International Journal of Algebra, Vol. 18, 2024, no. 4, 155 - 166
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2024.91917

Forms of Primes in Elliptic Curve $y^2 = x^3 - pqx$

Shin-Wook Kim

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

Abstract

Set E_{-pq} as an elliptic curve $y^2 = x^3 - pqx$ where p and q are distinct odd primes then, we will look into rank of it and compare with that of elliptic curve $y^2 = x^3 - px$.

Mathematics Subject Classification: 11A41, 11G05

Keywords: Primes, elliptic curve

1 Introduction

In [7], the author showed that rank of elliptic curve $y^2 = x^3 - pqx$ where p and q are such that $p = u^4 + 4v^4 + 38w^4 + 4u^2v^2 + 12u^2w^2 + 24v^2w^2$ and $q = u^4 + 4v^4 + 34w^4 + 4u^2v^2 + 12u^2w^2 + 24v^2w^2\ w.i.u.v.w.1$ and $p \equiv 3(mod\ 16)$ and $q \equiv 15(mod\ 16)$ and the case $p = 9u^4 + 4v^4 + 16w^4 + 14u^2v^2 + 24u^2w^2 + 16v^2w^2$ and $q = 9u^4 + 4v^4 + 16w^4 + 10u^2v^2 + 24u^2w^2 + 16v^2w^2\ w.i.u.v.w.1$ and $p \equiv 3(mod\ 16)$ and $q \equiv 15(mod\ 16)$ are both 2. In this article, we calculate rank of curve $y^2 = x^3 - pqx$ and compare the consequences with that of $y^2 = x^3 - px$.

Take E and $\bar{E}$ as elliptic curves $y^2 = x^3 + ax^2 + bx$ and $y^2 = x(x^2 - 2ax + a^2 - 4b)$. Put Γ as the set of rational points on E and $\bar{\Gamma}$ as the set of rational points on $\bar{E}$. Take $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ and $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ as relating equation for Γ and $\bar{\Gamma}$ in section 6 of Chapter III in [9] and [5] respectively. Next, we know that $2^r = \frac{\#\alpha(\Gamma)\#\bar{\alpha}(\bar{\Gamma})}{4}$ with rank r of E.

Let the notations be gotten as follows:

$w.i.c.d.f.g.h.i.j.k.l.s.t.u.v.w.z.1$: with integers c and d and f and g and h and i and j and k and l and s and t and u and v and w and z and $(c, d, f, g, h, i, j, k, l, s, t, u, v, w, z) = 1$([8]).

$w.i.s.t.u.1$: with integers s and t and u and $(s, t, u) = 1$([6]).

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

2 Calculation of Rank

Now we treat the rank of curve. By [5] and [4] it is enough that we only search the solutions of 3)$N^2 = pM^4 - qe^4$ for Γ and 5)$N^2 = 2pM^4 + 2qe^4$ for $\bar{\Gamma}$. $r4.4$ and $r4.2$ are in [5].

