Far East Journal of Mathematical Sciences (FJMS)
Volume 74, Number 2, 2013, Pages 379-388
Published Online: March 2013
Available online at http://pphmj.com/journals/fjms.htm
Published by Pushpa Publishing House, Allahabad, INDIA

RANGE OF RANK IN AN ELLIPTIC CURVE

Shin-Wook Kim and Hwasin Park

Department of Mathematics
Chonbuk National University
Chonju, Chonbuk 561-756, Korea

Abstract

We suppose an elliptic curve as $y^2 = x^3 + px$, where p is an odd prime. In this paper, we investigate the range of this form when p is an odd prime such that $p \equiv 13, 15 \pmod{16}$.

1. Introduction

In elliptic curve, we often find the case that the value of rank is less than 2. Namely, the rank is 0 or 1 or 0, 1. In [2], Hatley showed that the rank of an elliptic curve $y^2 = x(x-2)(x-p)$, where p and $p-2$ are twin primes and p is such that $p \equiv 5 \pmod{8}$ is 0 or 1. In [5, Chap. III, Exercise 3.8], we can find the result that the rank of $y^2 = x^3 + px$ is 0 or 1 if p is an odd prime such that $p \equiv 3 \pmod{16}$. And in [3], the authors proved that the rank of $y^2 = x^3 - px$ is 1 if $p = e^2 + 1$ and $e = 4t + 2$, $t \geq 0$. Furthermore, in CN-elliptic curve $y^2 = x^3 - d^2x$, the rank is 0 if $d = 1$ (by Fermat) and 1 if $d = 5$ ([4]).

2010 Mathematics Subject Classification: 11A41, 14H52.
Keywords and phrases: prime, rank of elliptic curve.
Submitted by K. K. Azad
Received December 23, 2012

And it is conjectured that if p satisfies $p \equiv 13, 15 \pmod{16}$, then the rank of $y^2 = x^3 + px$ is 1 but not always ([5]). Namely, the value of rank is 0 or 1. In this paper, we treat this by the method which is used in [1, 5]. Before computing the rank, we need to treat basic notations about elliptic curve.

Suppose that $E_p : y^2 = x^3 + px$ is an elliptic curve and let Γ be the set of rational points on E_p. And Γ is finitely generated abelian group by *Mordell's* theorem and it is isomorphic to $E_{tors}(Q) \oplus Z^r$. Here, $E_{tors}(Q)$ is a torsion subgroup and r is called the *Mordell-Weil* rank. And let α be a homomorphism from Γ to $Q^{\times}/Q^{\times 2}$, where $\alpha(P) = 1 \pmod{\times 2}$, $\alpha(P) = b \pmod{Q^{\times 2}}$, $\alpha(P) = x \pmod{Q^{\times 2}}$ if $P = O$ (O is an infinity point), $P = (0, 0)$, $P = (x, y)(x \neq 0)$, respectively. In addition, $Q^{\times}$, $Q^{\times 2}$ are the set of nonzero rational numbers, the set of squares of elements of $Q^{\times}$, respectively ($Q^{\times 2}$ is a multiplicative group).

And suppose that $\overline{\Gamma}$ is the set of rational points on the curve $\overline{E_p} : y^2 = x(x^2 - 2ax + a^2 - 4b)$ and $\overline{\alpha}$ is a homomorphism from $\overline{\Gamma}$ to $Q^{\times}/Q^{\times 2}$, where $\overline{\alpha}(P) = 1 \pmod{Q^{\times 2}}$, $\overline{\alpha}(P) = a^2 - 4b \pmod{Q^{\times 2}}$, $\overline{\alpha}(P) = x \pmod{Q^{\times 2}}$ if $P = \overline{O}$ (infinity point), $P = (0, 0)$, $P = (x, y)(x \neq 0)$, respectively. And $Q^{\times 2}$, $Q^{\times}$ are the same in case of Γ.

