Improvement of Correlation amongst elliptic points in Elliptic Curve Cryptography based on Metaheuristic algorithm and Implementation on Python

Md Asim Kamal Farooqui (M.Tech student) at Center of Development of Advanced Computing ,Noida

Abstract:-Elliptic curve cryptography has paved the way for making a communication system robust and highly secure with extremely small key size. It offers equivalent safety in contrast to RSA with only short key size. The present project focuses on amalgamating the ECC (Elliptic curve cryptography) with a global search metaheuristic named PSO (Particle Swarm Optimization) and then calculating the ECC curve points. Further the correlation among the points is calculated and is compared with other correlation work involving encryption without PSO. As the correlation factor tends to minus one value, a sense of randomization in key is induced which makes the system less prone to any adversary's attack.

Introduction

1.1 Overview

Elliptic curve cryptography (ECC) give a quicker option in contrast to open key cryptography. Smaller keysizes are needed with ECC to give an ideal dimension of security, which implies more rapidly key trade, client validation, signature age and check, notwithstanding littler key stockpiling needs. The well-being of ECC has not been certified nevertheless rather it relies on the trouble of reckoning "Elliptic curve discrete logarithm Problem" in the elliptic curve gathering. Metaheuristics are structured as well as assume significant job by means of complex enhancement issues.

The present elliptic curve cryptographic approach is mugged up with a population-based metaheuristic algorithm named as Particle Swarm Optimization or simply PSO.PSO belongs to a class of stochastic algorithm. It was first developed by James Kennedy and Russel Eberhart in 1995.It is basically used in combinatorial problem optimization and is an iteration-based method. The method tries to remove some pitfalls in the the candidate solution in regard to some level of quality based on the context in which the method needs to be applied. In the present scenarios, the whole algorithm has been amalgamated with elliptic curve points generated and the main goal is to minimize the correlation coefficient amongst elliptic curve points by applying PSO on the elliptic curve equation treating the same as an objective function or fitness function. The entire approach has been implemented on Spyder (Python 3.7) as platform.

The entire approach of Particle Swarm Optimization can be depicted with the given steps: -

1.First step of Particle swarm optimization deals with initialisation of position, pi of each particle as PSO algorithm keeps multiple solution of a problem at a time depending on the context

2.The PSO algorithm is an iterative approach. In each iteration, the solution of the problem is evaluated using an objective function which in turn gives its fitness value

3.The solutions are basically the particles in the fitness graph.

4.The particle move in the search space to determine the maximum or optimal value returned by the objective function

Each particle in PSO adheres to these parameters: -

1.Position
2Velocity
3.Individual best position

Apart from these, the particle also maintains its global best in the record

In nutshell entire PSO algorithm can be summed up in three steps.

1.Calculate fitness of each particle
2.Update particle individual and global best.
3.Update particle velocity and position after each iteration.

These three steps keep on running until some stopping condition is achieved

Each particle's velocity is updated using this equation

vi(t+1)=wvi(t)+c1r1[x*i(t)-xi(t)]+c2r2[g(t)-xi(t)]…………………………1.1

Where, vi(t) is the velocity of particle at time t
xi(t) is the position of particle at time t
x*i(t) is the particle individual best solution as of time t
g(t) is best solution of swarm as of time t
i is the particle index
w is the inertial coefficient
c1 and c2 are the acceleration coefficient where 0<c1,c2<2
r1 and r2 are random values where,0<r1,r2<1

Each particle position is updated using this equation

xi(t+1)=xi(t)+vi(t+1)……………..1.2

After applying Particle Swarm Optimization and seeing gbest and pbest on elliptic curve, a set of points is obtained as X values and Y values.

X values={xi}
Y values={yi}

The correlation between X values and Y values for each large prime number is computed using general Karl Pearson correlation coefficient formulae as given below: -

$$r = r_{xy} = \frac{\mathrm{Cov}(x,y)}{S_x \times S_y}$$

OR

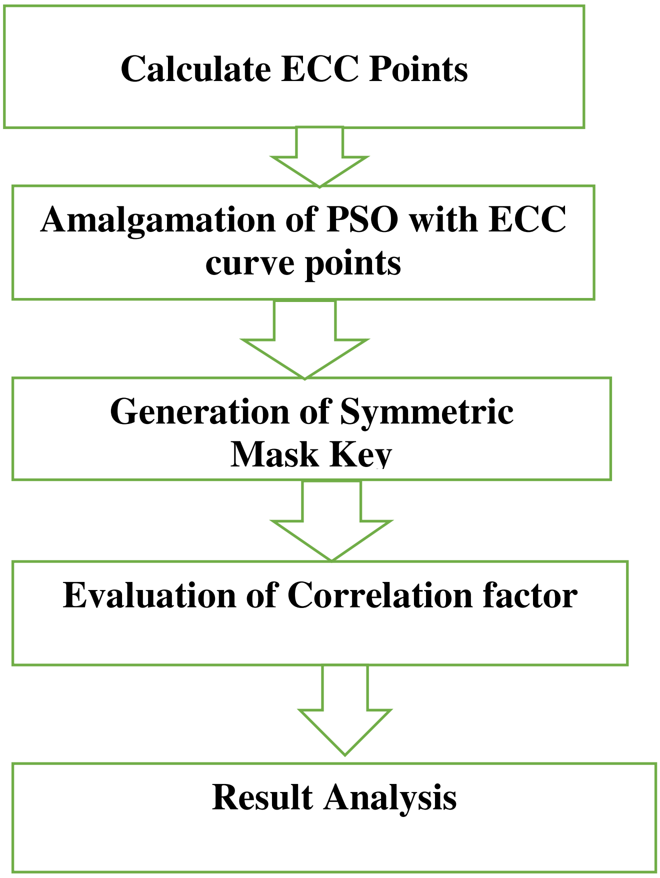
$$r = \frac{\Sigma(X-\overline{X})(Y-\overline{Y})}{\sqrt{\Sigma(X-\overline{X})^2}\sqrt{(Y-\overline{Y})^2}}$$

Where, $\overline{X}$ = mean of X variable
$\overline{Y}$ = mean of Y variable

It is observed from the calculated correlation coefficient, r valued considering different prime numbers that a level of improvement has been made when ECC generated were clubbed with PSO algorithms in comparison to alone ECC points correlation coefficient. This is the major Autocorrelation test for checking randomness amongst the elliptic curve points. Lesser the correlation value, more will be the degree of randomness in the key and lesser it will susceptible of any adversaries' attack.

Flowchart

Proposed Approach is as under



STEPS OF PROPOSED APPROACH: -

1. First and foremost step of proposed approach focuses on calculation of elliptic curve points based on following cubic equation with different prime number set.

$$y^2=x^3+a.x+b \bmod p \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 3.1$$

Where a=1.b=1 and p= {251,457,593,929}

2.On generating the elliptic curve points, it is amalgamated with global search metaheuristic named Particle Swarm Optimization [11] Algorithm to induce a sense of improvement.

3.Third step generates a symmetric mask key which is used for encryption and decryption. Here symmetric term is a misnomer as the cryptographic algorithm is using the symmetric property of elliptic curve. The key is used for signing as well as verifying purpose.