Theorem 2.1. (1). Set distinct odd primes p and q as $p = 51c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 + w^2 + z^2 + 14c^2d + 14c^2f +14c^2g + 14c^2h + 14c^2i + 14c^2j + 14c^2k + 14c^2l + 14c^2s + 14c^2t + 14c^2 \cdot u + 14c^2v + 14c^2w + 14c^2z + 2df + 2dg + 2dh + 2di + 2dj + 2dk + 2dl +2ds + 2dt + 2du + 2dv + 2dw + 2dz + 2fg + 2fh + 2fi + 2fj + 2fk + 2 \cdot fl + 2fs + 2ft + 2fu + 2fv + 2fw + 2fz + 2gh + 2gi + 2gj + 2gk + 2gl +2gs + 2gt + 2gu + 2gv + 2gw + 2gz + 2hi + 2hj + 2hk + 2hl + 2hs + 2h \cdot t + 2hu + 2hv + 2hw + 2hz + 2ij + 2ik + 2il + 2is + 2it + 2iu + 2iv + 2i \cdot w + 2iz + 2jk + 2jl + 2js + 2jt + 2ju + 2jv + 2jw + 2jz + 2kl + 2ks + 2kt +2ku + 2kv + 2kw + 2kz + 2ls + 2lt + 2lu + 2lv + 2lw + 2lz + 2st + 2su +2sv + 2sw + 2sz + 2tu + 2tv + 2tw + 2tz + 2uv + 2uw + 2uz + 2vw + 2 \cdot vz + 2wz$ and $q = 47c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 + w^2 + z^2 + 14c^2d + 14c^2f + 14c^2g + 14c^2h + 14c^2i + 14c^2j + 14 \cdot c^2k + 14c^2l + 14c^2s + 14c^2t + 14c^2u + 14c^2v + 14c^2w + 14c^2z + 2df + 2dg + 2dh + 2di + 2dj + 2dk + 2dl + 2ds + 2dt + 2du + 2dv + 2dw + 2dz +2fg + 2fh + 2fi + 2fj + 2fk + 2fl + 2fs + 2ft + 2fu + 2fv + 2fw + 2f \cdot z + 2gh + 2gi + 2gj + 2gk + 2gl + 2gs + 2gt + 2gu + 2gv + 2gw + 2gz +2hi + 2hj + 2hk + 2hl + 2hs + 2ht + 2hu + 2hv + 2hw + 2hz + 2ij + 2ik +2il + 2is + 2it + 2iu + 2iv + 2iw + 2iz + 2jk + 2jl + 2js + 2jt + 2ju + 2j \cdot v + 2jw + 2jz + 2kl + 2ks + 2kt + 2ku + 2kv + 2kw + 2kz + 2ls + 2lt + 2 \cdot lu + 2lv + 2lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2tu + 2tv + 2tw + 2tz + 2uv + 2uw + 2uz + 2vw + 2vz + 2wz$ $w.i.c.d.f.g.h.i.j.k.l.s.t.u.v.w.z.1$ and $p \equiv 11(mod\ 16)$ and $q \equiv 7(mod\ 16)$ in $E_{-pq}: y^2 = x^3 - pqx$ then, there derived that

$$rank(E_{-(51c^4+d^2+\cdots\cdots+z^2+\cdots\cdots+2vz+2wz)(47c^4+d^2+\cdots\cdots+z^2+\cdots\cdots+2vz+2wz)}(Q))$$

$$> rank(E_{-(2s^4t^4+10s^2t^2u^2+25u^4)}(Q))$$

where $E_{-p}: y^2 = x^3 - px$ is an elliptic curve with prime as $p = 2s^4t^4 + 10s^2t^2u^2 + 25u^4$ $w.i.s.t.u.1$ and $p \equiv 5(mod\ 16)$.

(2). Define the primes as $p = 27c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 + w^2 + z^2 - 10c^2d + 10c^2f + 10c^2g + 10c^2h + 10c^2i + 10c^2j + 10c^2k + 10c^2l + 10c^2s + 10c^2t + 10c^2u + 10c^2v + 10c^2w + 10c^2z - 2df - 2dg - 2dh - 2di - 2dj - 2dk - 2dl - 2ds - 2dt - 2du - 2dv - 2d \cdot w - 2dz + 2fg + 2fh + 2fi + 2fj + 2fk + 2fl + 2fs + 2ft + 2fu + 2fv + 2fw + 2fz + 2gh + 2gi + 2gj + 2gk + 2gl + 2gs + 2gt + 2gu + 2gv + 2g \cdot w + 2gz + 2hi + 2hj + 2hk + 2hl + 2hs + 2ht + 2hu + 2hv + 2hw + 2hz + 2ij + 2ik + 2il + 2is + 2it + 2iu + 2iv + 2iw + 2iz + 2jk + 2jl + 2js + 2jt + 2ju + 2jv + 2jw + 2jz + 2kl + 2ks + 2kt + 2ku + 2kv + 2kw + 2kz + 2ls + 2lt + 2lu + 2lv + 2lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2tu + 2tv + 2tw + 2tz + 2uv + 2uw + 2uz + 2vw + 2vz + 2wz$ and $q = 23c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 + w^2 + z^2 - 10c^2d + 10c^2f + 10c^2g + 10c^2h + 10c^2i + 10c^2j + 10c^2k + 10c^2l + 10c^2s + 10c^2t + 10c^2u + 10c^2v + 10c^2w + 10c^2z - 2df - 2dg - 2dh - 2di - 2dj - 2dk - 2dl - 2ds - 2dt - 2du - 2dv - 2dw - 2dz + 2fg + 2fh + 2fi + 2fj + 2f \cdot k + 2fl + 2fs + 2ft + 2fu + 2fv + 2fw + 2fz + 2gh + 2gi + 2gj + 2gk + 2gl + 2gs + 2gt + 2gu + 2gv + 2gw + 2gz + 2hi + 2hj + 2hk + 2hl + 2h \cdot s + 2ht + 2hu + 2hv + 2hw + 2hz + 2ij + 2ik + 2il + 2is + 2it + 2iu + 2i \cdot v + 2iw + 2iz + 2jk + 2jl + 2js + 2jt + 2ju + 2jv + 2jw + 2jz + 2kl + 2ks + 2kt + 2ku + 2kv + 2kw + 2kz + 2ls + 2lt + 2lu + 2lv + 2lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2tu + 2tv + 2tw + 2tz + 2uv + 2uw + 2uz + 2v \cdot w + 2vz + 2wz$ $w.i.c.d.f.g.h.i.j.k.l.s.t.u.v.w.z.1$ and $p \equiv 11(mod\ 16)$ and $q \equiv 7(mod\ 16)$ in $E_{-pq}: y^2 = x^3 - pqx$ then, there educed that

