**International Journal of Algebra, Vol. 13, 2019, no. 3, 143 – 152**
**HIKARI Ltd, www.m-hikari.com**
**https://doi.org/10.12988/ija.2019.9212**

# Algebraic Structure in Elliptic Curves

# $y^2 = x^3 - 5px$

**Shin-Wook Kim**

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



**Abstract**

Under the hypothesis that $E_{-5p}$ is an elliptic curves $y^2 = x^3 - 5px$ with prime $p$, the rank of $E_{-5p}$ will be enumerated in accordance with the form of prime $p$.

**Mathematics Subject Classification**: 11A41, 11G05

**Keywords**: Prime, Elliptic curves

## 1 Introduction

Accumulating generalized result of rank in elliptic curve of the form $E_{\pm Ap}: y^2 = x^3 \pm Apx$($p$ is an odd prime and $A$ is prime) is meaningful. The range of rank in $E_{\pm Ap}$ is not beyond 4. According to each value of $A$ the rank is determined. Compared with other forms like Mordell curve $y^2 = x^3 + B$ or $y^2 = x(x \pm A)(x \pm B)$ it can be relatively easily manipulated. Hence, the ranks in curves $E_{\pm Ap}$ are managed widely. In [4], the authors researched the rank of $y^2 = x^3 + pqx$. In [5], the author calculated that the rank of curve $y^2 = x^3 - 2px$ where $p$ is a prime of the form $p = u^8 + 6u^4v^4 + 4v^8$ with integers $u$ and $v$ and $(u,v)$=1 and $p \equiv 11(mod\ 16)$ is 1. In this article, we will consider the rank of elliptic curve of new form $y^2 = x^3 - 5px$ with prime $p$.

Prior to research the rank, it is necessary to treat some notations in [10] which are needed to consider the rank of elliptic curve.

Denote $E$ as an elliptic curve $y^2 = x^3 + ax^2 + bx$ and $\Gamma$ as the set of rational points on $E$. Then, $\Gamma$ is a finitely generated abelian group owing to $Mordell's$

Theorem. In addition, it is isomorphic to $E(Q)_{tors} \oplus Z^r$ where $r$ is Mordell-Weil rank and $E(Q)_{tors}$ denotes a torsion subgroup. Assign $Q^{\times}$ as multiplicative group which is consisted of non-zero rational numbers. In addition, denote $Q^{\times 2}$ as the subgroup of squares of elements of $Q^{\times}$.

Next, define $\alpha$ as a homomorphism $\alpha\colon \Gamma \to Q^{\times}/Q^{\times 2}$ that satisfies

$$\alpha(O) = 1(mod\ Q^{\times 2}) \text{ and}$$

$$\alpha(0, 0) = b(mod\ Q^{\times 2}) \text{ and } \alpha(x, y) = x(mod\ Q^{\times 2})$$

with infinity point $O$ and non-zero $x$.

Designate $N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4$ as relating equation for $\Gamma$ where $b_1$ and $b_2$ satisfy that $b = b_1 b_2$ as $b_1 \not\equiv 1, b(mod\ Q^{\times 2})$. Denote $(M, e, N)$ as an integral solution of above equation then, there derived that $M \neq 0$, $e \neq 0$ and $(M, N)=(M, e)=(N, e)=(b_1, e)=(b_2, e)=1$.

In the next step, we ought to notice the curve $y^2 = x(x^2 - 2ax + a^2 - 4b)$. Take $\overline{\Gamma}$ as the set of rational points on $\bar{E}$. Suppose that $\bar{\alpha}$ is a homomorphism $\bar{\alpha}\colon \overline{\Gamma} \to Q^{\times}/Q^{\times 2}$ where

$$\bar{\alpha}(O) = 1(mod\ Q^{\times 2}) \text{ and } \bar{\alpha}(0, 0) = a^2 - 4b(mod\ Q^{\times 2}) \text{ and}$$

$$\bar{\alpha}(x, y) = x(mod\ Q^{\times 2})$$

holds with infinity point $O$ and $x \neq 0$.

