International Journal of Algebra, Vol. 20, 2026, no. 1, 19 - 25
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2026.92002

Consequences of Ranks in $y^2 = x^3 - 2px$

Shin-Wook Kim

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

Abstract

We will numerate the rank of elliptic curve E_{-2p}: $y^2 = x^3 - 2px$ with prime p as $p = As^4 + Bt^4 + Cu^4 + Dv^4 + Fw^4 + Gs^2t^2 + Hs^2u^2 + Is^2v^2 + Js^2w^2 + Kt^2u^2 + Lt^2v^2 + Rt^2w^2 + Su^2v^2 + Uu^2w^2 + Vv^2w^2$ and submit examples of the result.

Mathematics Subject Classification: 11A41, 14G05

Keywords: Prime, elliptic curve

1 Introduction

Bigness is relative notation in elliptic curve. Elkies submitted the result that rank is at least 28([2]). If there suggested curve of rank 29 or 31 or 36 then, rank of at least 28 lose the position of the highest rank. If there is found curve of rank 42 or 53 then, it will be more. In systematized rank of elliptic curve value of 3 or 4 is not small rank. In outward range of rank in elliptic curve rank 3 or 4 is low value. But if it is restricted to systematization then, it is not low rank. In form of E_{-2p}: $y^2 = x^3 - 2px$ with $p \equiv 3, 5, 11, 13 (mod\ 16)$ then, there derived much results of rank 1(generalized). For the bigness of p, there is no certain standard that appoints the big or low. But if p is $p > 10000$ then, it is possible to say that it is large example. In some special form of prime p as the form $p = Hu^4 + Iu^2v^2 + Kv^4 \cdots\cdots (DB)$ there deduced many examples as $10000 < p < 100000000000000$. In this case, if p is the number of 5 places then, it is not large number. In E_{-2p} there educed much results of generalized rank 1 in form p

as $p = Hu^4 + Iu^2v^2 + Kv^4$ and also $p = As^4 + Bt^4 + Cu^4 + Ds^2t^2 + Fs^2u^2 + Gt^2u^2 \cdots\cdots (ND)$. The number of terms in (ND) are 6. The numbers of terms are more than (DB). But there also exists form of p which are more terms than (ND) that yields rank 1 in E_{-2p}. If p is $p = As^4 + Bt^4 + Cu^4 + Dv^4 + Fw^4 + Gs^2t^2 + Hs^2u^2 + Is^2v^2 + Js^2w^2 + Kt^2u^2 + Lt^2v^2 + Rt^2w^2 + Su^2v^2 + Uu^2 \cdot w^2 + Vv^2w^2 \cdots\cdots (FF)$ then, are the numbers of terms are many? We cannot say easily because there are primes p(induces rank 1 in E_{-2p}) which were more complex than (FF). In this article, we will research the rank of E_{-2p} with p as (FF).

Before calculation, we have to notice notations in [3], [5].

Assign E as an elliptic curve $y^2 = x^3 + ax^2 + bx$.

Let Γ be the set of rational points on E.

Then, the set became a finitely generated abelian group.

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

We appoint that $Q^\times$ is the set of non-zero rational numbers then, it is a multiplicative group.

Set $Q^{\times 2}$ as the subgroup of squares of elements of $Q^\times$.

Take homomorphism α and $\bar{\alpha}$ are in [5] and [3].

Suppose that $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ and $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ are relating equations for Γ and $\bar{\Gamma}$ in section 6 of chapter III in [5], [3].

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

Let (M, e, N) be a solution of above relating equations for Γ and $\bar{\Gamma}$ in [3], [5].

Lastly, we take $2^r = \frac{\#\alpha(\Gamma)\#\bar{\alpha}(\Gamma)}{4}$ with rank r of E.

The notations are defined as follows:

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

and $(s, t, u, v, w)=1$.

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

2 Numeration

We already attained many results of rank 1 in curve E_{-2p}. Its forms are mainly $p = Hu^4 + Iu^2v^2 + Kv^4$. And in forms of primes $p = As^4 + Bt^4 + Cu^4 + Ds^2t^2 + Fs^2u^2 + Gt^2u^2$, $p = At^4 + Bt^3u + Ctu^3 + Dt^2u^2 + Fu^4$ there also derived rank 1 often. In section 2, we shall calculate the rank of curve E_{-2p} with the form $p = As^4 + Bt^4 + Cu^4 + Dv^4 + Fw^4 + Gs^2t^2 + Hs^2u^2 + Is^2v^2 + Js^2w^2 + Kt^2u^2 + Lt^2v^2 + Rt^2w^2 + Su^2v^2 + Uu^2w^2 + Vv^2w^2$. For computing the rank, it is sufficient that we only find the solution of relating equation 4)$N^2 = -2M^4 + pe^4$ for Γ on account of [3].

