Advances in Computer, Signals and Systems (2021) 5: 1-4
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2021.050201
ISSN 2371-8838

Patterns of Points on Specific Elliptic Curves in Finite Field

Shutong Lu

Ulink College of Shanghai, Shanghai, China

Keywords: Elliptic curve, Finite field, Pythagorean triple

Abstract:In the process of finding Pythagorean triangular numbers, we can imagine a related problem about how many triples exist with a nonzero constant difference between the square of these triples. In fact, it requires more calculations and theory of elliptic curves. Although it is difficult to find all such triples with fixed differences in the field of real numbers, to find them in finite fields can be handled without using very advanced or Abstractmathematics. This dissertation is going to find the general pattern of solutions of some specific elliptic curves in finite field.

1. Introduction

Pythagoras triangle numbers refer to triples which satisfy:

$$X^2+Y^2=Z^2(X,Y,Z\in N) \quad (1)$$

It was first recorded in Plimpton 322 in Babylonian tablet at around 1800 BC, which was one of the most famous artefacts in terms of mathematics. Babylonian, at that time, discovered a way to create the length of three sides of triangles. They set the square of one side to be equal to the sum of the square of two other sides. [1]

According to Euclid's formula, three sides of a right triangle have a general formula

$$a=2mn, b=m^2-n^2, c=m^2+n^2 \quad (2)$$

It also means that for any given whole number *m* & *n*, we can find a specific right triangle. As a result, there should be infinite number of right triangles with different length of three sides.

However, the problem investigated in this dissertation is how many positive triples exist with nonzero fixed difference between the square of these three numbers. In other words, how many triples have the property that

$$Z^2-Y^2=Y^2-X^2 \quad (3)$$

But this statement has not been elaborated. Given that *(A, B, C)* is a triple which has property (3), *(kA, kB, kC)* must also be a such triple if $k\in N^+$, so that infinite number of these triples occur.

Therefore, we shall add one more restriction to the problem-- $\gcd(A,B,C)=1$. After some calculation, the general formula for these special triples are

$$\frac{A}{B}=\left|\frac{m^2-2m-1}{1+m^2}\right|, \frac{C}{B}=\left|\frac{1-2m-m^2}{m^2+1}\right|$$

After that, a further problem can be how many of these triples (3) exist with a fixed difference

$d \in N^+$ between the square of three numbers. With some calculation, it can be transformed into another problem: How many rational points exist on

$$dy^2 = x^3 - x \quad (4)$$

This dissertation is going to find some basic conjectures of solution in elliptic curves (4) with different coefficients *d* in the modulus field, and also expand the general law to larger values of *d*.

Acknowledgment. This dissertation was written with the guidance of professor Márton Hablicsek and teaching assistant Zetong Liu during an mathematical research program for high school students.

2. Design of the Code

All data and findings are mainly derived from a series of Python code which will be listed in the appendix, and explanation of the code will be stated as follow.

The *p* needs to be a prime number according to our assumption, 'def isprime(N)' is an important process to ensure that all *p* we input is a prime number. As the only divisor of the prime number is 1 and itself, we divide all number from 2 to $\sqrt{p}$ to *p* itself, and if p can be divided by any number, we break this cycle and state that the number is not a prime number.

The core procedure in the code is definitely finding out the number of solutions for different values of p and d. 'for *x* in range *(0,par.p)*' and 'for *y* in range*(0,par.p)*' is two cycles which tests the validity of all possible integer points in this particular finite field . All valid points on the elliptic curve must satisfy

$$dy^2 \equiv x^3 - x \pmod{p} \quad (5)$$

In the code, if $dy^2 - (x^3 - x) \equiv 0 \pmod{p}$, the pair of *x* and *y* should be one of valid points on this elliptic curve.

There are some theorem used in this dissertation.

Theorem 2.1 *Sum of Two Squares Theorem for Primes*

Let *p* be a prime. Then *p* is a sum of two squares if and only if

$$p \equiv 1 \pmod{4} \text{ or } p = 2 \quad (6)$$

Moreover, it is worth mentioning that, except for 2, all prime numbers are odd, and thus two squares adding up to *p* must include one odd number and one even number.

Theorem 2.2 *Quadratic Residue Theorem*

Let p be a prime. Then $x^2 \equiv 0 \pmod{p}$ if and only if $x \equiv 0 \pmod{p}$, and for $1 \le x \le p-1$, half of these values are quadratic residue and half of them are not.