4.. Fourth step deals with calculation of correlation [8] factors of generated elliptic points and points obtained after applying PSO (Particle Swarm Optimization)

5.Last step deals with result analysis check from by comparing the correlation values of elliptic points generated and the points obtained after PSO has been applied to them and further comparsion of results with earlier work of genetic algorithm based DES,Data Encryption Standard Cryptosystem

IMPLEMENTATION

4.1 Minimum Hardware and Software prerequisites: -
Processor: Intel i3 2.10 GHz
Working System: Windows 10.
Hard Disk: 320 GB
RAM: 4 GB
Programming: Anaconda (Spyder) version 3.7

4.2Python code for computing ECC Points with different prime numbers,Pon Spyder(Python 3.7)

a) P=251

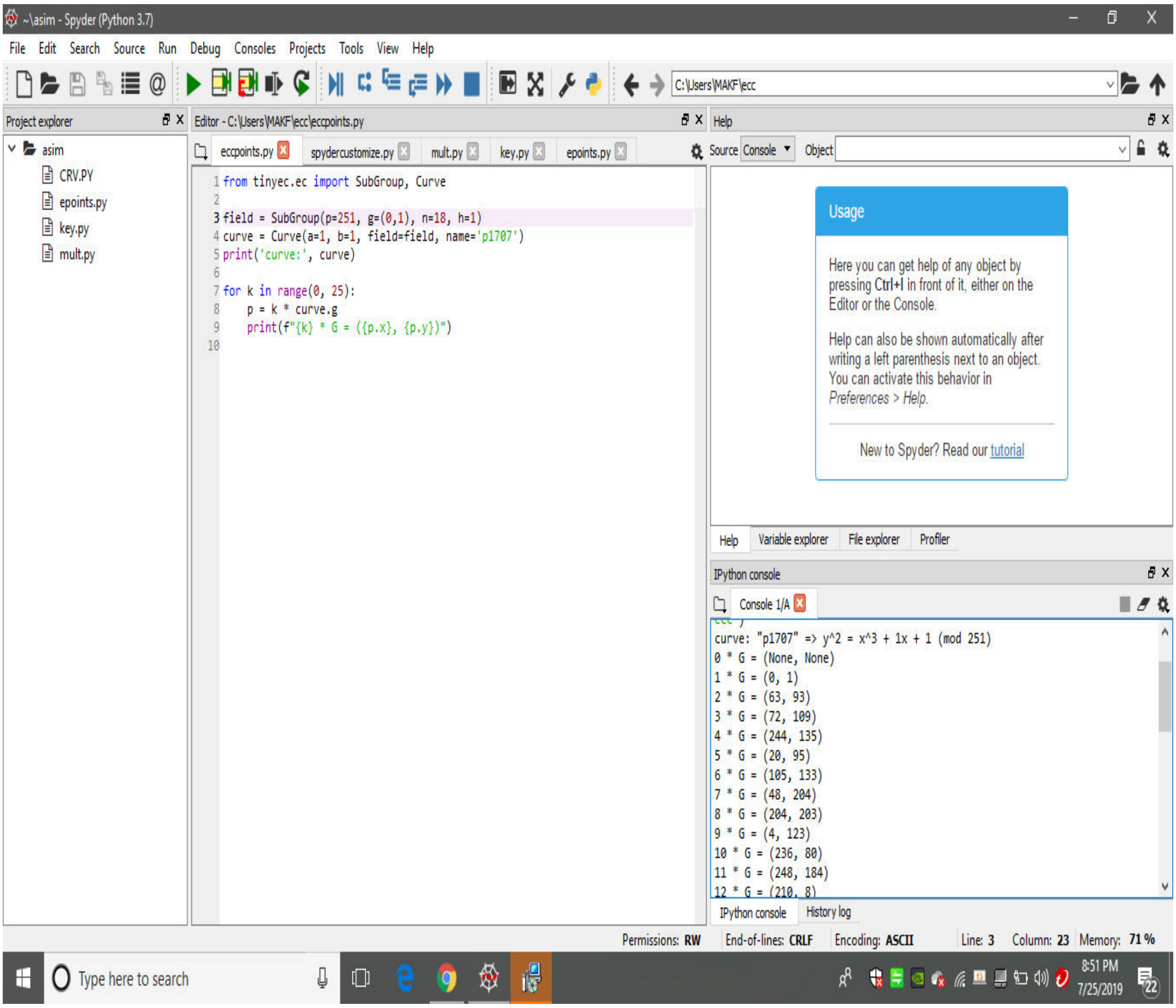


Fig.4.1.1.1 Python code for computing ECC Points with prime numbers,P=251 on Spyder(Python 3.7)