Theorem 2.1. (1). In curve E_{-2p} if prime p is established as the form $p = 51s^4 + t^4 + u^4 + v^4 + w^4 + 14s^2t^2 + 14s^2u^2 + 14s^2v^2 + 14s^2w^2 + 2t^2u^2 + 2t^2v^2 + 2t^2w^2 + 2u^2v^2 + 2u^2w^2 + 2v^2w^2$ $w.i.s.t.u.v.w.1$ and also $p \equiv 11(mod\ 16)$ then, there deduced the consequence

$$rank(E_{-2(51s^4+t^4+u^4+v^4+w^4+14s^2t^2+14s^2u^2+\cdots\cdots\cdots+2u^2v^2+2u^2w^2+2v^2w^2)}(Q)) = 1.$$

(2). If curve E_{-2p} satisfies that prime p is $p = 38s^4 + 4t^4 + u^4 + v^4 + w^4 + 24s^2t^2 - 12s^2u^2 + 12s^2v^2 + 12s^2w^2 - 4t^2u^2 + 4t^2v^2 + 4t^2w^2 - 2u^2v^2 - 2 \cdot u^2w^2 + 2v^2w^2$ $w.i.s.t.u.v.w.1$ and $p \equiv 3(mod\ 16)$ then, we are confronted with

$$rank(E_{-2(38s^4+4t^4+u^4+v^4+w^4+24s^2t^2-12s^2u^2+\cdots\cdots\cdots-2u^2v^2-2u^2w^2+2v^2w^2)}(Q)) = 1.$$

(3). In curve E_{-2p} assign the prime p as the form $p = 3s^4 + t^4 + u^4 + v^4 + w^4 + 2s^2t^2 - 2s^2u^2 + 2s^2v^2 + 2s^2w^2 - 2t^2u^2 + 2t^2v^2 + 2t^2w^2 - 2u^2v^2 - 2u^2w^2 + 2v^2w^2$ $w.i.s.t.u.v.w.1$ and $p \equiv 11(mod\ 16)$ then, we conclude that

$$rank(E_{-2(3s^4+t^4+u^4+v^4+w^4+2s^2t^2-2s^2u^2+\cdots\cdots\cdots-2u^2v^2-2u^2w^2+2v^2w^2)}(Q)) = 1.$$

Proof. (1). Four squares t^4 and u^4 and v^4 and w^4 are emerged in coefficient of e^4.

We are confronted with term $51s^4$ in coefficient of e^4, hence for accomplishing the square part we should note arithmetical value

$$-2M^4 + 51s^4e^4.$$

Denote $e = 1$ then, we got $-2M^4 + 51s^4$.

Wherefore, we can take $M = s$ since it yields the square term $49s^4$.

Under the selection of e and M in the above, we appoint that the components of N are $7s^2$, t^2, u^2, v^2, w^2.

Now our concern is above selection is matched to other terms in coefficient of e^4 or not.

There are remained the terms

$$14s^2t^2,\ 14s^2u^2,\ 14s^2v^2,\ 14s^2w^2 \text{ and}$$

$$2t^2u^2,\ 2t^2v^2,\ 2t^2w^2,\ 2u^2v^2,\ 2u^2w^2,\ 2v^2w^2.$$

The term $14s^2t^2$ is induced from $7s^2$, t^2.

$14s^2u^2$ is given from $7s^2$ and u^2.

We got $14s^2v^2$ from $7s^2$ and v^2.

Owing to $7s^2$ and w^2 there derived $14s^2w^2$.

In the next step, because of t^2 and u^2 there educed the term $2t^2u^2$.
By t^2 and v^2 we gain the term $2t^2v^2$.
The components t^2 and w^2 yields that $2t^2w^2$.
The components u^2 and v^2 deduces the term $2u^2v^2$.
Two components u^2 and w^2 educes that $2u^2w^2$.
v^2 and w^2 deduces the term $2v^2w^2$.
All remaining terms are gotten.
Now from the calculation

$$-2s^4 + 51s^4 + t^4 + u^4 + v^4 + w^4 + 14s^2t^2 + 14s^2u^2 + 14s^2v^2$$

$$+14s^2w^2 + 2t^2u^2 + 2t^2v^2 + 2t^2w^2 + 2u^2v^2 + 2u^2w^2 + 2v^2w^2$$

$$= 49s^4 + t^4 + u^4 + v^4 + w^4 + 14s^2t^2 + 14s^2u^2 + 14s^2v^2 +$$

$$14s^2w^2 + 2t^2u^2 + 2t^2v^2 + 2t^2w^2 + 2u^2v^2 + 2u^2w^2 + 2v^2w^2$$

the value N is given as

$$7s^2 + t^2 + u^2 + v^2 + w^2.$$

For this reason, the triple

$$(s, 1, 7s^2 + t^2 + u^2 + v^2 + w^2)$$

is derived as the solution of 4).
On that account, we get #α(Γ) = 4 and $r4.2$.
Eventually, we attain the consequence

$$rank(E_{-2(51s^4+t^4+u^4+v^4+w^4+14s^2t^2+14s^2u^2+\cdots\cdots\cdots+2u^2v^2+2u^2w^2+2v^2w^2)}(Q)) = 1.$$

(2). Squares $4t^4$, u^4, v^4, w^4 are shown in coefficient of e^4.
We should note numerical value

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

We appoint that $e = 1$.
Let $M = s$ then, the square term $36s^4$ is gotten.
Next, we consider other terms.
There are four negative terms as

$$-12s^2u^2, -4t^2u^2, -2u^2v^2 \text{ and } -2u^2w^2.$$

In these terms, there exists u^2.