Assume that $N^2 = b_1 M^4 - 2aM^2 e^2 + b_2 e^4$ is relating equation for $\overline{\Gamma}$ that satisfies $b_1$ and $b_2$ satisfy that $b_1 b_2 = a^2 - 4b$ with $b_1 \not\equiv 1, a^2 - 4b(mod\ Q^{\times 2})$.

Let $(M, e, N)$ be an integral solution of above relating equation then, there comes $M \neq 0$ and $e \neq 0$ and $(M, N)=(M, e)=(N, e)=(b_1, e)=(b_2, e)=1$ and $M \neq 0, e \neq 0$.

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

## 2 In $E_{-5p}$

In this section, we will research the rank of elliptic curve $E_{-5p}\colon y^2 = x^3 - 5px$ by the method in [10]. In the proof of following theorem, we will omit to manage about solvability of equation 1) for $\Gamma$ and 1) for $\overline{\Gamma}$. It is possible to refer in [5] for about this.

**Theorem 2.1.** (1). Designate prime $p$ as $p = 2u^4 + 8u^2 v^2 + 3v^4$ with two integers $u$ and $v$ and $(u,v)=1$ and $p \equiv 3(mod\ 16)$ in elliptic curve $E_{-5p}$ then, we obtain $rank(E_{-5(2u^4+8u^2v^2+3v^4)}(Q)) = 1$.

(2). If a prime $p$ is the form $p = 18u^4 + 72u^2 v^2 + 67v^4$ with integers $u$ and $v$

and $(u,v)=1$ and $p \equiv 3(mod\ 16)$ in curve $E_{-5p}$then, there is given the conclusion $rank(E_{-5(18u^4+72u^2v^2+67v^4)}(Q)) = 1$.

(3). Denote the prime $p$ as $p = 200u^4 + 80u^2v^2 + 3v^4$ with integers $u$ and $v$ and $(u,v)=1$ and $p \equiv 3(mod\ 16)$ in elliptic curve $E_{-5p}$. Then, we conclude that $rank(E_{-5(200u^4+80u^2v^2+3v^4)}(Q)) = 1$.

(4). We appoint that $p$ is a prime such that $p = 45u^4 + 60u^2v^2 + 2v^4$ with integers $u$ and $v$ and $(u,v)=1$ and $p \equiv 11(mod\ 16)$ in $E_{-5p}$ then, there obtained $rank(E_{-5(45u^4+60u^2v^2+2v^4)}(Q)) = 1$.

Proo$f$. (1). Take prime $p$ as $p = 2u^4 + 8u^2v^2 + 3v^4$ with integers $u$ and $v$ and $(u,v)=1$ and $p \equiv 3(mod\ 16)$ in elliptic curve $E_{-5p}: y^2 = x^3 - 5px$. Assign prime $p$ as $p = 16k + 3$ with integer $k$ then, there exist relating equations for Γ as follows:

$$1)N^2 = M^4 - 5(16k + 3)e^4 \text{ and } 2)N^2 = -M^4 + 5(16k + 3)e^4 \text{ and}$$

$$3)N^2 = 5M^4 - (16k + 3)e^4 \text{ and } 4)N^2 = -5M^4 + (16k + 3)e^4.$$

There is no solution in equation 2) since using 16 in cutting down on this produces that 0, 1, 4, 9 $\equiv N^2 \equiv 15M^4 + 15e^4 \equiv$ 14, 15 $(mod\ 16)$ and two sides don't match in this relation, hence there comes a contradiction.

Reducing equations 3) and 4) by 8 implies that 3)0, 1, 4 $\equiv N^2 \equiv 5M^4 + 5e^4 \equiv$ 5, 2 $(mod\ 8)$ and 4)0, 1, 4 $\equiv N^2 \equiv 3M^4 + 3e^4 \equiv$ 6, 3$(mod\ 8)$. Both sides $RHS$ and $LHS$ are unmatched, thus no solution exists in these equations.

