$. If M is chosen as u then, we are faced with $36u^4 + 32u^2v^2 + 8v^4$ but due to non-square term $8v^4$ we cannot expect an appearance of square. If we select prime as $p = 50u^4 + 14u^2v^2 + v^4$ then, there derived a solution $(u, 1, 7u^2 + v^2)$ of $2)N^2 = -M^4 + (50u^4 + 14u^2v^2 + v^4)e^4$ but for $\bar{\Gamma}$ we have that $2)N^2 = 2M^4 + 2(50u^4 + 14u^2v^2 + v^4)e^4 = 2M^4 + (100u^4 + 28u^2v^2 + 2v^4)e^4$. If we put $M = v$ and $e = 1$ then, there induced that $100u^4 + 28u^2v^2 + 4v^4$. There exist two squares but for non-square term it ought to be reduced $40u^2v^2$ but there is $28u^2v^2$, hence it doesn't match to our aim. Not only these attempts but in other tries under the hypothesis that prime is such that $p = Hu^4 + Iu^2v^2 + Kv^4$ it is difficult to attain rank 2 in curve E_{-p} . Therefore, we consider other forms. In curve $E_{-4p}: y^2 = x^3 - 4px$ we confront to primes $p = 68t^4 + 16t^3u + 16tu^3 + 104t^2u^2 + 29u^4$ with integers t and u and $(t, u) = 1$ and $p \equiv 13 \pmod{16}$ and the case $p = 349t^4 - 432t^3u - 48tu^3 + 336t^2u^2 + 148u^4$ with integers t and u and $(t, u) = 1$ and $p \equiv 13 \pmod{16}$ where rank is 1([8]). That is, we apply the form $p = At^4 + Bt^3u + Ctu^3 + Dt^2u^2 + Fu^4$ to the curve $y^2 = x^3 - px$. The value M of solution is given as $at \pm bu$ ([8]). In this paper, we approach to rank 2 of elliptic curve $y^2 = x^3 - px$ where prime is the form $p = At^4 + Bt^3u + Ctu^3 + Dt^2u^2 + Fu^4$. Suppose that $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ is relating equation for Γ in section 6 of chapter III in [10] and $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ is relating equation for $\bar{\Gamma}$ in [5]. And w. i. t. u. 1 and r4.4 are in [7] and [5].

2 Rank 2

As we mentioned in the previous it is necessary to look for the solutions of two equations $2)N^2 = -M^4 + pe^4$ for Γ and $2)N^2 = 2M^4 + 2pe^4$ for $\bar{\Gamma}$. If the triple satisfies the solutions of these then, treating the rank of curve $y^2 = x^3 - px$ is done.

Theorem 2.1. Elliptic curve p satisfies that $p = t^4 \pm 4t^3u \pm 4tu^3 + 6t^2u^2 + 2u^4$ w. i. t. u. 1 and $p \equiv 1 \pmod{8}$ in E_{-p} then, we reach that

$$\text{rank}(E_{-(t^4 \pm 4t^3u \pm 4tu^3 + 6t^2u^2 + 2u^4)}(Q)) = 2.$$

Proof. First, we treat the prime as the form $p = t^4 + 4t^3u + 4tu^3 + 6t^2u^2 + 2u^4$.

There are equations as

$$2)N^2 = -M^4 + (t^4 + 4t^3u + 4tu^3 + 6t^2u^2 + 2u^4)e^4 \text{ for } \Gamma \text{ and}$$

$$2)N^2 = 2M^4 + 2(t^4 + 4t^3u + 4tu^3 + 6t^2u^2 + 2u^4)e^4 \text{ for } \bar{\Gamma}.$$

In equation 2) for Γ there is a square t^4 in coefficient of e^4 .

In arithmetical value $-M^4 + 2u^4e^4$ take e as 1.

If the value M is given as u then, there comes u^4 .

Hence, there is remained

$$t^4 + 4t^3u + 4tu^3 + 6t^2u^2 + u^4.$$

And this is a quartic of $t + u$.

It means that square of $t + u$ satisfies the integer N .

That is, there derived that $N = t^2 + 2tu + u^2$.