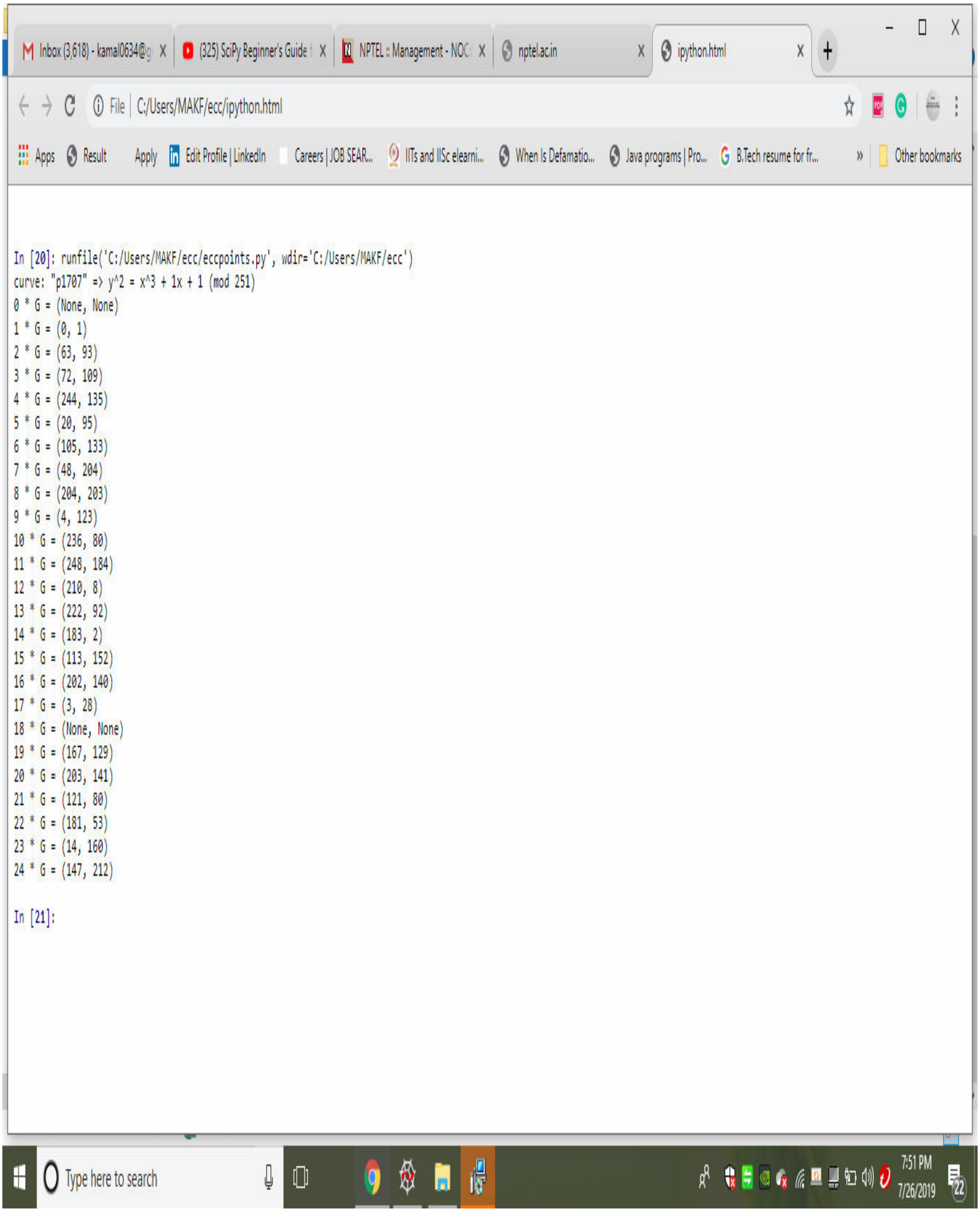


Fig. 4.1.1.2 ECC points output with P= 251

a) P=457

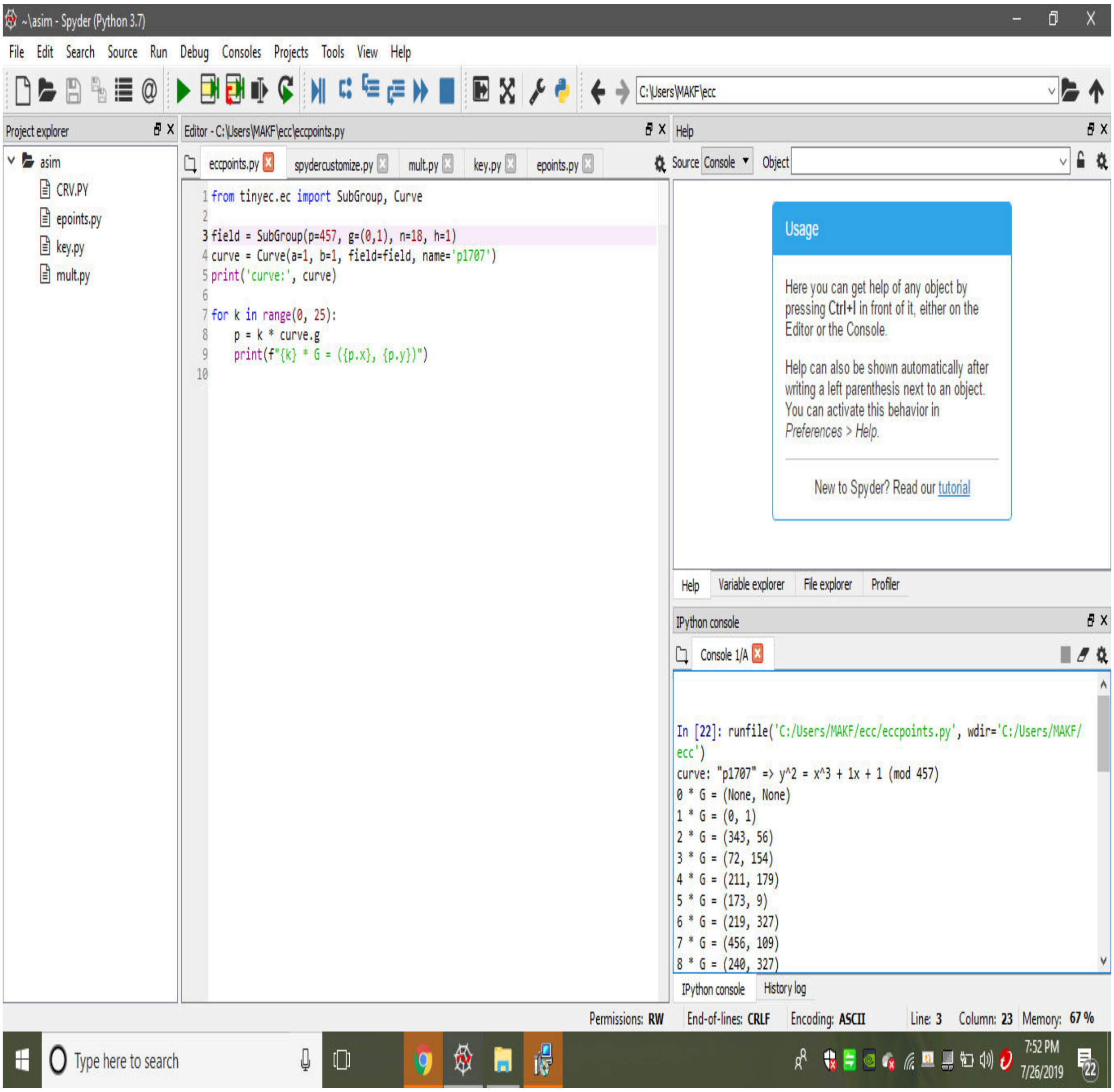


Fig.4.1.1.3 Python code for computing ECC Points with primenumber,P=457 on Spyder(Python 3.7)