And also, let $N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4$ and $N^2 = b_1 M^4 - 2aM^2 e^2 + b_2 e^4$ be relating equations for Γ and $\overline{\Gamma}$, respectively. Furthermore, for Γ, $b = b_1 b_2$ and b_1, b_2 are divisors of b. And b_1 is not congruent to 1, $b \pmod{Q^{\times 2}}$. For $\overline{\Gamma}$, $b_1 b_2 = a^2 - 4b$ and b_1, b_2 are the same in case of Γ. And put (M, e, N) is a solution of these two relating equations and $(M, N) = (M, e) = (N, e) = (b_1, e) = (b_2, M) = 1$. In addition, the formula

$2^r = \frac{|\alpha(\Gamma)||\overline{\alpha}(\overline{\Gamma})|}{4}$ holds, where r is the rank of an elliptic curve. For more things about this, refer to [1, 5].

2. Investigating the Rank in Elliptic Curve

Now we compute the rank of an elliptic curve $y^2 = x^3 + px$, where p is an odd prime such that $p \equiv 13, 15 \pmod{16}$.

Theorem 2.1. *Assume that E_p is an elliptic curve $y^2 = x^3 + px$, where p is an odd prime of the form $p \equiv 13, 15 \pmod{16}$. Then the rank of this curve is* 0 *or* 1.

Proof. Let E_p be an elliptic curve $y^2 = x^3 + px$ and p is an odd prime number.

First, we treat the case $p \equiv 13 \pmod{16}$.

Set $p = 16k + 3$, then the relating equation for Γ is $N^2 = M^4 + (16k + 13)e^4$. If this equation has a solution, then the values $\alpha(P)$ are $\alpha(P) = 1,\ 16 + 3 \pmod{Q^{\times 2}}$, but these were already defined as $\alpha(P) = 1, b \pmod{Q^{\times 2}}$ if P is O (infinity point) and $(0, 0)$, respectively, thus we do not have to consider the solvability of the equation and so $\#\alpha(\Gamma)$ is 2.

And from E_p, $\overline{E_p}$ is the curve $y^2 = x^3 - 4(16k + 3)x$ and relating equations for $\overline{\Gamma}$ are the following:

(i) $N^2 = M^4 - 4(16k + 13)e^4$, (ii) $N^2 = -M^4 + 4(16k + 13)e^4$,

(iii) $N^2 = 2M^4 - 2(16k + 13)e^4$, (iv) $N^2 = -2M^4 + 2(16k + 13)e^4$,

(v) $N^2 = 4M^4 - (16k + 3)e^4$, (vi) $N^2 = -4M^4 + (16k + 13)e^4$.

The values $\overline{\alpha}(P)$ in (i) are $\overline{\alpha}(P) = 1,\ -(16k+13) (\mathrm{mod}\, Q^{\times 2})$ and these were already defined by α in the previous section when P is an infinity point and $(0, 0)$, thus we do not have to treat the solvability.

Equation (v) cannot have a solution because of the induced result $1 \equiv N^2 \equiv 3e^4 \equiv 3 \pmod 4$.

Now we investigate each equation's solvability.

If we reduce (ii) by 4, then $1 \equiv N^2 \equiv 3M^4 \equiv 3 \pmod 4$ is induced, thus we arrive at a contradiction.

Reduce (iii) by p induces $N^2 \equiv 2M^4 \pmod p$, whereas the value of Legendre symbol $\left(\frac{2M^4}{p}\right)$ is –1 and so it is impossible to have a solution.

After reducing equation (iv) by p, then we get the result as $N^2 \equiv -2M^4 \pmod p$, whereas the Legendre symbol is

$$\left(\frac{-2M^4}{p}\right) = (-1)^{\frac{16k+13-1}{2}} \times (-1)^{\frac{(16k+13)^2-1}{8}} = -1,$$

hence there happens a contradiction.