Whence, we choose the components of N as $6s^2$, $2t^2$, $-u^2$, v^2, w^2.
Now this selection must be matched to other terms in prime p.
The remaining components are

$$24s^2t^2 \text{ and } 12s^2v^2 \text{ and } 12s^2w^2 \text{ and } 4t^2v^2 \text{ and } 4t^2w^2 \text{ and } 2v^2w^2.$$

We took $24s^2t^2$ from $6s^2$, $2t^2$.
The term $12s^2v^2$ from $6s^2$ and v^2.
Due to $6s^2$ and w^2 we got the term $12s^2w^2$.
Because of $2t^2$ and v^2 there educed that $4t^2v^2$.
From $2t^2$ and w^2 we obtain that $4t^2w^2$.
Terms v^2 and w^2 yields that $2v^2w^2$.
We checked all things.
Consequently, from the numeration

$$-2s^4 + 38s^4 + 4t^4 + u^4 + v^4 + w^4 + 24s^2t^2 - 12s^2u^2 + 12s^2v^2$$

$$+12s^2w^2 - 4t^2u^2 + 4t^2v^2 + 4t^2w^2 - 2u^2v^2 - 2u^2w^2 + 2v^2w^2$$

$$= 36s^4 + 4t^4 + u^4 + v^4 + w^4 + 24s^2t^2 - 12s^2u^2 + 12s^2v^2 +$$

$$12s^2w^2 - 4t^2u^2 + 4t^2v^2 + 4t^2w^2 - 2u^2v^2 - 2u^2w^2 + 2v^2w^2$$

the integer N is deduced as

$$6s^2 + 2t^2 - u^2 + v^2 + w^2.$$

On this account, there induced next triple as the solution of equation 4):

$$(s, 1, 6s^2 + 2t^2 - u^2 + v^2 + w^2).$$

And so there derived following conclusions:

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

As a result, we gain the consequence

$$rank(E_{-2(38t^4+4t^4+u^4+v^4+w^4+24s^2t^2-12s^2u^2+\cdots\cdots\cdots-2u^2w^2+2v^2w^2)}(Q)) = 1.$$

(3). The triple $(s, 1, s^2 + t^2 - u^2 + v^2 + w^2)$

satisfies the solution of 4).
It follows next conclusions:

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

Whence, we have the consequence

$$rank(E_{-2(3s^4+t^4+u^4+v^4+w^4+2s^2t^2-2s^2u^2+\cdots\cdots-2u^2v^2-2u^2w^2+2v^2w^2)}(Q)) = 1. \square$$

Primes p in the above are all $p \equiv 3, 11(mod\ 16)$. If $p \equiv 5, 13(mod\ 16)$ then, rank 1 also can be deduced. But the form p that is more than 3 terms, many cases the prime p is given as $p \equiv 3, 11(mod\ 16)$. We can guess of this in relating equation. This is not determined treatment. We just consider the things that we can approach. For $p \equiv 3, 11(mod\ 16)$ it is gotten as 4)$N^2 = -2M^4 + pe^4$ for Γ. Meanwhile for $p \equiv 5, 13(mod\ 16)$ it is 2)$N^2 = -M^4 + 2pe^4$ for Γ. Thereby, for equation 4) prime p exists independently. Namely, it only needs to coefficient -2 of M^4. Therefore, as in the above coefficient of s^4 can be odd in (1), (3) or even in (2). Whereas for the case of equation 2), p is involved to 2(coefficient of e^4) and -1 of M^4. Henceforth, the considerable factors are increased. In this p is difficult to be selected of odd coefficient of s^4 because 2 exists with prime p as a coefficient of e^4 if coefficient of s^4 is chosen as odd then, $2 \cdot odd$ is gotten and in calculation with $-M^4$ finding the solution became complex.

3 Examples

Here, we suggest examples of theorem 2.1(Primality was taken in [1]):

(p, s, t, u, v, w):

(4651, 3, 1, 1, 1, 1) and (8443, 3, 5, 1, 1, 1).

(p, s, t, u, v, w):

(83, 1, 1, 1, 1, 1) and (24659, 5, 1, 1, 1, 1).

(p, s, t, u, v, w):

(11, 1, 1, 1, 1, 1) and (283, 3, 1, 1, 1, 1) and (1979, 5, 1, 1, 1, 1, 1) and

(15131, 1, 11, 1, 1, 1) and (20011, 9, 1, 1, 1, 1) and (24571, 9, 5, 1, 1, 1) and

(141803, 13, 11, 1, 1, 1).

References

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

[2] A. Dujella, https://web.math.pmf.unizg.hr/~duje/tors/z1.html.

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

[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