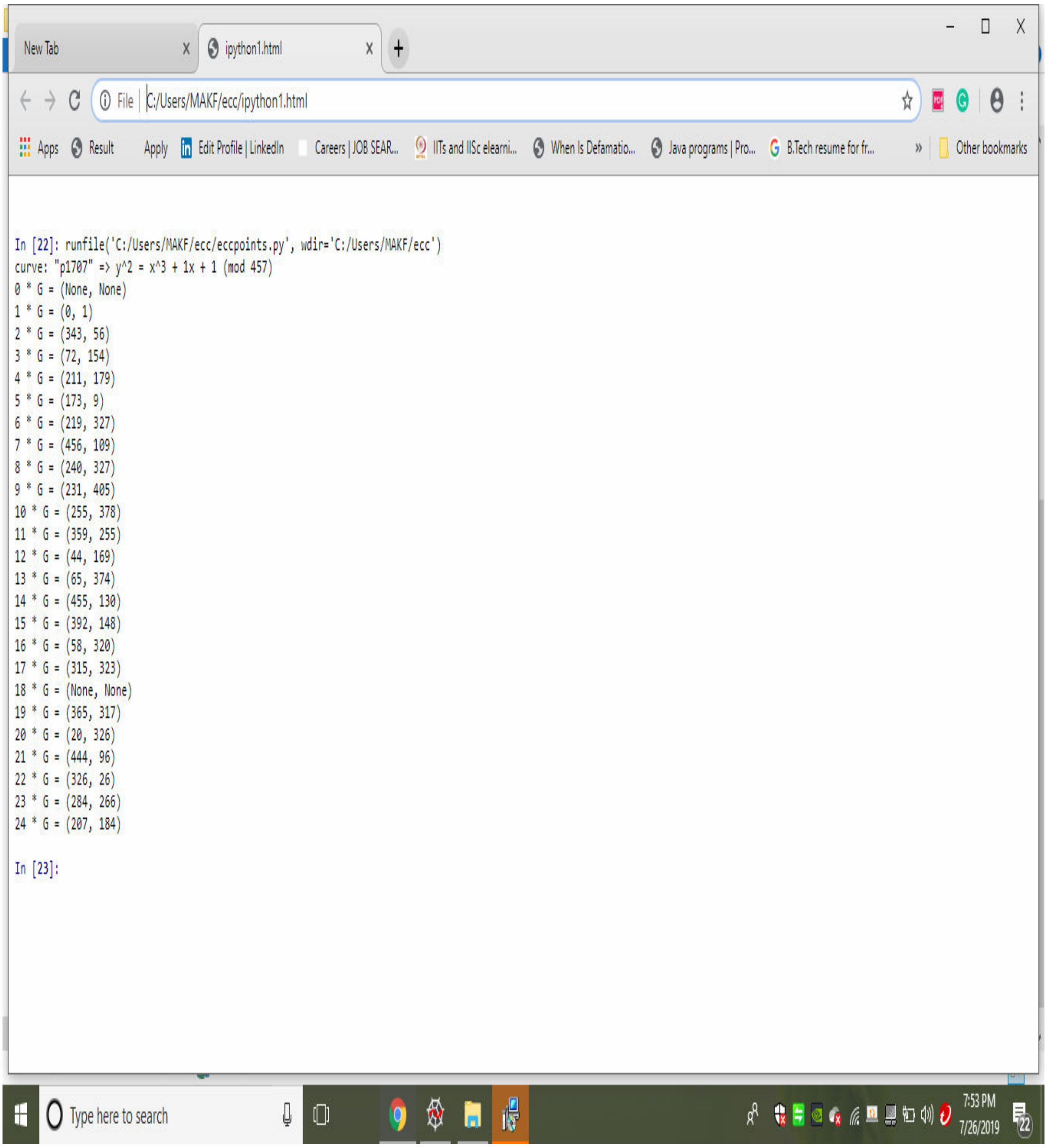


Fig. 4.1.1.4 ECC points output with P= 457

c) P=593

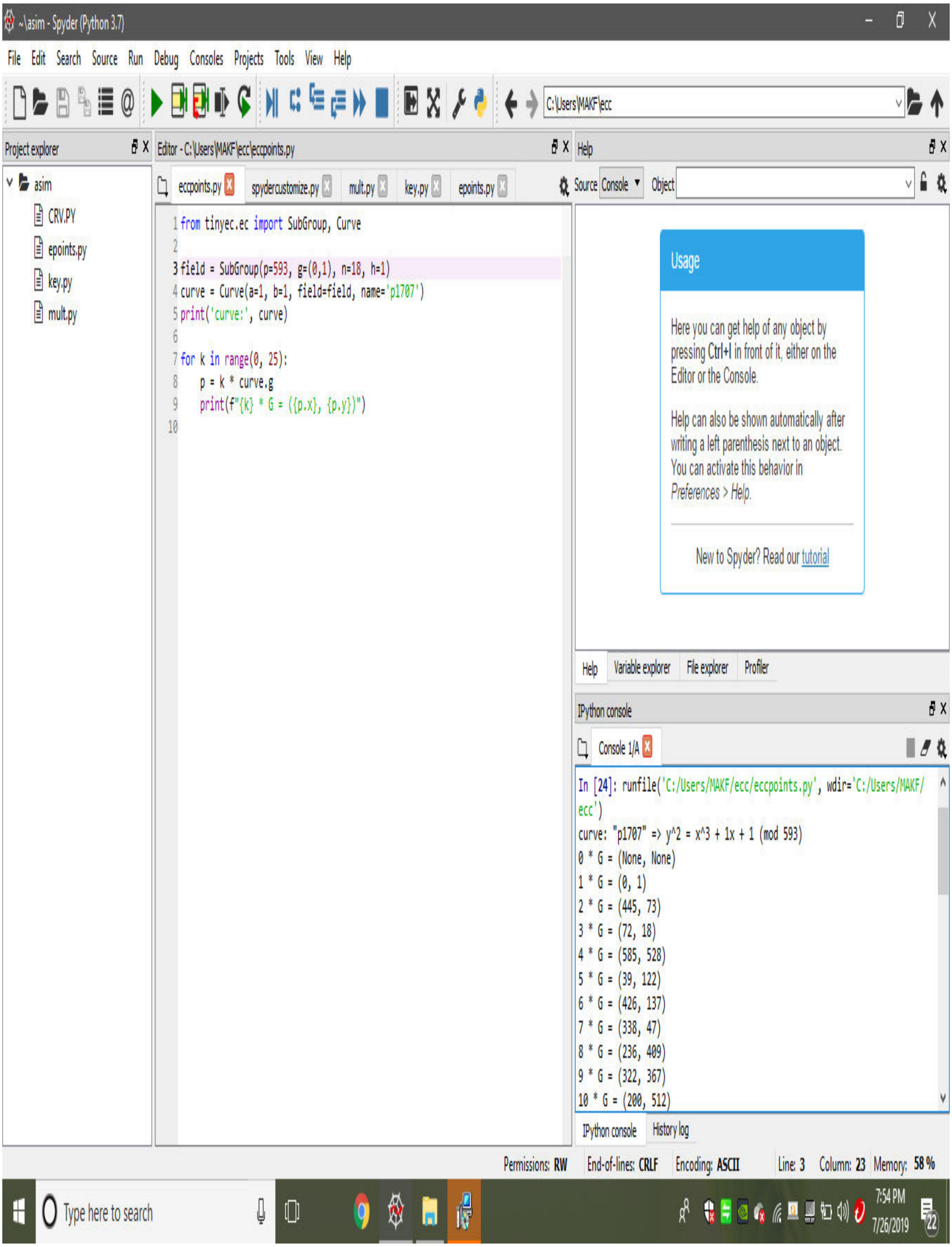


Fig.4.1.1.5 Python code for computing ECC Points with primenumber,P=593 on Spyder(Python 3.7)

