Problem 1:

Analysis of this equation mathematically:

*y2 = x3+7*

* Implies x < y
* Y = sqrt(cube(x) + 7)

Some sample values:

|  |  |
| --- | --- |
| X | sqrt(cube(x) + 7) = y |
| -999 | -31575.3544 |
| -15 | -58.1549 |
| -1 | -2.8284 |
| 0 | 2.6457 |
| 1 | 2.8284 |
| 15 | 58.1549 |
| 250 | 3952.8479 |
| 999 | 31575.3544 |

Graph:

Technical analysis

**Task1: Find two points on the curve *P1(x1, y1)* and *P2(x2, y2)***

Create method that takes value of x and finds value of y using below equation. It returns Point object that contains (x, y) coordinates.

*y* = sqrt(*x3* + 7)

**Task2: Define vectors**

-> ->

*a =* *P0P1* and*b =* *P0P2*

Create a method that takes 2 points as parameter and calculates vector for those points as below:

Vector from P0 to P1 = [x1-x0, y1-y0]

**Task3: Calculate the length of vector**

Create method that takes 2 vectors as parameter and returns length of distance between those vectors.

Length of a vector = sqr(x) + sqr(y)

Distance between two vectors = length of (vector b – vector a) = sqr(xb – xa) + sqr(yb – ya)

Problem 2:

Analysis of this equation mathematically:

Given equation -> *y = f(x) mod p*

When *f(x) = a0 + a1x + a2x2 +a3x3+…+ak-1xk-1*

And constant term S = a0 and Degree of polynomial = *k-1*

Graph (3rd order) for data points :->

|  |  |  |  |
| --- | --- | --- | --- |
| X | 1 | 2 | 3 |
| Y | 1494 | 2329 | 3965 |

Observation:

* We can use Langrage interpolation to find coefficients i.e. Lagrange terms [a0, a1, a2 … an]
* Requirement is to calculate a0 using Lagrange interpolation formula (symbol of *Π* denotes multiplication) for a0 as follows:

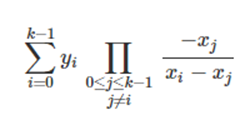
*ai (x)= [ Ʃk-1i=0  yi Π 0<=j<=k-1, j≠i (x-xj)/( xi – xj) ] mod p*

For a0 since x = 0, in above formula (x – xj) becomes (-xj). That simplifies formula to below:

*mod p*

]

[

**

*a0 =*

where *xi – xj ≠ 0*

Pseudo code to find a0 coefficient:

Given n + 1 data points (x0, y0), (x1, y1) …. (xn, yn)

And condition that j is not equal to i (i for finding a0 is 0).

For j from 0 to n, when j is not 0

* find multiplications of –x(j) as dividend
* find multiplication of (x0 – x(j)) as divisor
* find dividend / divisor as result
* multiply result by y[0] as result
* find result mod p as a0

Assumption – we can start j from 1 as i = 0, but keeping the solution generic