The congruence relation $N^2 \equiv -4M^4 \pmod p$ is induced after reducing (vi) by p. And we know that $\left(\frac{-4M^4}{p}\right) = 1$. And if we reduce equation (vi) by 32, then we get

$$1, 9, 17, 25 \equiv N^2 \equiv 28M^4 + (16k+13)e^4 \equiv 28M^4 + (16k+13)\cdot 17$$
$$\equiv 28M^2 + 16k + 29 \pmod{32}.$$

Let k and M be odds (put $k = 2a+1$). Then the induced thing is $28M^4 + 16(2a+1) + 29 \equiv 28 + 16 + 29 = 73 \equiv 9 \pmod{32}$, hence there can exist a

solution. Reductions by 4, 8, 16 makes the same result and it is easy to treat, thus we omit to compute here.

In conclusion, the number of $\overline{\alpha}(\overline{\Gamma})$ is 2 or 4, and thus by cumbersome computation, the rank is 0 or 1.

Second, we compute the case $p \equiv 15 \pmod{16}$.

Suppose that E_p is an elliptic curve $y^2 = x^3 + (16k + 15)x$. Put $p = 16k + 15$, then the relating equation for Γ is $N^2 = M^4 + (16k + 15)e^4$ and $\alpha(P)$ of this equation are $\alpha(P) = 1,\ 16k + 15 \pmod{Q^{\times 2}}$ and these were defined by α from $P = O$ (infinity point), $P = (0, 0)$, respectively, and so we do not have to consider the solvability of these equations, thus $\#\alpha(\Gamma) = 2$.

And we get $\overline{E_p}$ is the curve $y^2 = x^3 - 4(16k + 15)$ from E_p.

Then the relating equations for $\overline{\Gamma}$ are as follows:

(i) $N^2 = M^4 - 4(16k + 15)e^4$, (ii) $N^2 = -M^4 + 4(16k + 15)e^4$,

(iii) $N^2 = 2M^4 - 2(16k + 15)e^4$, (iv) $N^2 = -2M^4 + 2(16k + 15)e^4$,

(v) $N^2 = 4M^4 - (16k + 15)e^4$, (vi) $N^2 = -4M^4 + (16k + 15)e^4$.

The values $\overline{\alpha}(P)$ in (i), (v) are $\overline{\alpha}(P) = 1,\ -(16k + 15) \pmod{Q^{\times 2}}$ but these were defined by $\overline{\alpha}$ from P is infinity point and $(0, 0)$, respectively, thus we can omit to treat the solvability of these equations.

We check other equations' solvability.

Here, we change the order in treating the equations. We investigate the equation (iii) later.

Reducing (ii) by 4 leaves $1 \equiv N^2 \equiv 3M^4 \equiv 3 \pmod{4}$, thus there cannot exist a solution in equation (ii).

If we reduce equation (iv) by p, then the induced congruence relation is $N^2 \equiv -2M^4 \pmod{p}$, but the value of Legendre symbol is

$$\left(\frac{-2M^4}{p}\right) = (-1)^{\frac{16k+15-1}{2}} \times (-1)^{\frac{(16k+15)^2-1}{8}} = -1,$$

whence we get a contradiction.

There induced a congruence relation $N^2 \equiv -4M^4 \pmod{p}$ from equation (vi), but at the same time, the value of $\left(\frac{-4M^4}{p}\right)$ is –1, thus (vi) cannot have a solution.

After reducing equation (iii) by p, the congruence relation is $N^2 \equiv 2M^4 \pmod{p}$ and the value of $\left(\frac{2M^4}{p}\right)$ is 1. And reducing both sides of the equation by 32 induces $0, 4, 16 \equiv N^2 \equiv 2M^4 + 2e^4 \equiv 2 + 2 = 4 \pmod{32}$, thus equation (iii) can have a solution. And cases of reduction by 4, 8, 16 induce the same result and here we omit to compute.