Henceforth, induced fact is $\#\alpha(\Gamma) = 2$.

Next from $E_{-5p}$, the curve $\overline{E_{-5p}}$ is deduced as $y^2 = x^3 + 20(16k + 3)x$.

Accordingly, it implies the following relating equations for $\bar{\Gamma}$:

$$1)N^2 = M^4 + 20(16k + 3)e^4 \text{ and}$$

$$2)N^2 = 2M^4 + 10(16k + 3)e^4 \text{ and}$$

$$3)N^2 = 4M^4 + 5(16k + 3)e^4 \text{ and}$$

$$4)N^2 = 5M^4 + 4(16k + 3)e^4 \text{ and}$$

$$5)N^2 = 10M^4 + 2(16k + 3)e^4 \text{ and}$$

$$6)N^2 = 20M^4 + (16k + 3)e^4.$$

If $p$ is used in cutting down on relating equation 2) then, we confront to $2)N^2 \equiv 2M^4\ (mod\ p)$ but at the same time we acquire that $\left(\frac{2M^4}{p}\right) = -1$. There two results cannot coexist, hence there cannot exist a solution in 2).

If relating equation 3) is cut down on by 8 then, we obtain the congruence $3)1 \equiv N^2 \equiv 4M^4 + 7 \equiv 7, 3(mod\ 8)$. Two sides $LHS$ and $RHS$ are unmatched and so possessing a solution is impossible in 3).

The values $\bar{\alpha}(P)$ in equation 4) are the same in it of 1) in $Q^\times/Q^{\times 2}$ and it is possible to omit to examine the solvability of 4).

Cutting down on 6) by 8 shows that $6)1\equiv N^2 \equiv 4M^4 + 3 \equiv 3, 7\ (mod\ 8)$. Here, we face unmatched calculation, thus it also cannot take a solution.

Equation 5) is $N^2 = 10M^4 + (4u^4 + 16u^2v^2 + 6v^4)e^4$. In coefficient of $e^4$, there is a square term $4u^4$, thus we can expect the advent of polynomial's square that is consisted of variables $u$ and $v$ after substituting some integers into $M$ and $e$. Because the term $16u^2v^2$ is factored as $2 \cdot 2 \cdot 4u^2v^2$, there should be shown $16v^4$. Now we are confronted with $10M^4 + 6v^4e^4$. Owing to our objective $16v^4$, the equality $10M^4 + 6v^4e^4 = 16v^4$ must be hold. If $M$ and $e$ are taken as $v$ and 1 then, we attain that $10v^4 + 6v^4 = 16v^4$. This is the result what we searched for. Besides, from the calculation $10v^4 + 4u^4 + 16u^2v^2 + 6v^4 = 4u^4 + 16u^2v^2 + 16v^4$ the integer $N$ is derived as $2u^2 + 4v^2$. As a result, the triple $(v, 1, 2u^2 + 4v^2)$ satisfies the solution of 5).

In the next step, assume that relating equation 4) has a solution then, we obtain that $5 \cdot 10 \equiv 2 \in \bar{\alpha}(\bar{\Gamma})(mod\ Q^{\times 2})$ but as we examined already in above, equation $2)N^2 = 2M^4 + 10(16k + 3)e^4$ cannot take a solution, thus there is emerged a contradiction. Therefore, no solution exists in 4).

Resultantly, it follows that $\#\bar{\alpha}(\bar{\Gamma}) = 4$.

Thereby, the conclusion $rank(E_{-5(2u^4+8u^2v^2+3v^4)}(Q)) = 1$ is derived due to $2^r = \frac{2\cdot 4}{4} = 2$.