$$rank(E_{-(27c^4+d^2+\cdots\cdots+z^2+\cdots\cdots+2vz+2wz)(23c^4+d^2+\cdots\cdots+z^2+\cdots\cdots+2vz+2wz)}(Q))$$

$$> rank(E_{-(26s^4t^4+10s^2t^2u^2+u^4)}(Q))$$

where the curve $E_{-p}: y^2 = x^3 - px$ satisfies that $p = 26s^4t^4 + 10s^2t^2u^2 + u^4$ $w.i.s.t.u.1$ and $p \equiv 5(mod\ 16)$.

(3). Denote primes as $p = 83u^4 + v^4 + w^4 + 18u^2v^2 - 18u^2w^2 - 2v^2w^2$ and $q = 79u^4 + v^4 + w^4 + 18u^2v^2 - 18u^2w^2 - 2v^2w^2$ $w.i.u.v.w.1$ and $p \equiv 3(mod\ 16)$ and $q \equiv 15(mod\ 16)$ in $E_{-pq}: y^2 = x^3 - pqx$ then, it follows that

$$rank(E_{-(83u^4+v^4+w^4+\cdots\cdots-2v^2w^2)(79u^4+v^4+w^4+\cdots\cdots-2v^2w^2)}(Q))$$

$$> rank(E_{-(106u^4+90u^2v^2+81v^4)}(Q))$$

where the curve $E_{-p}: y^2 = x^3 - px$ satisfies that $p = 106u^4 + 90u^2v^2 + 81v^4$ with integers u and v and $(u, v) = 1$ and $p \equiv 5(mod\ 16)$.

Proo$f$. (1). In equation 3) for Γ if we take 1 into both M and e then, we confront to

$$(51c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 + w^2 +$$

$$z^2 + 14c^2d + 14c^2f + 14c^2g + 14c^2h + 14c^2i + 14c^2j + 14c^2k + 14c^2l +$$

$$14c^2s + 14c^2t + 14c^2u + 14c^2v + 14c^2w + 14c^2z + 2df + 2dg + 2dh + 2d$$

$$\cdot i + 2dj + 2dk + 2dl + 2ds + 2dt + 2du + 2dv + 2dw + 2dz + 2fg + 2fh$$

$$+2fi + 2fj + 2fk + 2fl + 2fs + 2ft + 2fu + 2fv + 2fw + 2fz + 2gh + 2g$$

$$\cdot i + 2gj + 2gk + 2gl + 2gs + 2gt + 2gu + 2gv + 2gw + 2gz + 2hi + 2hj +$$

$$2hk + 2hl + 2hs + 2ht + 2hu + 2hv + 2hw + 2hz + 2ij + 2ik + 2il + 2is +$$

$$2it + 2iu + 2iv + 2iw + 2iz + 2jk + 2jl + 2js + 2jt + 2ju + 2jv + 2jw + 2j$$

$$\cdot z + 2kl + 2ks + 2kt + 2ku + 2kv + 2kw + 2kz + 2ls + 2lt + 2lu + 2lv + 2$$

$$\cdot lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2tu + 2tv + 2tw + 2tz + 2uv +$$

$$2uw + 2uz + 2vw + 2vz + 2wz) - (47c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2$$

$$+l^2 + s^2 + t^2 + u^2 + v^2 + w^2 + z^2 + 14c^2d + 14c^2f + 14c^2g + 14c^2h + 14$$

$$\cdot c^2i + 14c^2j + 14c^2k + 14c^2l + 14c^2s + 14c^2t + 14c^2u + 14c^2v + 14c^2w +$$