Consequently, $\#\overline{\alpha}(\overline{\Gamma}) = 2, 4$ and by using the formula $2^r = \frac{|\alpha(\Gamma)||\overline{\alpha}(\overline{\Gamma})|}{4}$, we get $2^r = \frac{2 \cdot 2}{4}, \frac{2 \cdot 4}{4}$ and this completes the proof of Theorem 2.1. □

Remark 2.2. As we proved in the above, the rank of an elliptic curve $y^2 = x^3 + px$ (p is an odd prime) with $p \equiv 13, 15 \pmod{16}$ is 0 or 1. According to the solvability of relating equations (vi) $N^2 = -4M^4 + (16k+13)e^4$ (case of $p \equiv 13 \pmod{16}$), (iii) $N^2 = 2M^4 - 2(16k+15)e^4$ (case of $p \equiv 15 \pmod{16}$), the value rank is determined 0 or 1. We can find easily the examples which induce solutions in the above relating equations. But it is not simple that these equations always have solutions. Thus without

showing the solvability of these equations, we only can say that the rank in case of $p \equiv 13 \pmod{16}$, $p \equiv 15 \pmod{16}$ is 0 or 1. Instantly, the rank 0 means the above two relating equations have no solution. And this is the point why the author uses the word range.

Remark 2.3. In the above, we compute the reduction by 32 in equations (vi) (case of $p \equiv 13 \pmod{16}$), (iii) (case of $p \equiv 15 \pmod{16}$), respectively. Even though, we cannot check the solvability of equation by reduction for all natural numbers *n*, computation by 32 is meaningful because in several cases, even if there is no matter in reduction by 4, 8, 16, there happens a contradiction after reducing by 32.

As we saw in the proof, $N^2 = 1, 9, 17, 25 \pmod{32}$ (N is an odd). It is natural that 1, 9, 25 are residues. But in the case of 17, we can face a question why this emerges. We need to consider about this.

Assume that $N = 2k + 1$ (k is an integer). Then $N^2 = 4k^2 + 4k + 1$.

(A) Let k be an odd ($k = 2k' + 1$ with k' is an integer). Then

$$N^2 = 4(2k' + 1)^2 + 4(2k' + 1) + 1$$
$$= 4 \cdot 4k'(k' + 1) + 8k' + 9 \equiv 8k' + 9 \pmod{32}.$$

(1) k' is an odd ($k' = 2a + 1$ with a is an integer): $8k' + 9 = 8(2a + 1) + 9 = 16a + 17$.

If a is an even, then $16a + 17 \equiv 17 \pmod{32}$ and if a is an odd, then $16a + 17 \equiv 33 \equiv 1 \pmod{32}$.

(2) k' is an even ($k' = 2a$ with a is an integer): $8k' + 9 = 8 \cdot 2a + 9 = 16a + 9$.

If a is an even, then $16a + 9 \equiv 9 \pmod{32}$ and if a is an odd, then $16a + 9 \equiv 25 \pmod{32}$.

Accordingly, $N^2 \equiv 1, 9, 17, 25 \pmod{32}$.

(B) Let k be an even ($k = 2k'$ with k' is an integer). Then $N^2 = 4 \cdot 4k'^2 + 4 \cdot 2k' + 1 = 16k'^2 + 8k' + 1$.

(1) k' is an odd ($k' = 2a + 1$ with a is an integer):

$$16k'^2 + 8k' + 1 = 16(4a^2 + 4a + 1) + 8(2a + 1) + 1 \equiv 16a + 25 \pmod{32}.$$

If a is an even, then $16a + 25 \equiv 25 \pmod{32}$ and if a is an odd, then $16a + 25 \equiv 9 \pmod{32}$.

(2) k' is an even ($k' = 2a$ with a is an integer):

$$16k'^2 + 8k' + 1 = 16 \cdot 4a^2 + 8 \cdot 2a + 1 \equiv 16a + 1 \pmod{32}.$$

If a is an even, then $16a + 1 \equiv 1 \pmod{32}$ and if a is an odd, then $16a + 1 \equiv 17 \pmod{32}$.

Consequently, $N^2 \equiv 1, 9, 17, 25 \pmod{32}$.

In conclusion, if N is an odd, then reducing it by 32 induces $N^2 \equiv 1, 9, 17, 25 \pmod{32}$. And this is the reason why in the process of proving Theorem 2.1, there emerges 17 as the residue in modulo 32.

3. Examples

Now we consider examples of the previous section's theorem.

In the following examples, we omit to mention about relating equation $N^2 = M^4 + pe^4$ for Γ and $N^2 = M^4 - 4pe^4$ for $\overline{\Gamma}$ because it is repeated.