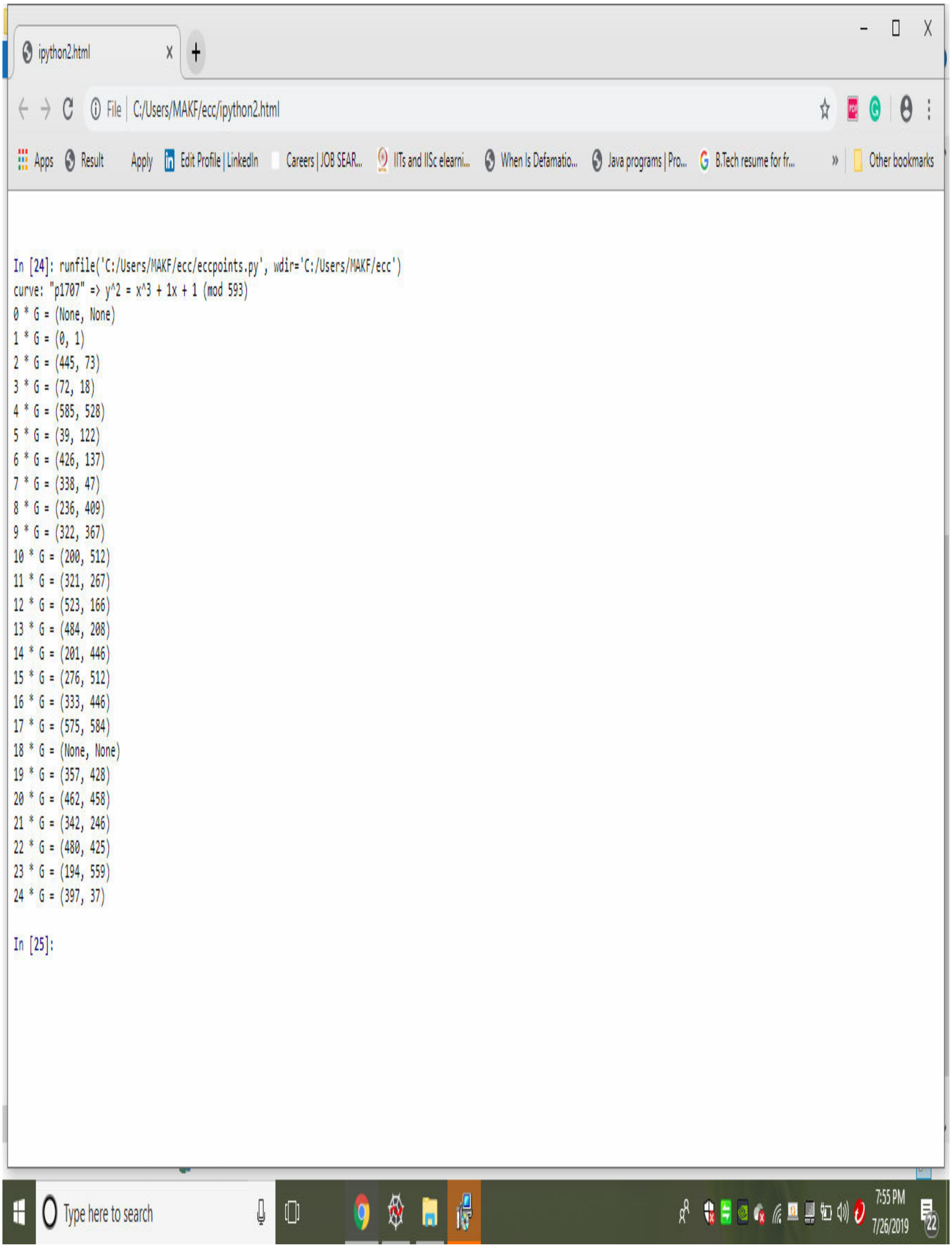


Fig. 4.1.1.6 ECC points output with P= 593

d) P=929

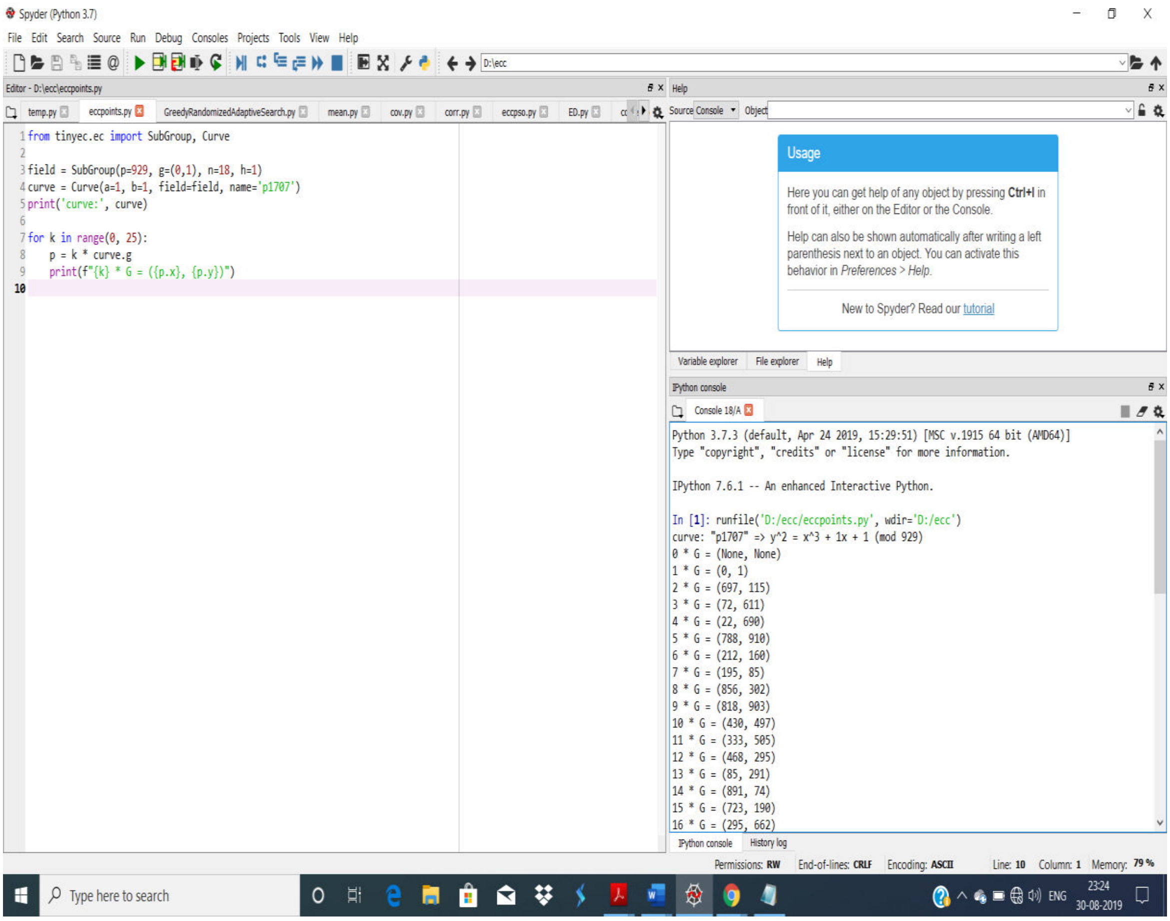


Fig.4.1.1.7 Python code for computing ECC Points with primenumber,P=929 on Spyder(Python 3.7)

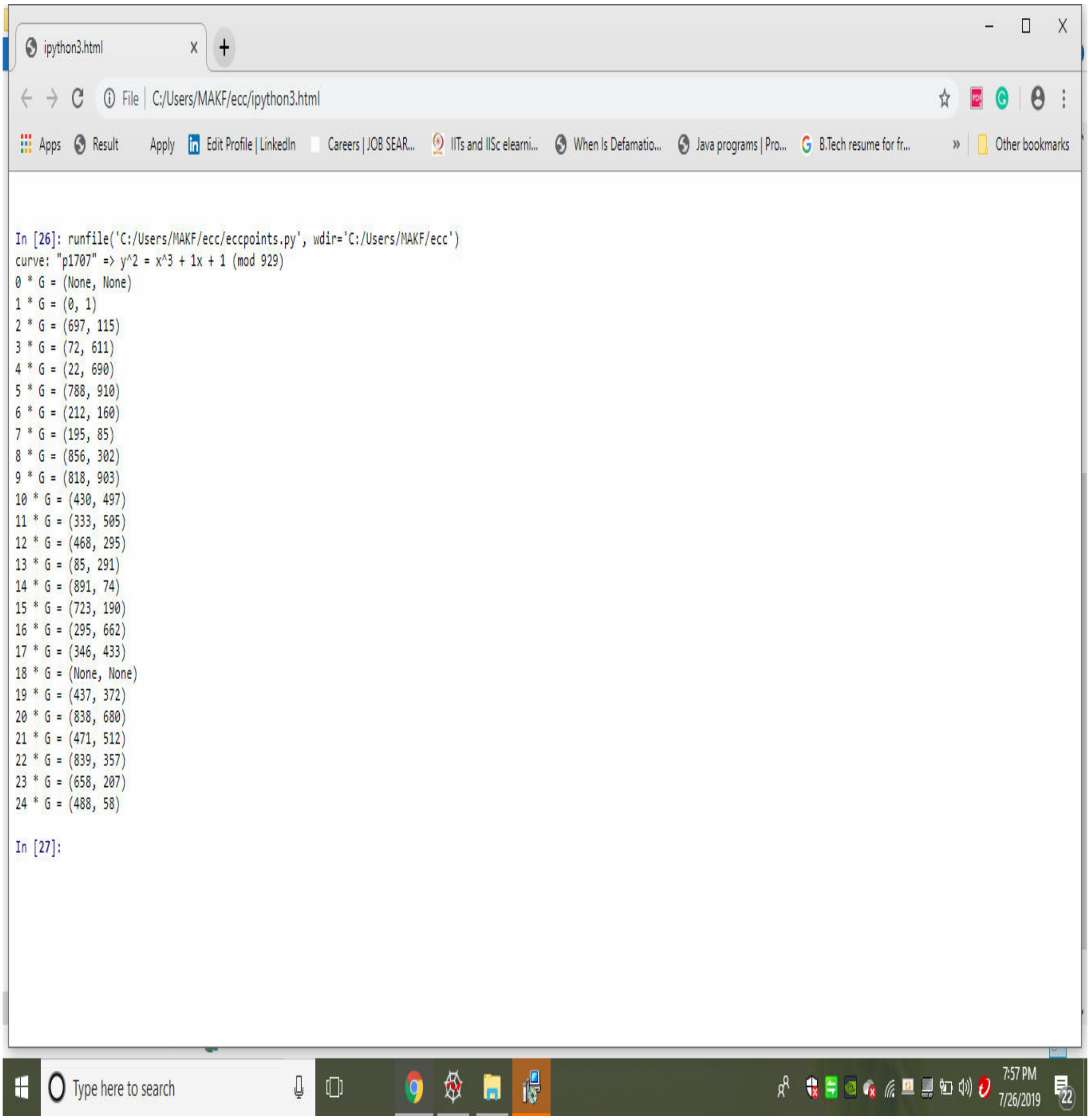


Fig.4.1.1.8 ECC points output with P= 929

4.3Python code for amalgamation of ECC points with PSO in Spyder(Python 3.7)