$$14c^2z + 2df + 2dg + 2dh + 2di + 2dj + 2dk + 2dl + 2ds + 2dt + 2du + 2$$

$$\cdot dv + 2dw + 2dz + 2fg + 2fh + 2fi + 2fj + 2fk + 2fl + 2fs + 2ft + 2fu$$

$$+2fv + 2fw + 2fz + 2gh + 2gi + 2gj + 2gk + 2gl + 2gs + 2gt + 2gu + 2$$

$$\cdot gv + 2gw + 2gz + 2hi + 2hj + 2hk + 2hl + 2hs + 2ht + 2hu + 2hv + 2hw$$

$+2hz + 2ij + 2ik + 2il + 2is + 2it + 2iu + 2iv + 2iw + 2iz + 2jk + 2jl + 2j$

$\cdot s + 2jt + 2ju + 2jv + 2jw + 2jz + 2kl + 2ks + 2kt + 2ku + 2kv + 2kw + 2$

$\cdot kz + 2ls + 2lt + 2lu + 2lv + 2lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2$

$\cdot tu + 2tv + 2tw + 2tz + 2uv + 2uw + 2uz + 2vw + 2vz + 2wz) = 4c^4.$

Accordingly, we gain $(1, 1, 2c^2)$ as the solution of equation.
Thus, it follows that $\#\alpha(\Gamma) = 4$.
Next, equation 5) for $\bar{\Gamma}$ is given as

$N^2 = 2(51c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 +$

$w^2 + z^2 + 14c^2d + 14c^2f + 14c^2g + 14c^2h + 14c^2i + 14c^2j + 14c^2k + 14$

$\cdot c^2l + 14c^2s + 14c^2t + 14c^2u + 14c^2v + 14c^2w + 14c^2z + 2df + 2dg + 2d$

$\cdot h + 2di + 2dj + 2dk + 2dl + 2ds + 2dt + 2du + 2dv + 2dw + 2dz + 2fg$

$+2fh + 2fi + 2fj + 2fk + 2fl + 2fs + 2ft + 2fu + 2fv + 2fw + 2fz + 2g$

$\cdot h + 2gi + 2gj + 2gk + 2gl + 2gs + 2gt + 2gu + 2gv + 2gw + 2gz + 2hi$

$+2hj + 2hk + 2hl + 2hs + 2ht + 2hu + 2hv + 2hw + 2hz + 2ij + 2ik + 2il$

$+2is + 2it + 2iu + 2iv + 2iw + 2iz + 2jk + 2jl + 2js + 2jt + 2ju + 2jv + 2j$

$\cdot w + 2jz + 2kl + 2ks + 2kt + 2ku + 2kv + 2kw + 2kz + 2ls + 2lt + 2lu + 2$

$\cdot lv + 2lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2tu + 2tv + 2tw + 2tz +$

$2uv + 2uw + 2uz + 2vw + 2vz + 2wz)M^4 + 2(47c^4 + d^2 + f^2 + g^2 + h^2 +$

$i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 + w^2 + z^2 + 14c^2d + 14c^2f + 14c^2g +$

$14c^2h + 14c^2i + 14c^2j + 14c^2k + 14c^2l + 14c^2s + 14c^2t + 14c^2u + 14c^2v$

$+14c^2w + 14c^2z + 2df + 2dg + 2dh + 2di + 2dj + 2dk + 2dl + 2ds + 2dt$

$+2du + 2dv + 2dw + 2dz + 2fg + 2fh + 2fi + 2fj + 2fk + 2fl + 2fs + 2$

$\cdot ft + 2fu + 2fv + 2fw + 2fz + 2gh + 2gi + 2gj + 2gk + 2gl + 2gs + 2gt$

$+2gu + 2gv + 2gw + 2gz + 2hi + 2hj + 2hk + 2hl + 2hs + 2ht + 2hu + 2h$

$\cdot v + 2hw + 2hz + 2ij + 2ik + 2il + 2is + 2it + 2iu + 2iv + 2iw + 2iz + 2jk$