Thus, the triple $(u, 1, t^2 + 2tu + u^2)$ is induced as the solution of equation.

In addition, we can find another solution.

If we choose M and e as $t + u$ and 1 then, we confront to

$$\begin{aligned} & -(t + u)^4 + t^4 + 4t^3u + 4tu^3 + 6t^2u^2 + 2u^4 \\ &= -(t^4 + 4t^3u + 4tu^3 + 6t^2u^2 + u^4) \\ & \quad + t^4 + 4t^3u + 4tu^3 + 6t^2u^2 + 2u^4 \\ &= u^4. \end{aligned}$$

Whence, we get the solution as $(t + u, 1, u^2)$.

Consequently, there induced that $\#\alpha(\Gamma) = 4$.

Next, we regard solution of 2) for $\bar{\Gamma}$.

The square $4u^4$ is found in coefficient of e^4 .

But there exists a non-square term $2t^4$ simultaneously.

In considering term $2M^4$ with $2t^4$ if we suppose $M = t$ and $e = 1$ then, we have that

$$2t^4 + 2t^4 = 4t^4.$$

Now, we notice that

$$4t^4 + 8t^3u + 8tu^3 + 12t^2u^2 + 4u^4.$$

This can be factored as

$$4 \cdot (t^4 + 2t^3u + 2tu^3 + 3t^2u^2 + u^4).$$

There are two squares t^4 and u^4 .
 Now we treat the terms $2t^3u$ and $2tu^3$.
 These are expressed as

$$2t^3u = 2 \cdot t^2 \cdot t \cdot u \text{ and}$$

$$2tu^3 = 2 \cdot t \cdot u \cdot u^2 \cdots (UU).$$

Our purpose is attaining a square.
 And the numbers of components are meaningless.
 We decide numbers of it as 3.
 We assume that t^2 and u^2 are components of integer N .
 Except 2 in above factorizations (UU) there are common factors t and u .
 Henceforth, we determine another component as tu then, from the multiplications

$$2 \cdot t^2 \cdot tu \text{ and } 2 \cdot tu \cdot u^2$$

non-square terms $2t^3u$ and $2tu^3$ are reduced.
 Accordingly, the value N is gotten as $2(t^2 + tu + u^2)$.
 Therefore, the solution is given as

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

On this account, we confront to the conclusion $r4.4$.
 Thereby, the rank of $E_{-(t^4+4t^3u+4tu^3+6t^2u^2+2u^4)}$ became 2.
 Second, we investigate the rank where prime is such that $p = t^4 - 4t^3u - 4tu^3 + 6t^2u^2 + 2u^4$.
 The difference with first case is symbols of terms for t^3u and tu^3 .
 Thus, solutions of 2) for Γ are derived as

$$(u, 1, t^2 - 2tu + u^2) \text{ and } (t - u, 1, u^2).$$

And that of 2) for $\bar{\Gamma}$ are given as

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

Wherefore, there deduced that $r4.4$.

For this reason, rank of $E_{-(t^4-4t^3u-4tu^3+6t^2u^2+2u^4)}$ is given as 2. $\square$

We got the primes as $p = t^4 \pm 4t^3u \pm 4tu^3 + 6t^2u^2 + 2u^4$ in the above. These are different from (GG) and (NN) and (WW) . For the first time, the form of prime $p = At^4 + Bt^3u + Ctu^3 + Dt^2u^2 + Fu^4 \cdots (RR)$ was treated in curve $E_{-4p}: y^2 = x^3 - 4px$ which induces rank 1([8]), thus it was considered that the

form (RR) is valid for rank 1. And in curves $E_{\pm 2p}: y^2 = x^3 \pm 2px$ and $E_{-3p}: y^2 = x^3 - 3px$ when rank is correlated to 2 prime is gotten as the form $p = Hu^8 + Iu^4v^4 + Kv^8$, hence we tried to find prime as $p = Hu^4 + Iu^2v^2 + Kv^4$ in E_{-p} which induces rank 2. But form of the prime was not induced readily. From breaking the conventional wisdom and applying the form (RR) to curve $E_{-p}: y^2 = x^3 - px$ we get new consequences. We also needed to mention about bigness. That of coefficient of t^4 is 1 and it is smaller than we guessed. That of u^4 is 2. Due to attempt to taking as $p = 17u^4 + 16u^2v^2 + 4v^4$ or $p = 50u^4 + 14u^2v^2 + v^4$ in preceding section it is apt to guess that absolute value of t^4 is two places of numbers or more. But number 1 is decided as coefficient of t^4 in prime.