a) P=251

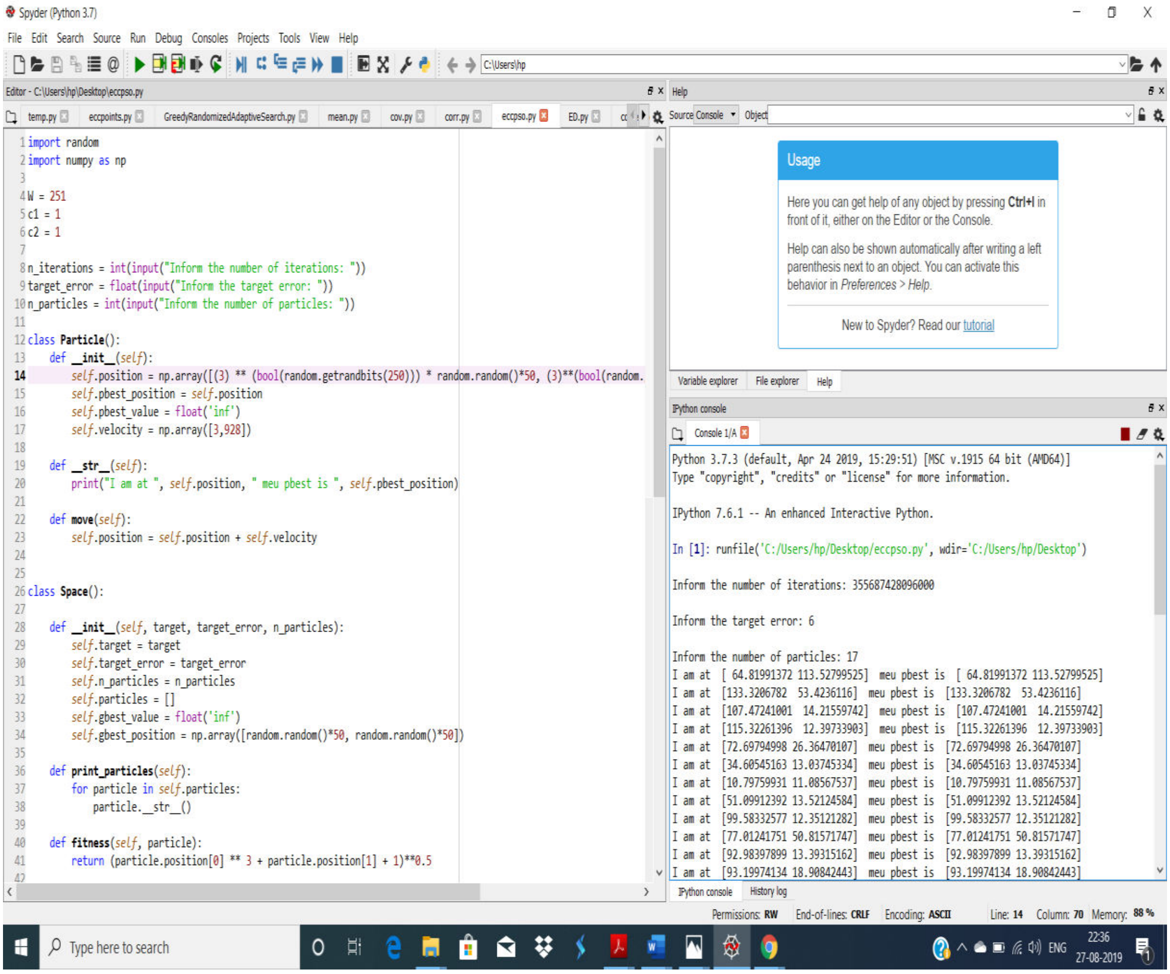


Fig.4.1.1.9 Python code for computing ECC Points with PSO with prime number,P=251 on Spyder(Python 3.7)

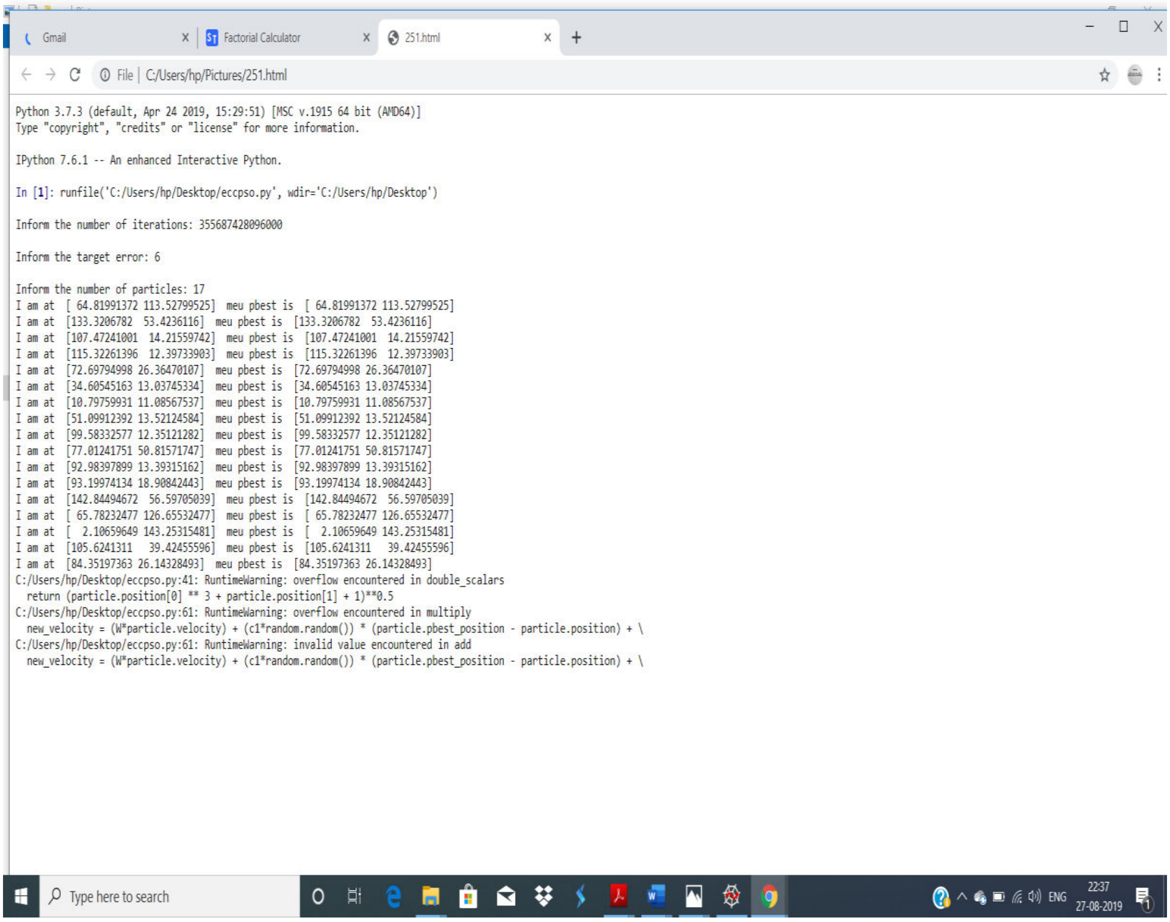


Fig.4.1.2.0 PSO output for P=251

b)P=457

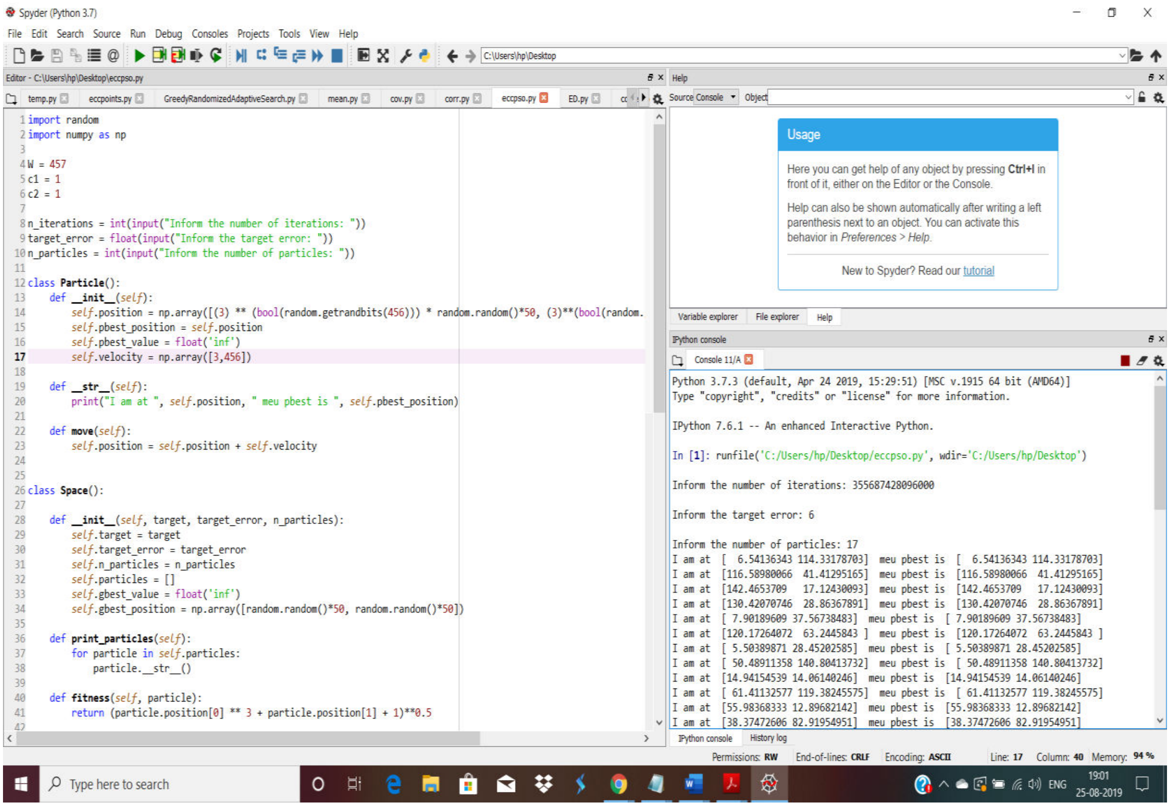


Fig.4.1.2.1 Python code for computing ECC Points with PSO with prime number,P=457 on Spyder(Python 3.7)