$+2jl + 2js + 2jt + 2ju + 2jv + 2jw + 2jz + 2kl + 2ks + 2kt + 2ku + 2kv +$

$2kw + 2kz + 2ls + 2lt + 2lu + 2lv + 2lw + 2lz + 2st + 2su + 2sv + 2sw +$

$2sz + 2tu + 2tv + 2tw + 2tz + 2uv + 2uw + 2uz + 2vw + 2vz + 2wz)e^4.$

There are terms $102c^4$ and $94c^4$ in each coefficient of M^4 and e^4.
Whence, we can anticipate an appearance of square $196c^4$.
And there are terms from $2d^2$ to $2z^2$ in each coefficient, hence we can consider the squares $4d^2$ and $4f^2$ and $4g^2$ and $4h^2$ and $4i^2$ and $4j^2$ and $4k^2$ and $4l^2$ and $4s^2$ and $4t^2$ and $4u^2$ and $4v^2$ and $4w^2$ and $4z^2$ after taking the values M and e.
Thus, we choose the components of value N as $14c^2$ and $2d$ and $2f$ and $2g$ and $2h$ and $2i$ and $2j$ and $2k$ and $2l$ and $2s$ and $2t$ and $2u$ and $2v$ and $2w$ and 2z.
Now by taking a pair from$14c^2$ to others in each case the terms $56c^2d$ and $56c^2f$ and $56c^2g$ and $56c^2h$ and $56c^2i$ and $56c^2j$ and $56c^2k$ and $56c^2l$ and $56c^2s$ and $56c^2t$ and $56c^2u$ and $56c^2v$ and $56c^2w$ and $56c^2z$ can be given.
Lastly, from doing a pair in $2d$ and $2f$ and $2g$ and $2h$ and $2i$ and $2j$ and $2k$ and $2l$ and $2s$ and $2t$ and $2u$ and $2v$ and $2w$ and 2z in each case we can obtain other terms from $8df$ to $8wz$.
And all above treatment can be done under the hypothesis $M = e = 1$.
Wherefore, the triple

$$(1, 1, 14c^2 + 2d + 2f + 2g + 2h + 2i + 2j + 2k + 2l + 2s + 2t + 2u +$$

$$2v + 2w + 2z)$$

satisfies the solution of equation.
Hence, we take the conclusion $\#\bar{\alpha}(\bar{\Gamma}) = 4$ and it derives that $r4.4$.
Consequentially, we obtain that

$$rank(E_{-(51c^4+d^2+\cdots\cdots+3z^2+\cdots\cdots+2wz)(47c^4+d^2+\cdots\cdots-z^2+\cdots\cdots+2wz)}(Q)) = 2.$$

In the next step, we regard the rank of curve E_{-p} .
If the solution of equation

$$2)N^2 = -M^4 + (2s^4t^4 + 10s^2t^2u^2 + 25u^4)e^4$$

for Γ is appeared then, computation of rank is done by [3].
Assume that $M = st$ and $e = 1$ then, we gain

$$-(st)^4 + 2s^4t^4 + 10s^2t^2u^2 + 25u^4$$

$$= s^4t^4 + 10s^2t^2u^2 + 25u^4.$$

On that account, the solution is derived as $(st,\, 1,\, s^2t^2 + 5u^2)$.
On this account, we take both $\#\alpha(\Gamma) = 4$ and $r4.2$ and so the result

$$rank(E_{-(2s^4t^4+10s^2t^2u^2+25u^4)}(Q)) = 1$$

is deduced.
(2). In 3) for Γ we set both M and e as 1 then, we gain

$$(27c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 + w^2 +$$

$$z^2 - 10c^2d + 10c^2f + 10c^2g + 10c^2h + 10c^2i + 10c^2j + 10c^2k + 10c^2l +$$

$$10c^2s + 10c^2t + 10c^2u + 10c^2v + 10c^2w + 10c^2z - 2df - 2dg - 2dh - 2$$

$$\cdot di - 2dj - 2dk - 2dl - 2ds - 2dt - 2du - 2dv - 2dw - 2dz + 2fg + 2fh$$

$$+2fi + 2fj + 2fk + 2fl + 2fs + 2ft + 2fu + 2fv + 2fw + 2fz + 2gh + 2g$$

$$\cdot i + 2gj + 2gk + 2gl + 2gs + 2gt + 2gu + 2gv + 2gw + 2gz + 2hi + 2hj +$$

$$2hk + 2hl + 2hs + 2ht + 2hu + 2hv + 2hw + 2hz + 2ij + 2ik + 2il + 2is +$$

$$2it + 2iu + 2iv + 2iw + 2iz + 2jk + 2jl + 2js + 2jt + 2ju + 2jv + 2jw + 2j$$

$$\cdot z + 2kl + 2ks + 2kt + 2ku + 2kv + 2kw + 2kz + 2ls + 2lt + 2lu + 2lv + 2$$

$$\cdot lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2tu + 2tv + 2tw + 2tz + 2uv +$$

$$2uw + 2uz + 2vw + 2vz + 2wz) - (23c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2$$