3. Number of Solutions

Sample base chosen in the project is p the prime from 2 to 200, and the coefficient d chosen is from 1 to 50, which is enough to find the general pattern.

The first significant pattern existing in these elliptic curves is the number of solutions when $p \equiv 3 \pmod{4}$, and surprisingly, it does not matter what the value of d is. For example, the number of solutions given that $d = 1, p = 3$ is 3, and the counterpart when $d = 1, p \equiv 7$ is 7. Most importantly, no matter how d changes, as long as the p we choose has a remainder of 3 when divided by 4, the number of solutions always equal to the *p* itself.

The second pattern observed in the group of data is related to the number of solutions when $p \equiv 1 \pmod{4}$. At first, it seems a bit messy when $p \equiv 1 \pmod{4}$. For instance, when *p*=5, *d*=1, the number of solutions is 7, and the number of solutions becomes 15 when *p* and *d* are respectively 17

and 1. In other words, the number of solutions is never equal top, which is quite different from the first case.

However, after trying to research the defect(*N-p*) between *p* and the number of solutions *N*, Some patterns appear out. In the case of *d*=1, the corresponding defect of *p*=5 is 2, *p*=13 is -6, *p*=17 is -2, and *p*=29 is 10. Theorem 2.1 tell us that these are the primes that can be written as a sum of two squares $p = A^2 + B^2$. Comparing the result to the sum of two square theorem for primes (6), there exists some relationship between the half of defect's absolute value and *p* itself.

For instance, as the number stated above, we can easily observe that the quantity $p - (\frac{N-p}{2})^2$ is always a perfect square.

Another question is when (*N-p*) is positive and when it becomes negative. Hence, if we write $p = a^2 + b^2$ with a positive and odd, then $N - p = -2a$ if $a \equiv 1(\text{mod } 4)$ and $N - p = 2a$ if $a \equiv 3(\text{mod } 4)$.

Above all, from the observation of prime numbers from 0 to 200, the conclusion comes out to be Result 3.1.1

Conjecture 3.1.1 *When d=1, the sign of N-p(defect) has the following pattern.*

(1)If $p \equiv 1(\text{mod } 4)$, *write* $p = a^2 + b^2$ *with a positive and odd, then*

$a \equiv 1(mod\ 4), b \equiv 0(mod\ 4)$ *defect=-2a*

$a \equiv 1(mod\ 4), b \equiv 2(mod\ 4)$ *defect=2a*

$a \equiv 3(mod\ 4), b \equiv 0(mod\ 4)$ *defect=2a*

$a \equiv 3(mod\ 4), b \equiv 2(mod\ 4)$ *defect=-2a*

(2) If $p \equiv 3(\text{mod } 4)$ *,defect=0, in other words, N=p*

In the process of expanding the result of *d*=1 to a larger value of *d*, for all values of *d* which do not show a consistency in terms of the sign of *N-p* when *a* and *b* ($p = a^2 + b^2$, with a positive and odd) is congruent modulus 4, we call such *d* 'irregular'. In fact, quite a large proportion of values of *p* do not show any general pattern. For example, in the specific case where *d*=3, defect is -2 when *p*=5, 2 when *p*=37. However, write $5 = 1^2 + 2^2$ and $37 = 1^2 + 6^2$, we can see that 2 and 6 are congruent modulus 4, which means that these two defects are not consistent with sign although their *a* and *b* are congruent. As a result, *d*=3 is 'irregular'.

However, except for 'irregular' *d*, other numbers still show some interesting relationship between the number of solutions and the value of *p*. There are mainly two groups of d, and d inside each group show exactly the same pattern. Group 1 is called 'Square Group', where $d = n^2, n \in N^+$ and Group 2 is called 'Double Square Group', where $d = 2n^2, n \in N^+$.

Results in two different groups are stated below.

