Elliptic Curve Cryptography

Sai Manoj

02/02/2022

1 Introduction

1.1 Why elliptic curves ?

A recent shift observed is that the crypto community is quickly moving away from the RSA standard. People have started to crack secure keys by factoring huge numbers. *ECC (Elliptic Curve Cryptography)* achieves higher security with lesser keys.

1.2 Equations

Solving equations, or a system of equations is one of the most commonly faced problems in all of mathematics. We can describe an elliptic curve as a cubic function in two variables.

A simple elliptic curve can be represented by

$$y^2 = x^3 + ax + b$$

1.3 Example : Pyramid of balls

The points $(0, 0)$ and $(1, 1)$ lie on the elliptic curve, and the line joining these two points is $y = x$. We substitute this line into the curve to find more points

$$x^2 = \frac{x(x+1)(2x+1)}{6}$$

Two roots of this curve are $0, 1$, and the third root will be $\frac{1}{2}$. This is the method of Diophantus. Redoing this method will eventually result in the solution $x = 24, y = 70$.

Doubt :- If we are able to find two points (does this happen every time), Can we keep finding points from the line joining these two points ? In the next example, we see that it doesn't work for the

1.4 Example-2

The elliptic curve is $y^2 = x^3 - 25x$ The three obvious points on the curve are $(-5,0),(0,0),(5,0)$. But the lines from this do not result in new points on the elliptic curve.

The only point that we can find after some trial and error is $x = -4, y = 6$. Now, joining this point with the other three points, we get three lines, which we can substitute in the elliptic curve equation. But this doesn't result in any new points.

So, the method that we use here is that we consider the tangent line at this point (and the slope is obtained by differentiating the curve). This results in more points on the elliptic curve.

1.5 Congruent Number Problem

For a whole number N, does there exist a^2 such that both $a^2 - N$ and $a^2 + N$ are both squares ?

t-congruent number : - A rational number n is called t-congruent if there exists positive rational numbers a, b, c such that

$$a^2 = b^2 + c^2 - 2bc(\frac{t^2-1}{t^2+1}) \qquad 2n = bc(\frac{2t}{t^2+1})$$

This idea comes from a triangle of rational sides and area (also known as a Heron's triangle).

An integer n is square-free if it is not a multiple of any perfect square other than 1.

Theorem : - Any square-free positive integer n is a t-congruent number for some positive rational number t.

There is another theorem that relates t-congruent numbers and elliptic curves.

Theorem : -

For a fixed positive rational number t, n is a t-congruent number *if and only if*

i. Either both $\frac{n}{t}$ and $t^2 + 1$ are rational squares

ii. Or the elliptic curve $y^2 = (x)(x - \frac{n}{t})(x + nt)$ has a rational point

Reference from : https ://www.math.hkust.edu.hk/ yangwang/Course/2016FSMath4999

2 Exercises

2.1 Question - 1

We have to use induction to show that the sum of the first x positive integers is $\frac{x(x+1)(2x+1)}{6}$.
The base case, when $x = 1$ is true because $1^2 = \frac{1(2)(3)}{6}$. Let the statement be true for the first x integers. Now, we have to prove the statement for the first $x + 1$ integers. $1^2 + 2^2 + ... + x^2 = \frac{x(x+1)(2x+1)}{6}$
$1^2 + 2^2 + ... + x^2 + (x + 1)^2 = \frac{x(x+1)(2x+1)}{6}$
$= (x + 1)(\frac{x(2x+1)}{6} + (x + 1))$
$= (x + 1)(\frac{x^2}{3} + \frac{x}{6} + x + 1)$
$= (\frac{1}{6})(x + 1)(2x^2 + 7x + 6)$
$= (\frac{1}{6})(x + 1)(2x^2 + 4x + 3x + 6)$
$= (\frac{1}{6})(x + 1)(x + 2)(2x + 3)$
$= \frac{(x+1)(x+2)(2(x+1)+1)}{6}$
The statement is true for the case of $x + 1$ integers. Hence, the statement is true for all integers $x >= 0$.

2.2 Question - 2 (a)

The given elliptic curve is $y^2 = x^3 - 25x$. We have found the point $(-4, 6)$ by some trial and error before. Using the tangent line, we find the point where $x = \frac{25}{4}, y = \frac{75}{4}$.
$\frac{25}{4}$ is a square, but $x + 5 = \frac{45}{4}$ and $x - 5 = \frac{5}{4}$ are not squares. l

Even though we have derived the elliptic curve from the condition that $x - 5, x, x + 5$ have to be squares, it is not equivalent to saying that every point on the ellipse will satisfy this property.