$$+l^2 + s^2 + t^2 + u^2 + v^2 + w^2 + z^2 - 10c^2d + 10c^2f + 10c^2g + 10c^2h + 10$$

$$\cdot c^2i + 10c^2j + 10c^2k + 10c^2l + 10c^2s + 10c^2t + 10c^2u + 10c^2v + 10c^2w +$$

$$10c^2z - 2df - 2dg - 2dh - 2di - 2dj - 2dk - 2dl - 2ds - 2dt - 2du - 2$$

$$\cdot dv - 2dw - 2dz + 2fg + 2fh + 2fi + 2fj + 2fk + 2fl + 2fs + 2ft + 2fu$$

$$+2fv + 2fw + 2fz + 2gh + 2gi + 2gj + 2gk + 2gl + 2gs + 2gt + 2gu + 2$$

$$\cdot gv + 2gw + 2gz + 2hi + 2hj + 2hk + 2hl + 2hs + 2ht + 2hu + 2hv + 2hw$$

$+2hz + 2ij + 2ik + 2il + 2is + 2it + 2iu + 2iv + 2iw + 2iz + 2jk + 2jl + 2j$

$\cdot s + 2jt + 2ju + 2jv + 2jw + 2jz + 2kl + 2ks + 2kt + 2ku + 2kv + 2kw + 2$

$\cdot kz + 2ls + 2lt + 2lu + 2lv + 2lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2$

$\cdot tu + 2tv + 2tw + 2tz + 2uv + 2uw + 2uz + 2vw + 2vz + 2wz) = 4c^4.$

For that reason, we have (1, 1, $2c^2$) as the solution of above equation.
So it deduces that $\#\alpha(\Gamma) = 4$.
In the next step, equation 5) for $\bar{\Gamma}$ is $N^2 = 2(27c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 + w^2 + z^2 - 10c^2d + 10c^2f + 10c^2g + 10 \cdot c^2h + 10c^2i + 10c^2j + 10c^2k + 10c^2l + 10c^2s + 10c^2t + 10c^2u + 10c^2v + 10c^2w + 10c^2z - 2df - 2dg - 2dh - 2di - 2dj - 2dk - 2dl - 2ds - 2dt - 2du - 2dv - 2dw - 2dz + 2fg + 2fh + 2fi + 2fj + 2fk + 2fl + 2fs + 2ft +2fu + 2fv + 2fw + 2fz + 2gh + 2gi + 2gj + 2gk + 2gl + 2gs + 2gt + 2 \cdot gu + 2gv + 2gw + 2gz + 2hi + 2hj + 2hk + 2hl + 2hs + 2ht + 2hu + 2hv +2hw + 2hz + 2ij + 2ik + 2il + 2is + 2it + 2iu + 2iv + 2iw + 2iz + 2jk + 2 \cdot jl + 2js + 2jt + 2ju + 2jv + 2jw + 2jz + 2kl + 2ks + 2kt + 2ku + 2kv + 2 \cdot kw + 2kz + 2ls + 2lt + 2lu + 2lv + 2lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2tu + 2tv + 2tw + 2tz + 2uv + 2uw + 2uz + 2vw + 2vz + 2wz)M^4 + 2(23c^4 + d^2 + f^2 + g^2 + h^2 + i^2 + j^2 + k^2 + l^2 + s^2 + t^2 + u^2 + v^2 + w^2 + z^2 - 10c^2d + 10c^2f + 10c^2g + 10c^2h + 10c^2i + 10c^2j + 10c^2k + 10c^2l + 10c^2s + 10c^2t + 10c^2u + 10c^2v + 10c^2w + 10c^2z - 2df - 2dg - 2dh - 2d \cdot i - 2dj - 2dk - 2dl - 2ds - 2dt - 2du - 2dv - 2dw - 2dz + 2fg + 2fh +2fi + 2fj + 2fk + 2fl + 2fs + 2ft + 2fu + 2fv + 2fw + 2fz + 2gh + 2g \cdot i + 2gj + 2gk + 2gl + 2gs + 2gt + 2gu + 2gv + 2gw + 2gz + 2hi + 2hj + 2hk + 2hl + 2hs + 2ht + 2hu + 2hv + 2hw + 2hz + 2ij + 2ik + 2il + 2is + 2it + 2iu + 2iv + 2iw + 2iz + 2jk + 2jl + 2js + 2jt + 2ju + 2jv + 2jw + 2j \cdot z + 2kl + 2ks + 2kt + 2ku + 2kv + 2kw + 2kz + 2ls + 2lt + 2lu + 2lv + 2 \cdot lw + 2lz + 2st + 2su + 2sv + 2sw + 2sz + 2tu + 2tv + 2tw + 2tz + 2uv + 2uw + 2uz + 2vw + 2vz + 2wz)e^4.$