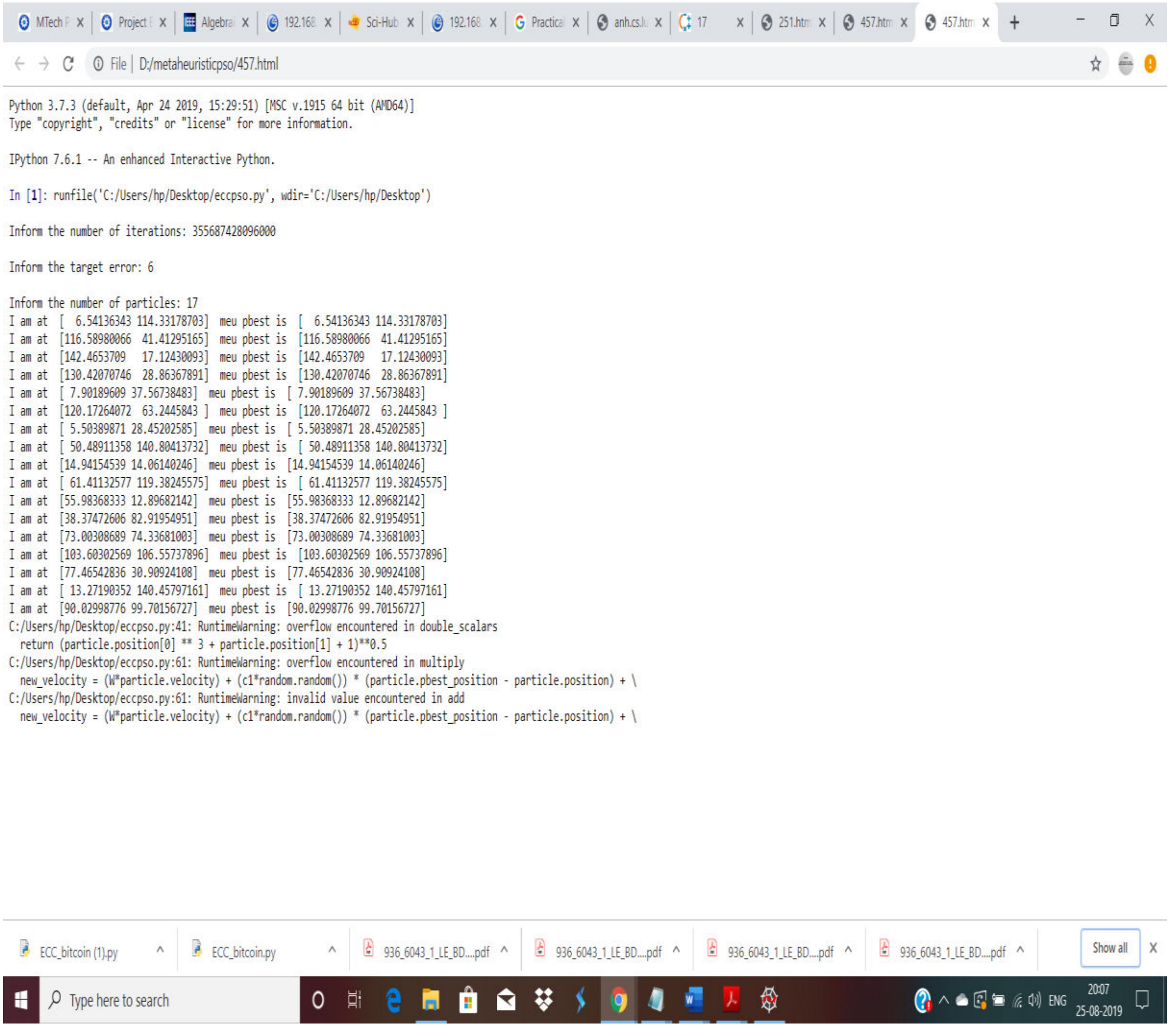


Fig.4.1.2.2 PSO output for P=457

c)P=593

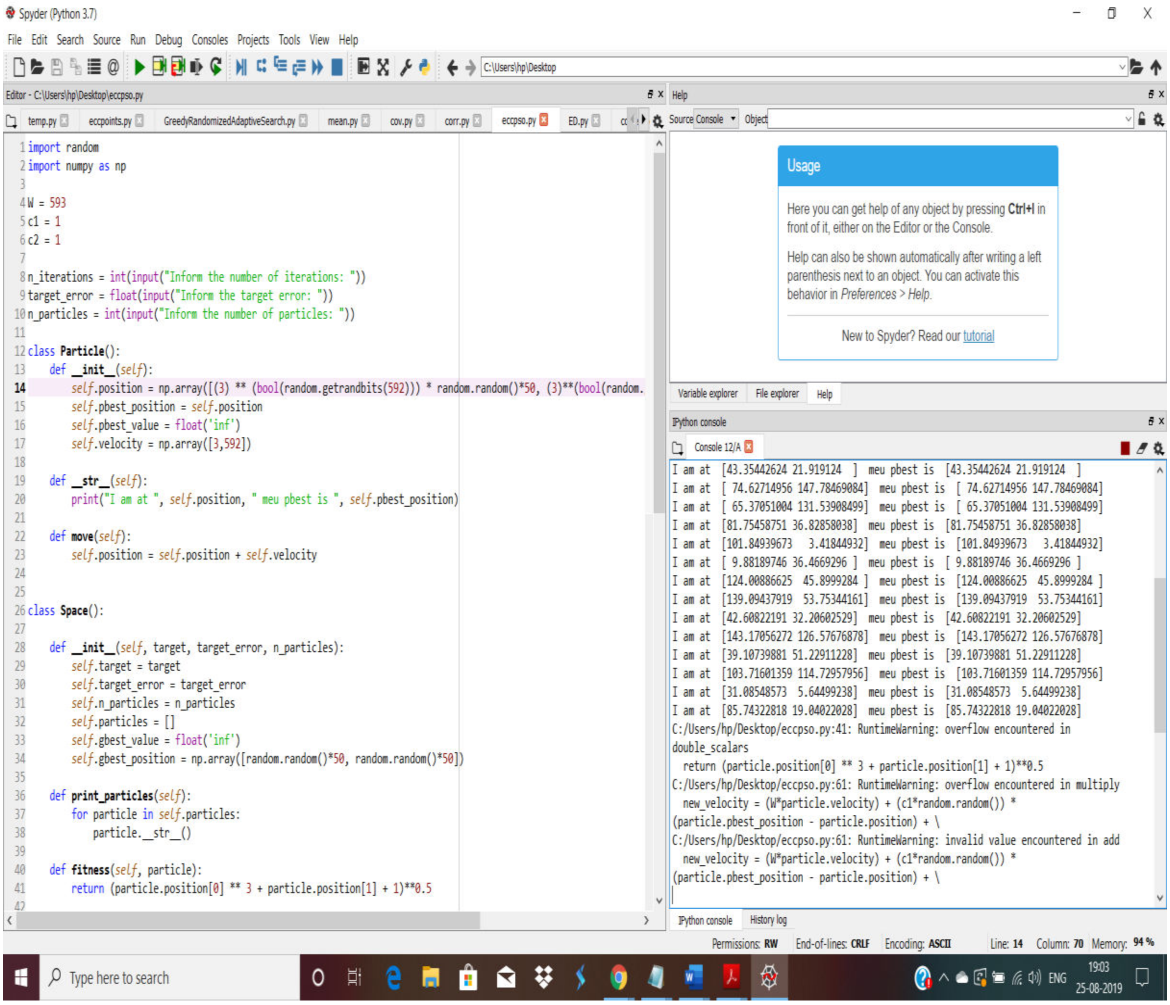


Fig.4.1.2.3 Python code for computing ECC Points with PSO with prime number,P=593 on Spyder(Python 3.7)

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 10 | Oct -2020 ISSN: 2582-3930