Remark 2.2. Above primes are the forms $p = t^4 + 4t^3u + 4tu^3 + 6t^2u^2 + 2u^4$ and $p = t^4 - 4t^3u - 4tu^3 + 6t^2u^2 + 2u^4 \dots (ZZ)$. The terms for squares are the same and other two terms have same absolute values of coefficients and only symbols are different. In [9] parity primes were defined. The forms are $p = Hu^4 \pm Iu^2v^2 + Ku^4$. If we attempt to define parity primes to (ZZ) then, it will be profitable such that $p = At^4 + Bt^3u + Ctu^3 + Dt^2u^2 + Fu^4$ and $p = At^4 - Bt^3u - Ctu^3 + Dt^2u^2 + Fu^4$.

Remark 2.3. In above equation for Γ there derived two solutions. In [8], the author regarded the rank of curve $E_{-4p}: y^2 = x^3 - 4px$ where prime is such that $p = 68t^4 + 16t^3u + 16tu^3 + 104t^2u^2 + 29u^4$ with integers t and u and $(t, u) = 1$ and $p \equiv 13 \pmod{16}$ and the case $p = 349t^4 - 432t^3u - 48tu^3 + 336t^2u^2 + 148u^4$ with integers t and u and $(t, u) = 1$ and $p \equiv 13 \pmod{16}$ and solutions of relating equations $6)N^2 = -4M^4 + pe^4$ for Γ are $(t + u, 1, 8t^2 + 5u^2)$ and $(3t - u, 1, 5t^2 + 12u^2)$ respectively. The coefficients of t^4 and u^4 in primes are 68, 29 and 349, 148 and these are not squares. And in these cases it is difficult to find another solution.

3 Examples

In section 3, we will suggest examples.

Primality is done by [1].

Now we submit examples:

$$(p, t, u)_{+4,+4}:$$

$$(17, 1, 1) \text{ and } (97, 1, 2) \text{ and } (881, 1, 4) \text{ and}$$

$$(10657, 1, 8) \text{ and } (149057, 1, 16).$$

$$(p, t, u)_{-4,-4}:$$

(17, 3, 1) and (257, 5, 1) and (641, 7, 2) and
 (1297, 7, 1) and (2417, 9, 2) and (6577, 11, 2) and (14657, 13, 2).

References

- [1] C. Caldwell, <http://primes.utm.edu/curios/includes/primetest.php>.
- [2] A. J. Hollier, B. K. Spearman and Q. Yang, On the rank and integral points of elliptic curves $y^2 = x^3 - px$, *Int. J. of Algebra*, **3** (2009), 401-406.
- [3] S. W. Kim, Investigating ranks in several elliptic curves, *Far East J. Math. Sci.(FJMS)*, **96** (2015), 887- 898.
- [4] S. W. Kim, Searching the ranks of elliptic curves $y^2 = x^3 - px$, *Int. J. of Algebra*, **12** (2018), 311-318. <https://doi.org/10.12988/ijcms.2018.8934>.
- [5] 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>.
- [6] S. W. Kim, Ranks in elliptic curves $y^2 = x^3 \pm Ax$ with varied primes, *Int. J. of Cont. Math. Sci*, **15** (2020), 127-162. <https://doi.org/10.12988/ija.2026.92010>.
- [7] 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>.
- [8] 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>.
- [9] S. W. Kim, Same rank in curve $y^2 = x^3 - 2px$, *Int. J. of Algebra*, **20** (2026), 89-94. <https://doi.org/10.12988/ijcms.2020.91442>.
- [10] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, New York, (1992).
- [11] B. K. Spearman, Elliptic curves $y^2 = x^3 - px$ of rank two, *Math. J. Okayama Univ*, **49** (2007), 183-184.

Received: September 15, 2026; Published: October 14, 2026