On account of terms $54c^4$ and $46c^4$ in coefficient of M^4 and e^4 we can anticipate an appearance of $100c^4$.
Next, there are terms from $2d^2$ to $2z^2$ in coefficient of M^4 and e^4.
So the squares $4d^2$ and $4f^2$ and $4g^2$ and $4h^2$ and $4i^2$ and $4j^2$ and $4k^2$ and $4l^2$ and $4s^2$ and $4t^2$ and $4u^2$ and $4v^2$ and $4w^2$ and $4z^2$ can be given.
Next, there are negative terms $-20c^2d$ and $-4df$ and $-4dg$ and $-4dh$ and $-4di$ and $-4dj$ and $-4dk$ and $-4dl$ and $-4ds$ and $-4dt$ and $-4du$ and $-4dv$ and $-4dw$ and $-4dz$ in both coefficients of M^4 and e^4. The common variable of these is d.
Thus, we select the components of integer N as $10c^2$ and $-2d$ and $2f$ and $2g$ and $2h$ and $2i$ and $2j$ and $2k$ and $2l$ and $2s$ and $2t$ and $2u$ and $2v$ and $2w$ and $2z$.

Namely, it is gotten as $N = 10c^2 - 2d + 2f + 2g + 2h + 2i + 2j + 2k + 2l + 2s + 2t + 2u + 2v + 2w + 2z$.

Now remaining terms in coefficients of M^4 and e^4 can be induced from the computation.

Wherefore, we take the solution as $(1,\ 1,\ 10c^2 - 2d + 2f + 2g + 2h + 2i + 2j + 2k + 2l + 2s + 2t + 2u + 2v + 2w + 2z)$.

Thereby, it follows the conclusion $\#\bar{\alpha}(\bar{\Gamma}) = 4$.

Whence, it deduces that $r4.4$.

So we gain $rank(E_{-(27c^4+d^2+\cdots\cdots+z^2+\cdots\cdots+2wz)(23c^4+d^2+\cdots\cdots+z^2+\cdots\cdots+2wz)}(Q)) = 2$.

Next, we investigate rank of curve E_{-p}.

There is remained only equation

$$2)N^2 = -M^4 + (26s^4t^4 + 10s^2t^2u^2 + u^4)e^4$$

for Γ that is necessary to investigate the solvability from [3].

Suppose that $M = st$ and $e = 1$ then, we have that

$$-(st)^4 + 26s^4t^4 + 10s^2t^2u^2 + u^4$$

$$= 25s^4t^4 + 10s^2t^2u^2 + u^4.$$

For this reason, we get the triple

$$(st,\ 1,\ 5s^2t^2 + u^2)$$

as the solution of equation.

And so there comes that $\#\alpha(\Gamma) = 4$ and $r4.2$.

Thus, next result is gotten:

$$rank(E_{-(26s^4t^4+10s^2t^2u^2+u^4)}(Q)) = 1.$$

(3). Relating equations are $3)N^2 = (83u^4 + v^4 + w^4 + 18u^2v^2 - 18u^2w^2 - 2v^2w^2)M^4 - (79u^4 + v^4 + w^4 + 18u^2v^2 - 18u^2w^2 - 2v^2w^2)e^4$ for Γ and $5)N^2 = 2(83u^4 + v^4 + w^4 + 18u^2v^2 - 18u^2w^2 - 2v^2w^2)M^4 + 2(79u^4 + v^4 + w^4 + 18u^2v^2 - 18u^2w^2 - 2v^2w^2)e^4$ for $\bar{\Gamma}$.

The triples $(1, 1, 2u^2)$ and $(1, 1, 18u^2 + 2v^2 - 2w^2)$ satisfy the solution of 3) and 5) respectively.

Thereby, we acquire that $\#\alpha(\Gamma) = \#\bar{\alpha}(\bar{\Gamma}) = 4$.

Hence, it derives $r4.4$ and so it comes that

$$rank(E_{-(83u^4+v^4+w^4+\cdots\cdots-2v^2w^2)(79u^4+v^4+w^4+\cdots\cdots-2v^2w^2)}(Q)) = 2.$$

In addition, from [3] we take that $rank(E_{-(106u^4+90u^2v^2+81v^4)}(Q)) = 1$.

