International Mathematical Forum, Vol. 21, 2026, no. 1, 73 - 78
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/imf.2026.914568

Parity Primes in Elliptic Curves

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

Parity primes p_1 and p_2 were defined as $p_1 = Hu^4 + Iu^2v^2 + Kv^4$ and $p_2 = Hu^4 - Iu^2v^2 + Kv^4$ in [7]. We shall treat it in elliptic curves $E_{-2p}: y^2 = x^3 - 2px$ and $E_{-4p}: y^2 = x^3 - 4px$ and $E_{-3p}: y^2 = x^3 - 3px$.

Mathematics Subject Classification: 11A41, 11G05

Keywords: Parity primes, elliptic curve

1 Introduction

In [7], the author defined parity primes. The reason that we treat the parity primes in elliptic curves is due to convenience. Only just changing one symbol of term for u^2v^2 we can get more results of rank 1. The crucial thing in this treatment is searching the examples. In theoretical, we can get various results of parity primes in elliptic curves. But the significant thing is submitting examples. Namely, we pursue some values u and v that satisfy the primes $p_1 = Hu^4 + Iu^2v^2 + Kv^4$ and $p_2 = Hu^4 - Iu^2v^2 + Kv^4$ simultaneously. In this article, we will apply parity primes to several forms of elliptic curves. Namely, we shall treat parity primes in elliptic curves $E_{-2p}: y^2 = x^3 - 2px$ and $E_{-4p}: y^2 = x^3 - 4px$ and $E_{-3p}: y^2 = x^3 - 3px$ where the forms are $p = Hu^4 \pm Iu^2v^2 + Kv^4$. It is sufficient that we only find the solutions of relating equations for Γ as $4) N^2 = -2M^4 + pe^4$ in E_{-2p} and for Γ as $6) N^2 = -4M^4 + pe^4$ in curve E_{-4p} for $\bar{\Gamma}$ as $6) N^2 = 12M^4 + pe^4$ in curve E_{-3p} on account of [3] and [2], [6] and [5]. Several notations $w.i.u.v.1$ and $r4.2$ and $r2.4$ are in [4]. Moreover, we define parity primes as $p.p.$

2 Parity primes in E_{-2p} and E_{-4p} and E_{-3p}

Now we regard parity primes in curves.

Theorem 2.1. (1). If p_1 and p_2 are $p.p$ as $p_1 = 6u^4 + 4u^2v^2 + v^4\ w.i.u.v.1$, $p_1 \equiv 11(mod\ 16)$ and $p_2 = 6u^4 - 4u^2v^2 + v^4\ \ w.i.u.v.1$, $p_2 \equiv 3(mod\ 16)$ in E_{-2p} then, we have that

$$rank(E_{-2(6u^4 \pm 4u^2v^2 + v^4)}(Q)) = 1.$$

(2). Set p_1 and p_2 as $p.p$ such that $p_1 = 38u^4 + 12u^2v^2 + v^4\ w.i.u.v.1$, $p_1 \equiv 3(mod\ 16)$ and $p_2 = 38u^4 - 12u^2v^2 + v^4\ \ w.i.u.v.1$, $p_2 \equiv 11(mod\ 16)$ in E_{-2p} then, there comes that

$$rank(E_{-2(38u^4 \pm 12u^2v^2 + v^4)}(Q)) = 1.$$

(3). If p_1 and p_2 are $p.p$ as the forms $p_1 = 1229u^4 + 140u^2v^2 + 4v^4\ w.i.u.v.1$ and $p_1 \equiv 13(mod\ 16)$ and $p_2 = 1229u^4 - 140u^2v^2 + 4v^4$ $w.i.u.v.1$, $p_2 \equiv 5(mod\ 16)$ in E_{-4p} then, we attain that

$$rank(E_{-4(1229u^4 \pm 140u^2v^2 + 4v^4)}(Q)) = 1.$$

(4). If p_1 and p_2 are $p.p$ as the forms $p_1 = 5u^4 + 4u^2v^2 + 4v^4\ w.i.u.v.1$and $p_1 \equiv 13(mod\ 16)$ and $p_2 = 5u^4 - 4u^2v^2 + 4v^4\ w.i.u.v.1$, $p_2 \equiv 5(mod\ 16)$ in E_{-4p} then, we attain that

$$rank(E_{-4(5u^4 \pm 4u^2v^2 + 4v^4)}(Q)) = 1.$$

(5). If p_1 and p_2 are $p.p$ such that $p_1 = 13u^4 + 12u^2v^2 + 4v^4\ w.i.u.v.1$and $p_1 \equiv 13(mod\ 16)$ and $p_2 = 13u^4 - 12u^2v^2 + 4v^4\ \ \ w.i.u.v.1$, $p_2 \equiv 5(mod\ 16)$ in E_{-4p} then, we acquire that

$$rank(E_{-4(13u^4 \pm 12u^2v^2 + 4v^4)}(Q)) = 1.$$

(6). Take p_1 and p_2 as $p.p$ such that $p_1 = 13u^4 + 20u^2v^2 + 4v^4\ w.i.u.v.1$and $p_1 \equiv 5(mod\ 16)$ and $p_2 = 13u^4 - 20u^2v^2 + 4v^4\ \ \ w.i.u.v.1$, $p_2 \equiv 13(mod\ 16)$ in E_{-3p} then, the following result is induced:

$$rank(E_{-3(13u^4 \pm 20u^2v^2 + 4v^4)}(Q)) = 1.$$

Proo$f$. (1). We should find the solutions of equations

$$4)N^2 = -2M^4 + (6u^4 \pm 4u^2v^2 + v^4)e^4 \text{ for } \Gamma.$$

The triples $(u, 1, 2u^2 \pm v^2)$ satisfies the solutions of equations.
Therefore, we reach the conclusion $r4.2$.
Henceforth, we complete the proof.
(2). Now it is sufficient that we only find the solutions of