(2). Because of the result (1) in the above, it is enough that we only check the solvability of equation $5)N^2 = 10M^4 + (36u^4 + 144u^2v^2 + 134v^4)e^4$ for $\bar{\Gamma}$. Above all, there is a square term $36u^4$ in it, hence the condition for being shown the square of polynomial which is composed of variables $u$ and $v$ is gotten. Next, from the factorization $144u^2v^2 = 2 \cdot 6 \cdot 12u^2v^2$, there has to be appeared $144v^4$. The remanent arithmetical value that ought to be treated is $10M^4 + 134v^4e^4$. Since our aim is $144v^4$, the relation $10M^4 + 134v^4e^4 = 144v^4$ ought to be hold. Thereby, we select $M$ and $e$ as $v$ and 1 respectively then, there educed that $10v^4 + 134v^4 = 144v^4$. We obtained what we pursued. Furthermore, from $10v^4 + 36u^4 + 144u^2v^2 + 134v^4 = 36u^4 + 144u^2v^2 + 144v^4$, the integer $N$ is given as $6u^2 + 12v^2$. Hence, we conclude that $(v, 1, 6u^2 + 12v^2)$ is a solution of relating equation 5). On that account, there is derived $\#\bar{\alpha}(\bar{\Gamma}) = 4$. As a result, there comes $rank(E_{-5(18u^4+72u^2v^2+67v^4)}(Q)) = 1$ owing to $2^r = \frac{2\cdot 4}{4} = 2$.

(3). On account of (1) in the above, the only relating equation which should be surveyed the solvability is $5)N^2 = 10M^4 + (400u^4 + 160u^2v^2 + 6v^4)e^4$ for $\bar{\Gamma}$.

First of all, there exists a term $400u^4$ in coefficient of $e^4$ and this is a square form. Henceforth, a probability for being emerged the square of polynomial whose components are two variables $u,\ v$ exists. Because the term $160u^2v^2$ is factored as $2\cdot 20\cdot 4u^2v^2$, there should be appeared the term $16v^4$. Now the numerical value that must be noticed is $10M^4+6v^4e^4$. From our purpose $16v^4$, the relation $10M^4+6v^4e^4=16v^4$ ought to be valid. Whence, we choose $M$ and $e$ as $v$ and 1 respectively then, there comes $10v^4+6v^4=16v^4$. In addition, from $10v^4+400u^4+160u^2v^2+6v^4=400u^4+160u^2v^2+16v^4$ the integer $N$ is induced as $N=20u^2+4v^2$. Therefore, we attain $(v, 1, 20u^2+4v^2)$ as a solution of 5). Hence, we acquire the conclusion $\#\bar{\alpha}(\bar{\Gamma})=4$. For that reason, we face the consequence $rank(E_{-5(200u^4+80u^2v^2+3v^4)}(Q))=1$ on account of $2^r=\frac{2\cdot 4}{4}=2$.

(4). Denote prime $p$ as $p=45u^4+60u^2v^2+2v^4$ with integers $u$ and $v$ and $(u,v)=1$ and $p\equiv 11(mod\ 16)$ in $E_{-5p}\colon y^2=x^3-5px$. Take $p$ as $p=16k+11$ with integer $k$ then, there are relating equations for $\Gamma$ as follows:

1)$N^2=M^4-5(16k+11)e^4$ and 2)$N^2=-M^4+5(16k+11)e^4$ and

3)$N^2=5M^4-(16k+11)e^4$ and 4)$N^2=-5M^4+(16k+11)e^4$.

If 2) is cut down on by 8 then, we gain the congruence $0, 1, 4\equiv N^2\equiv -M^4+7e^4\equiv 7,\ 6\ (mod\ 8)$. We acquired unmatched enumeration and thus, taking a solution is impossible in equation 2).

Reducing 3) by 8 shows that 3)$0,\ 1,\ 4\equiv\ N^2\equiv 5M^4+5e^4\equiv 2,\ 5\ (mod\ 8)$. Two sides are unmatched here, hence it cannot have a solution.

Cutting down on equation 4) by 4 implies that 4)$0, 1\equiv N^2\equiv -5M^4+11e^4\equiv 3, 2\ (mod\ 4)$ and both $LHS$ and $RHS$ do not match. Whence, a solution cannot exist in this equation.