Example 3.1. We may suppose that E_p is an elliptic curve $y^2 = x^3 + 29x$. Then it is clear that $\#\alpha(\Gamma) = 2$. And from E_p, $\overline{E_p}$ is the curve $y^2 = x^3 - 116x$, thus the relating equations for $\overline{\Gamma}$ are the following:

(i) $N^2 = M^4 - 116e^4$, (ii) $N^2 = -M^4 + 116e^4$,

(iii) $N^2 = 2M^4 - 58e^4$, (iv) $N^2 = -2M^4 + 58e^4$,

(v) $N^2 = 4M^4 - 29e^4$, (vi) $N^2 = -4M^4 + 29e^4$.

We know that the value of $\overline{\alpha}(\overline{\Gamma})$ in (i) is same to (v), hence it need not to check equation (v).

By reducing (ii) $(\mathrm{mod}\, 4)$, we arrive at a congruence relation $1 \equiv N^2 \equiv 3M^4 \equiv 3 \,(\mathrm{mod}\, 4)$, therefore (ii) has no solution.

Using the number 29 in reducing equation (iii), the congruence relation $N^2 \equiv 2M^4 \,(\mathrm{mod}\, 29)$ is induced, whereas the Legendre symbol of $\left(\frac{-2M^4}{29}\right)$ is –1 and so we get a contradiction.

If we reduce (iv) by 29, then the result is $N^2 \equiv -2M^4 \,(\mathrm{mod}\, 29)$ but at the same time, we know that $\left(\frac{-2M^4}{29}\right) = -1$. Therefore, (vi) has no solution and equation (vi) has a solution $(1, 1, 1)$.

Consequently, $\#\overline{\alpha}(\overline{\Gamma}) = 4$ and thus the rank is 1.

Example 3.2. Suppose that E_p is an elliptic curve $y^2 = x^3 + 31x$. Then it is easy to get that $\#\alpha(\Gamma) = 2$. And $\overline{E_p}$ is the curve $y^2 = x^3 - 124x$. Hence, the relating equations for $\overline{\Gamma}$ are the following:

(i) $N^2 = M^4 - 124e^4$, (ii) $N^2 = -M^4 + 124e^4$,

(iii) $N^2 = 2M^4 + 62e^4$, (iv) $N^2 = -2M^4 + 62e^4$,

(v) $N^2 = 4M^4 - 31e^4$, (vi) $N^2 = -4M^4 + 31e^4$.

The value of $\overline{\alpha}(\overline{\Gamma})$ in (v) is same to (i), thus it does not have to be treated.

After reducing equation (ii) by 4, then the result is $1 \equiv N^2 \equiv 3M^4 \equiv 3 \pmod 4$, hence a contradiction happens.

Equation (iii) has a solution $(3, 1, 10)$.

Reducing (iv) by 31 leaves the result $N^2 \equiv -2M^4 \pmod{31}$, whereas $\left(\frac{-2M^4}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right) = -1$, thus we arrive at a contradiction.

The congruence relation $N^2 \equiv -4M^4 \pmod{31}$ is induced from reducing (vi) by 31. But the Legendre symbol is $\left(\frac{-4M^4}{31}\right) = \left(\frac{-1}{31}\right) = -1$ and so (vi) cannot have a solution.

Whence, $\#\overline{\alpha}(\overline{\Gamma}) = 4$ and so the rank is 1.

References

[1] J. H. Chahal, Topics in Number Theory, Kluwer Academic/Plenum Publisher, 1988.

[2] Jeffrey Hatley, On the Rank of Elliptic Curve $y^2 = x(x - p)(x - 2)$, April 29, (2009), 1-16.

[3] Angela J. Hollier, Blair K. Spearman and Qiduan Yang, On the rank and integral points of elliptic curves $y^2 = x^3 - px$, Int. J. Algebra 3(8) (2009), 401-406.

[4] Karl Rubin, Ranks, Ross Program, 2003.

[5] J. H. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer, New York, 1985.