$$4)N^2 = -2M^4 + (38u^4 \pm 12u^2v^2 + v^4)e^4 \text{ for } \Gamma.$$

Taking $M = u$ and $e = 1$ then, we are confronted with

$$-2u^4 + 38u^4 \pm 12u^2v^2 + v^4$$

$$= 36u^4 \pm 12u^2v^2 + v^4.$$

Thus, the triple $(u, 1, 6u^2 \pm v^2)$ satisfies the solution.
Accordingly, we gain $r4.2$.
Therefore, we accomplish the proof.
(3). There are equations

$$6)N^2 = -4M^4 + (1229u^4 \pm 140u^2v^2 + 4v^4)e^4 \text{ for } \Gamma.$$

Taking M and e as u and 1 yields that

$$-4u^4 + 1229u^4 \pm 140u^2v^2 + 4v^4$$

$$= 1225u^4 \pm 140u^2v^2 + 4v^4.$$

Accordingly, we get the solution as $(u, 1, 35u^2 \pm 2v^2)$.
Hence, we take that $r4.2$.
Thereby, the proof is done.
(4). Relating equations are given as

$$6)N^2 = -4M^4 + (5u^4 + 4u^2v^2 + 4v^4)e^4 \text{ for } \Gamma \text{ and}$$

$$6)N^2 = -4M^4 + (5u^4 - 4u^2v^2 + 4v^4)e^4 \text{ for } \Gamma.$$

Set M and e as u and 1 then, it implies that

$$-4u^4 + 5u^4 + 4u^2v^2 + 4v^4$$

$$= u^4 + 4u^2v^2 + 4v^4 \text{ and}$$

$$-4u^4 + 5u^4 - 4u^2v^2 + 4v^4$$

$$= u^4 - 4u^2v^2 + 4v^4.$$

Accordingly, we gain the solution as $(u, 1, u^2 \pm 2v^2)$.
Hence, we take that $r4.2$.
Thereby, the proof is done.
(5). We face equations

$$6)N^2 = -4M^4 + (13u^4 + 12u^2v^2 + 4v^4)e^4 \text{ for } \Gamma \text{ and}$$

$$6)N^2 = -4M^4 + (13u^4 - 12u^2v^2 + 4v^4)e^4 \text{ for } \Gamma.$$

Taking M and e as u and 1 then, we obtain that

$$-4u^4 + 13u^4 + 12u^2v^2 + 4v^4$$

$$= 9u^4 + 12u^2v^2 + 4v^4 \text{ and}$$

$$-4u^4 + 13u^4 - 12u^2v^2 + 4v^4$$

$$= 9u^4 - 12u^2v^2 + 4v^4.$$

Whence, the triples $(u, 1, 3u^2 \pm 2v^2)$ are derived as the solutions.
Thus, we get the conclusion $r4.2$.
And it finishes the proof.
(6). We confront to equations

$$6)N^2 = 12M^4 + (13u^4 + 20u^2v^2 + 4v^4)e^4 \text{ for } \bar{\Gamma} \text{ and}$$

$$6)N^2 = 12M^4 + (13u^4 - 20u^2v^2 + 4v^4)e^4 \text{ for } \bar{\Gamma}.$$

Assume that $M = e = 1$ then, we get that

$$12u^4 + 13u^4 + 20u^2v^2 + 4v^4$$

$$= 25u^4 + 20u^2v^2 + 4v^4 \text{ and}$$

$$12u^4 + 13u^4 - 20u^2v^2 + 4v^4$$

$$= 25u^4 - 20u^2v^2 + 4v^4.$$

Henceforth, we took the solutions as $(u, 1, 5u^2 \pm 2v^2)$.
Therefore, the conclusion $r2.4$ is given.
For this reason, the proof became completed. □

From above we checked that parity primes are valid in E_{-2p} and E_{-4p} and E_{-3p}. The bigness of coefficients in H and I and K are less than 10000 in the above. It is small in relative. We can obtain more results of parity primes in curve E_{-2p}.

Remark 2.2. It doesn't yest found parity primes in curves $E_{-p}: y^2 = x^3 - px$ and $E_{-5p}: y^2 = x^3 - 5px$.

3 Examples

Now we suggest examples as follows:(Primality was checked in [1])

(p_1, u, v): (11, 1, 1) and (48091, 9, 5).
(p_2, u, v): (3, 1, 1) and (31891, 9, 5).

(p_1, u, v): (3187, 3, 1) and (680531, 11, 9).
(p_2, u, v): (2971, 3, 1) and (445307, 11, 9).

(p_1, u, v): (1373, 1, 1) and (771629, 5, 1).
(p_2, u, v): (1093, 1, 1) and (764629, 5, 1).

(p_1, u, v): (4349, 5, 3) and (306829, 15, 7).
(p_2, u, v): (2549, 5, 3) and (218629, 15, 7).

(p_1, u, v): (29, 1, 1) and (11149, 5, 3).
(p_2, u, v): (5, 1, 1) and (5749, 5, 3).

(p_1, u, v): (1237, 3, 1) and (40357, 7, 3).
(p_2, u, v): (877, 3, 1) and (22717, 7, 3).

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). https://doi.org/10.12988/ija.2015.5421

[3] 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

[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] S. W. Kim, Ranks of several elliptic curves $y^2 = x^3 \mp 3px$, *Int. J. of Algebra,* **15** (2021), 191-203. https://doi.org/10.12988/ija.2021.91565

[6] 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.

[7] 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/ija.2026.92010

Received: October 15, 2026; Published: November 10, 2026