Thereby, it is derived that $\#\alpha(\Gamma)=2$.

Now, from $E_{-5p}$ the curve $\overline{E_{-5p}}$ is gotten as $y^2=x^3+20(16k+11)x$.
Accordingly, there exist relating equations for $\bar{\Gamma}$:

1)$N^2=M^4+20(16k+11)e^4$ and

2)$N^2=2M^4+10(16k+11)e^4$ and

3)$N^2=4M^4+5(16k+11)e^4$ and

4)$N^2=5M^4+4(16k+11)e^4$ and

5)$N^2=10M^4+2(16k+11)e^4$ and

6)$N^2=20M^4+(16k+11)e^4$.

There is no solution in equation 2) since using the prime $p$ in cutting down on equation 2) then, there produced $N^2 \equiv 2M^4(mod\, p)$ but we also encounter to $\left(\frac{2M^4}{p}\right) = -1$. These two things cannot exist simultaneously, thus we arrive at a contradiction.

After reducing relating equation 3) by 8 then, we take that $1 \equiv N^2 \equiv 4M^4 + 7 \equiv 7, 3(mod\, 8)$. Two sides $LHS$ and $RHS$ do not match in this congruence, hence there cannot appear the solution in equation 3).

Using 16 in cutting down on equation 6) then, we obtain the congruence $1, 9 \equiv N^2 \equiv 4M^4 + 11 \equiv 15, 11(mod\, 16)$. Here, both sides are unmatched and so there cannot exist a solution in 6).

Equation 5) can be rewritten as $N^2 = 10M^4 + (90u^4 + 120u^2v^2 + 4v^4)e^4$. Above all, there is a term $4v^4$ in coefficient of $e^4$ and it is a square form. Thus, there is a potentiality of emergence of polynomial that is comprised of variables $u$ and $v$. Due to the factorization $120u^2v^2 = 2 \cdot 30 \cdot 2u^2v^2$, there should be derived the term $900u^4$. The next thing to do is considering the relation $10M^4 + 90u^4e^4 = 900u^4 \cdots\cdots (H)$. Now, finding the values $M$ and $e$ is important thing. The existence of pair $(e, M)$ which satisfies $(H)$ is significant thing. In $(H)$, the term for $u^4$ exists in both sides and in $LHS$ it is $90u^4e^4$ and so determining the integer $e$ earlier is better to search the pair $(e, M)$. The smaller in value $e$ the better to find another integer $M$. Whence, if we select $e$ as 1 then, we gain $10M^4 + 90u^4 = 900u^4$. Hence, the equality $10M^4 = 810u^4$ is produced and thus the value $M$ is deduced as $3u$. Now, from the calculation $10(3u)^4 + 90u^4 + 120u^2v^2 + 4v^4 = 900u^4 + 120u^2v^2 + 4v^4$ the integer $N$ is educed as $30u^2 + 2v^2$. Accordingly, the solution of equation 5) is derived as $(3u, 1, 30u^2 + 2v^2)$.

Next, if there exists a solution in relating equation 4) then, we attain that $5 \cdot 10 \equiv 2 \in \bar{\alpha}(\bar{\Gamma})(mod\, Q^{\times 2})$ but as we researched in the above, there is no solution in equation 2)$N^2 = 2M^4 + 10(16k + 11)e^4$. Thus, a contradiction is given and hence equation 4) has no solution.

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

On this account, it implies that $2^r = \frac{2\cdot 4}{4} = 2$.

Therefore, there comes $rank(E_{-5(45u^4+60u^2v^2+2v^4)}(Q)) = 1$. □

As the consequence of other curves $y^2 = x^3 \pm px$, the results of rank 1 were emerged frequently in curve $E_{-5p}$. Above results were also all 1. Compared with other values of rank, systematizing the rank 1 in curve $E_{-5p}$ is relatively easy.