Thus, we achieved the proof of (3). □

In above we got the rank 2 in $y^2 = x^3 - pqx$. In curve $y^2 = x^3 + pqx$ we can obtain rank at least 2 where primes are the forms as more than 8 variables and 40 terms. In detail, we can attain the primes as the forms $p = (\ )A^2 + (\ )B^2 + (\ )C^2 + (\ )D^2 + (\ )F^2 + (\ )G^2 + (\ )H^2 + (\ )I^2 + (\ )J^2 + (\ )AB + (\ )AC + (\ )AD + (\ )AF + (\ )AG + (\ )AH + (\ )AI + (\ )AJ + (\ )BC + (\ )BD + (\ )BF + (\ )BG + (\ )BH + (\ )BI + (\ )BJ + (\ )CD + (\ )CF + (\ )CG + (\ )CH + (\ )CI + (\ )CJ + (\ )DF + (\ )DG + (\ )DH + (\ )DI + (\ )DJ + (\ )FG + (\ )FH + (\ )FI + (\ )FJ + (\ )GH + (\ )GI + (\ )GJ + (\ )HI + (\ )HJ + (\ )IJ$ and $q = (\ )A^2 + (\ )B^2 + (\ )C^2 + (\ )D^2 + (\ )F^2 + (\ )G^2 + (\ )H^2 + (\ )I^2 + (\ )J^2 + (\ )AB + (\ )AC + (\ )AD + (\ )AF + (\ )AG + (\ )AH + (\ )AI + (\ )AJ + (\ )BC + (\ )BD + (\ )BF + (\ )BG + (\ )BH + (\ )BI + (\ )BJ + (\ )CD + (\ )CF + (\ )CG + (\ )CH + (\ )CI + (\ )CJ + (\ )DF + (\ )DG + (\ )DH + (\ )DI + (\ )DJ + (\ )FG + (\ )FH + (\ )FI + (\ )FJ + (\ )GH + (\ )GI + (\ )GJ + (\ )HI + (\ )HJ + (\ )IJ$ $w.i.A.B.C.D.F.G.H.I.J.1$ where $w.i.A.B.C.D.F.G.H.I.J.1$ denotes with integers A and B and C and D and F and G and H and I and J and $(A, B, C, D, F, G, H, I, J) = 1$.

Remark 2.2. In above $y^2 = x^3 - px$ we confront to the form of prime $p = Hs^4t^4 + Is^2t^2u^2 + Ku^4$. It is different from general form of prime $p = Hu^4 + Iu^2v^2 + Kv^4$.

Remark 2.3. In [2], the author treated rank of $y^2 = x^3 + 4px$ where prime is $p = t^4 + 16$(t is an odd integer) and $p \equiv 1 (mod\ 8)$ is 2. Searching other cases of rank 2 in $y^2 = x^3 + 4px$ is not simple. Since the coefficient 4 is exponent of 2 it is different from considering the rank of $y^2 = x^3 - pqx$.

3 Examples

In section 3, we treat examples of previous theorem.

The primality was taken by [1].

Now we submit examples from theorem 2.1(1) to (3):

$(p, q, c, d, f, g, h, i, j, k, l, s, t, u, v, w, z)$:

(443, 439, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) and

(56171, 56167, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 217);

(p, s, t, u):

(37, 1, 1, 1) and (277, 3, 1, 1) and (15877, 1, 1, 5) and (428864197, 11, 11, 1).

$(p, q, c, d, f, g, h, i, j, k, l, s, t, u, v, w, z)$:

(443, 439, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 5) and

(13691, 13687, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 101);

(p, s, t, u):

(37, 1, 1, 1) and (197, 1, 1, 3) and (15877, 1, 1, 11).

(p, q, u, v, w):

(83, 79, 1, 1, 1) and (93187, 92863, 3, 15, 1).

References

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

[2] 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

[3] 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/ija.2018.8934

[4] 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

[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 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

[7] S. W. Kim, Distinct primes in elliptic curve $y^2 = x^3 - pqx$, *Int. J. of Algebra,* **18** (2024), 41-48. https://doi.org/10.12988/ija.2024.91854

[8] S. W. Kim Compositions of distinct primes in elliptic curve $y^2 = x^3 - pqx$, *Int. J. of Algebra*, **18** (2024), 105-116. https://doi.org/10.12988/ija.2024.91862

[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: November 1, 2024; Published: November 28, 2024