Conjecture 3.1.2 *If d belongs to the 'Square Group', for* $p \equiv 1(\text{mod } 4)$, *write* $p = a^2 + b^2$ *with a positive and odd,*

(1) If $a \equiv 1(\text{mod } 4), b \equiv 0(\text{mod } 4)$ *or* $a \equiv 3(\text{mod } 4), b \equiv 2(\text{mod } 4)$, *then defect=-2a*

(2) If $a \equiv 1(\text{mod } 4), b \equiv 2(\text{mod } 4)$ *or* $a \equiv 3(\text{mod } 4), b \equiv 0(\text{mod } 4)$, *then defect=2a.*

For $p \equiv 3(\text{mod } 4)$,

defect=0, in other words, N=p

If d belongs to the 'Double Square Group',for $p \equiv 1(\text{mod } 4)$, *and* $p = a^2 + b^2$, *with a positive and odd,*

(1) $a \equiv 1(\text{mod } 4)$ *defect=-2a*

(2) $a \equiv 3(\text{mod } 4)$ *defect=2a.*

For $p \equiv 3(\text{mod } 4)$ *,defect=0, in other words, N=p.*

If d is 'irregular', no pattern exists for $p \equiv 1(\text{mod } 4)$.

However, for $p \equiv 3 (\mathrm{mod}\, 4)$,defect=0, in other words, N=p

4. Coordinates Pattern of Solutions

In this sector, the main focus is on the case where *d*=1 and $p \equiv 3 (\mathrm{mod}\, 4)$, because it is beyond the scope of this essay to investigate the reason of defect $(N - p)$, and some patterns of quadratic residue no longer holds when $d > 1$.

It is clear that three points must be on the elliptic curve(5) in the finite field in any cases where *d*=1, respectively (0,0),(1,0) and (*p*-1,0). It is easy to prove the first two one. For the last one, we just need to translate *p*-1 to -1 as they are congruent modulus *p*, and then we get $(-1)^3 - (-1) = 0$. I claim that the *y*-coordinate equals to 0 only in these three cases, which will be shown in Theorem 4.1

Theorem 4.1 *For any values of prime number p, y-coordinate in all valid points are zero if and only if x=0 or x=1 or x=p-1.*

Proof Assume there exists a $2 \le m \le p-1$ which creates a valid point(m,0). It means that $m^3 - m \equiv 0 (\mathrm{mod}\, p)$, so that $m(m^2 - 1) \equiv 0 (\mathrm{mod}\, p)$. Hence, $p \mid m(m^2 - 1)$, as p is a prime either $p \mid m$ or $p \mid m^2 - 1$. But as m<p, m can never divided by p; $m^2 - 1 = (m+1)(m-1)$, so $p \mid m+1$ or $p \mid m-1$, for $2 \le m \le p-1$, the only chance for this to hold is *m*=*p*-1, which completes the proof.

Through observation of all valid points in the first few values of *d*, except for *x*=0, *x*=1, *x*=*p-1*, all other coordinates appear in pair with same value of *x*. This is easy to guess with the quadratic residue theorem. Once the value of $x^3 - x$ is congruent to y^2, *y* can then have two distinct values.

Furthermore, different *x*, besides 0,1, *p*-1, may create the same value of $x^3 - x$, and this phenomenon occur for every $p \ge 11$ in the case where *d*=1. For example, when *d*=1 and *p*=11, *x*=2 and *x*=7 responds to the same value 6 for $x^3 - x$. Hence, *p*=7 is the only special case where different x creates different values of $x^3 - x$. Result 4.1 will show some general patterns for coordinates of solutions for *d*=1 and $p \equiv 3 (\mathrm{mod}\, 4)$.

Conjecture 4.1 *For d=1 and $p \equiv 3 (\mathrm{mod}\, 4)$ .Except x=0,1,p-1, we define all x which has the same value of $x^3 - x$ as some other x as S_1, and the remaining as S_2.*

The x-coordinates of valid coordinates include

(1)0,1,p-1

(2)Half of x in S_1, occuring in pairs as one x corresponds to two valid y values

(3)Half of x in S_2, occuring in pairs for the same reason

5. Conclusion

This project used sufficient number of experiments with Python codes to find out some general patterns of the number of solutions (valid coordinates) depending on the value of *d* and *p*, which was discussed in conjecture 3.1.2. Moreover, the patterns of *x*-coordinates in the situation where $d \equiv 1, p \equiv 3 (\mathrm{mod}\, 4)$ was mentioned in conjecture 3.2.1. Since the academic level of author is limited, the project cannot give a further proof for patterns observed, and I sincerely hope that readers who have access to more advanced academic knowledge can help to prove the conjecture.

References

[1] Robson Eleanor. Mathematical Association of America Monthly, no.02, pp.105-120, 2002.