**Remark 2.2.** Congruent number is significant dispute in elliptic curve. It is well-known that a positive integer $n$(:squarefree) is congruent if and only if congruent number elliptic curve $E_n: y^2 = x^3 - n^2x$ takes a positive rank $r_n$. Therefore, by treating the congruent for arbitrary integer $n$ we can approach to rank of elliptic curve $E_n$. In [8], Nemenzo suggested that

| $s_n$ | $r_n$ | $No.\ of\ curves$ $E_n\ with\ n$ <100000 |
|---|---|---|
| 4 | 4 | 4 |
| 3 | 3 | 177 |
| 3 | $3 \leq r_n \leq 5$ | 8 |
| 2 | $1 \leq r_n \leq 2$ | 1558($n$ <42553) |
| 2 | $1 \leq r_n \leq 4$ | 107 ($n < 42553$) |
| 2 | $0 \leq r_n \leq 2$ | 1767 ($n \geq 42553$) |
| 2 | $0 \leq r_n \leq 4$ | 244 ($n \geq 42553$) |
| 1 | 1 | 30220 |
| 0 | 0 | 26729 |

($s_n$ denotes Hasse-Weil $L$ -function $L(E_n, s)'s$ order $s_n$ of vanishing at $s = 1$ and $r_n$ is rank of $E_n: y^2 = x^3 - n^2x)$ .)

In addition, Lemmermeyer showed that for prime $p \equiv 1(mod\ 8)$ and elliptic curve $E: y^2 = x(x^2 - 4p^2)$ the Selmer groups are $Sel^{(\psi)}(\hat{E}/Q)$=$< -1,\ 2,\ p >$ and $Sel^{(\phi)}(E/Q)$=$< p >$ and if prime $p$ is given as $p \equiv 9(mod\ 16)$ then, there derived the consequences $III(E/Q)[2] \simeq III(\hat{E}/Q)[2] \simeq (Z/2Z)^2$ ([6]). In [1], under the supposition that the curve $E: y^2 = x(x^2 - n^2)$ is an elliptic curve with $n \geq 1$ is an integer, the authors dealt with the problem of finding three integral points $P_1$ and $P_2$ and $P_3$ whose $x$ -coordinates $x_i = x(P_i)$ form an arithmetic progression with $x_1 < x_2 < x_3$. If $n \geq 1$ is a squarefree integer and $\Gamma \subset E(Q)$ is a subgroup of rank 1 then, $\Gamma$ contains no non-trivial integral arithmetic progressions([1]). There are no arithmetic progressions $(P_1, P_2, P_3)$ on $E$ when one of the points $P_i$ is equal to the torsion point $T_2 = (0, 0)$ and the other two points are non-torsion([1]).

**Remark 2.3.** In structure $E(Q) \cong E(Q)_{tors} \oplus Z^r$, torsion part is one component of $E(Q)$. In previous theorem, we only considered the rank of elliptic curve but it is needed to notice the torsion points. In [3], Dujella showed that the torsion points in $E_k{}': y^2 = x^3 + (9k^2 - 1)x^2 + 24k^2(k^2 - 1)x + 16\ k^2(k^2 - 1)^2$ are isomorphic to Z/2Z⊕Z/2Z. In [7], Lemmermeyer suggested that torsion points of *Mordell* elliptic curve $y^2 = x^3 + 1$ is $E(Q)_{tors}$≃Z/6Z. In [9], Robledo presented the followings:

| $Curve$ | $Torsion$ | $Generators$ |
|---|---|---|
| $y^2 = x^3 - 2$ | $trivial$ | $O$ |
| $y^2 = x^3 + 8$ | Z/2Z | $(-2, 0)$ |
| $y^2 = x^3 + 4$ | Z/3Z | (0, 2) |
| $y^2 = x^3 + 4x$ | Z/4Z | (2, 4) |
| $y^2 - y = x^3 - x^2$ | Z/5Z | (0, 1) |
| $y^2 = x^3 + 1$ | Z/6Z | (2, 3) |
| $y^2 = x^3 - 43x+166$ | Z/7Z | (3, 8) |
| $y^2 + 7xy = x^3 + 16x$ | Z/8Z | $(-2, 10)$ |
| $y^2 + xy + y$ $= x^3 - x^2 - 14x + 29$ | Z/9Z | (3, 1) |
| $y^2 + xy$ $= x^3 - 45x + 81$ | Z/10Z | (0, 9) |
| $y^2 + 43xy - 210y$ $= x^3 - 210x^2$ | Z/12Z | (0, 210) |
| $y^2 = x^3 - 4x$ | Z/2Z⊕Z/2Z | (2, 0), (0, 0) |
| $y^2 = x^3 + 2x^2 - 3x$ | Z/4Z⊕Z/2Z | (3, 6), (0, 0) |
| $y^2 + 5xy - 6y$ $= x^3 - 3x^2$ | Z/6Z⊕Z/2Z | $(-3, 18), (2, -2)$ |
| $y^2 + 17xy - 120y$ $= x^3 - 60x^2$ | Z/8Z⊕Z/2Z | $(30, -90), (-40, 400)$ |

## 4 Examples

In section 3, examples of theorem 2.1 will be suggested. The primes were checked in [2].

The followings are examples of theorem 2.1(1) :

| $(p, u, v)$ |
|---|
| (67, 2, 1) |
| (563, 2, 3) |
| (643, 4, 1) |
| (1907, 4, 3) |
| (2707, 2, 5) |
| (8803, 2, 7) |
| (13043, 8, 3) |
| (107827, 4, 13) |
| (1118563, 8, 23) |
| (29008867, 8, 55) |
| (129350147, 2, 81) |

Examples of theorem 2.1(2) are given as :

| $(p, u, v)$ |
|---|
| (643, 2, 1) |
| (5827, 4, 1) |
| (383683, 12, 1) |
| (4251523, 22, 1) |
| (11120323, 28, 1) |
| (46195267, 40, 1) |

Some examples of theorems 2.1(3) are the followings::

| $(p, u, v)$ |
|---|
| (6323, 2, 3) |
| (26083, 2, 7) |
| (85843, 2, 11) |
| (142963, 2, 13) |
| (2394163, 2, 29) |
| (32710883, 2, 57) |
| (42731443, 2, 61) |
| (48532163, 2, 63) |
| (77851363, 2, 71) |
| (396905683, 2, 107) |

We have examples of theorems 2.1(4):

| $(p, u, v)$ |
|---|
| (107, 1, 1) |
| (36587, 1, 11) |
| (67307, 1, 13) |

## References

[1] A. Bremner and J. H. Silverman and N. Tzanakis, Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$, *J. of Number theory*, **80** (2000), 187-208. https://doi.org/10.1006/jnth.1999.2430

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

[3] A. Dujella, A parametric family of elliptic curves, *Acta Arith*, *XCIV* (2000), 87-101. https://doi.org/10.4064/aa-94-1-87-101

[4] A. J. Hollier and B. K. Spearman and Q. Yang, Elliptic curves $y^2 = x^3 + pqx$ with maximal rank, *Int. Math. Forum,* **5** (2010), 1105-1110.

[5] 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

[6] F. Lemmermeyer, Some families of non-congruent numbers, *Acta Arith.*, **110** (2003), 15 - 36. https://doi.org/10.4064/aa110-1-2

[7] F. Lemmermeyer, Introduction to elliptic curves, 2003, *preprint*.

[8] F. R. Nemenzo, All congruent numbers less than 40000, *Proc. Japan Acad. Ser. A Math. Sci.,* **74** (1998), 29 - 31. https://doi.org/10.3792/pjaa.74.29

[9] A. L. Robledo, Elliptic curves, modular form, and their *L*-functions, *AMS, Student mathematical library; IAS/Park city mathematical subseries,* **58** (2011).

[10] 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: March 14, 2019; Published: April 17, 2019**