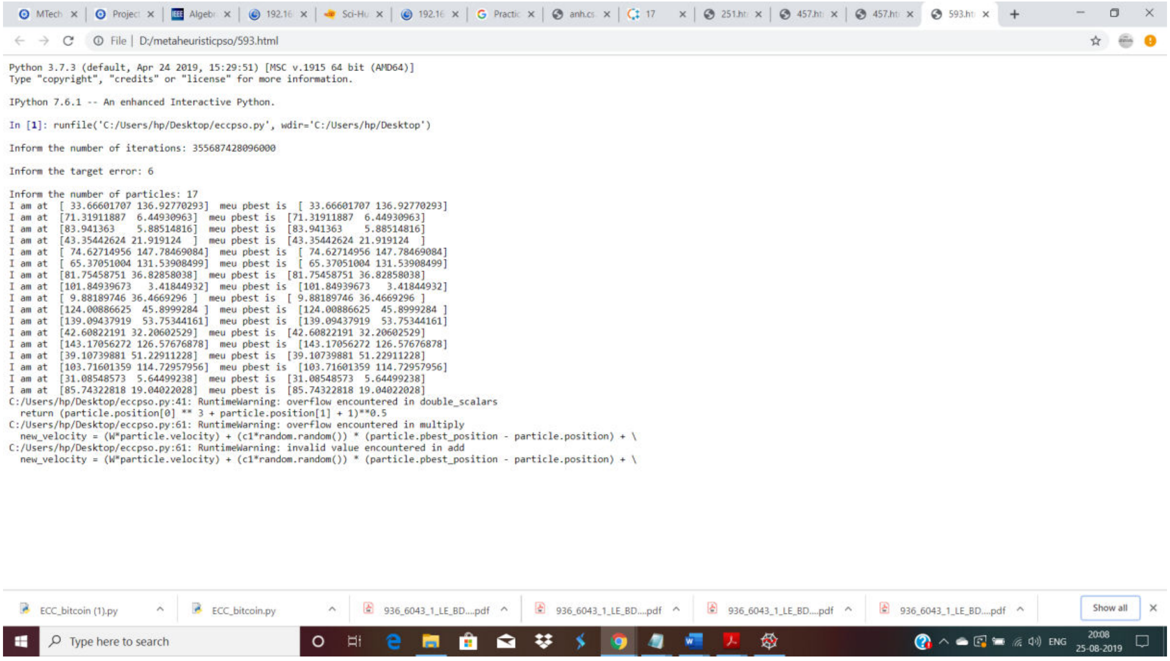


Fig.4.1.2.4 PSO output with P=593

d) P=929

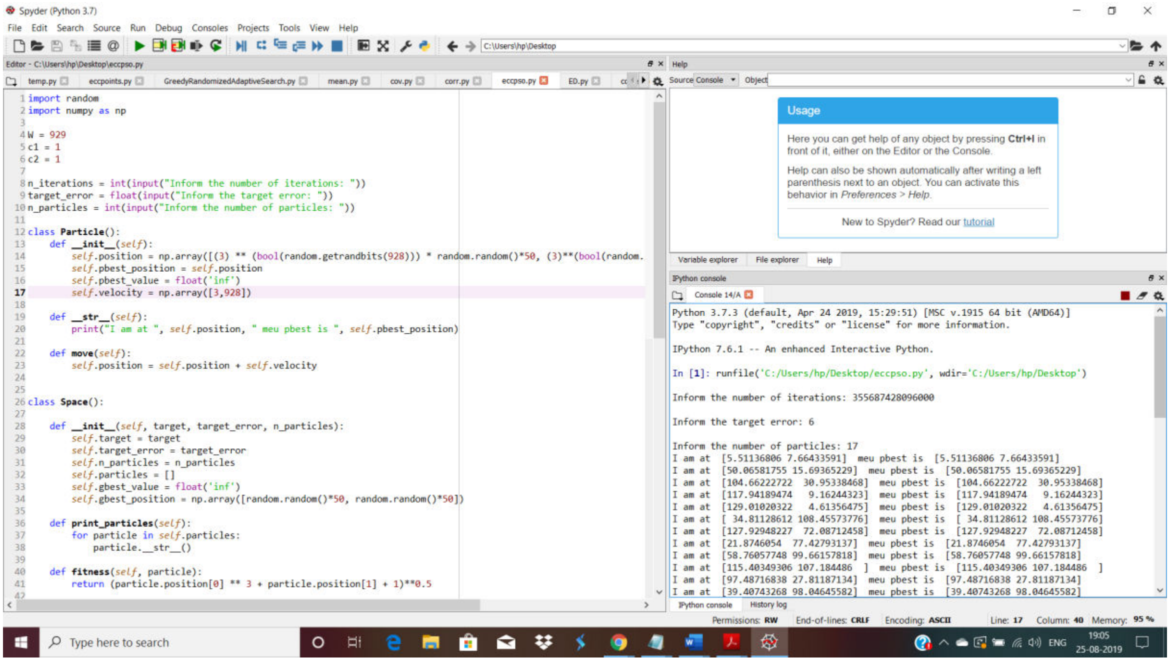


Fig.4.1.2.5 Python code for computing ECC Points with PSO with prime number,P=929 on Spyder(Python 3.7)

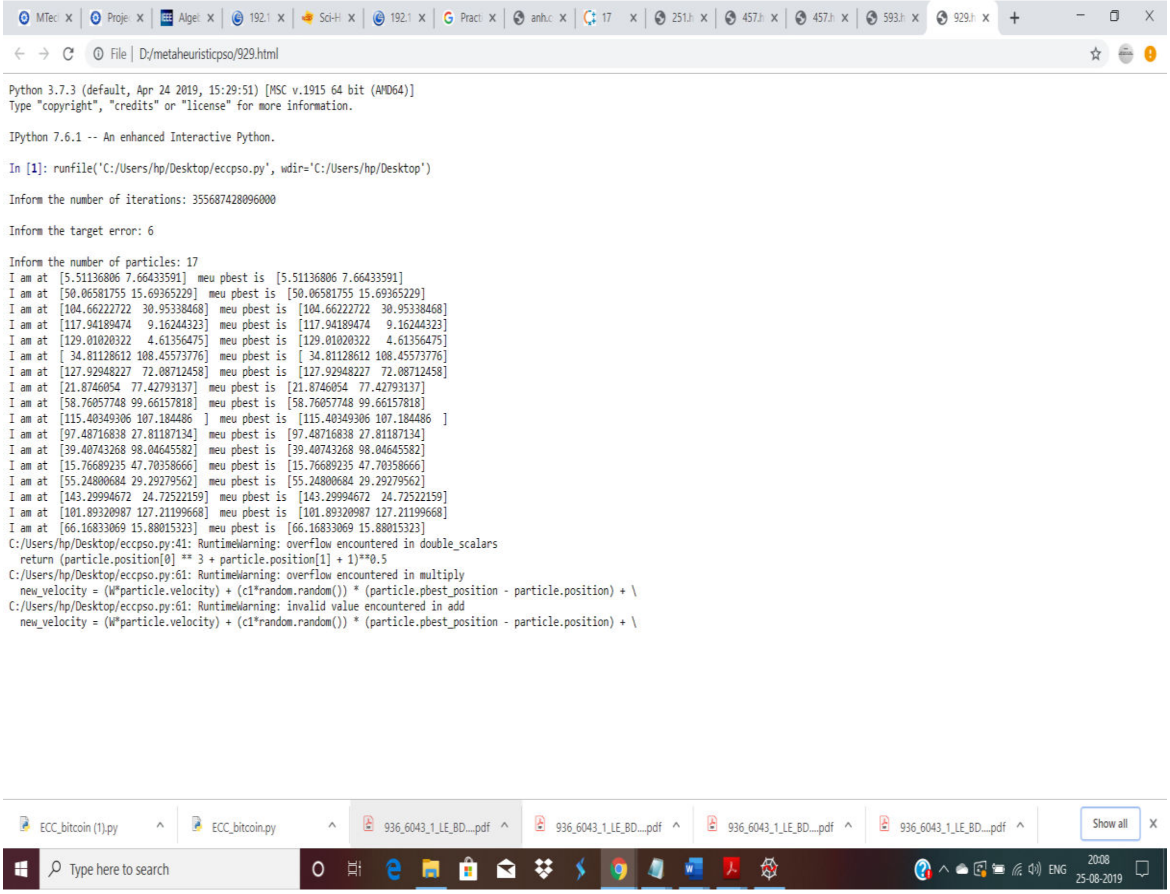


Fig.4.1.2.6 PSO output with P=929

4.4 CORRELATION OUTPUT:-

4.4.1 WITHOUT PSO

a) P=251

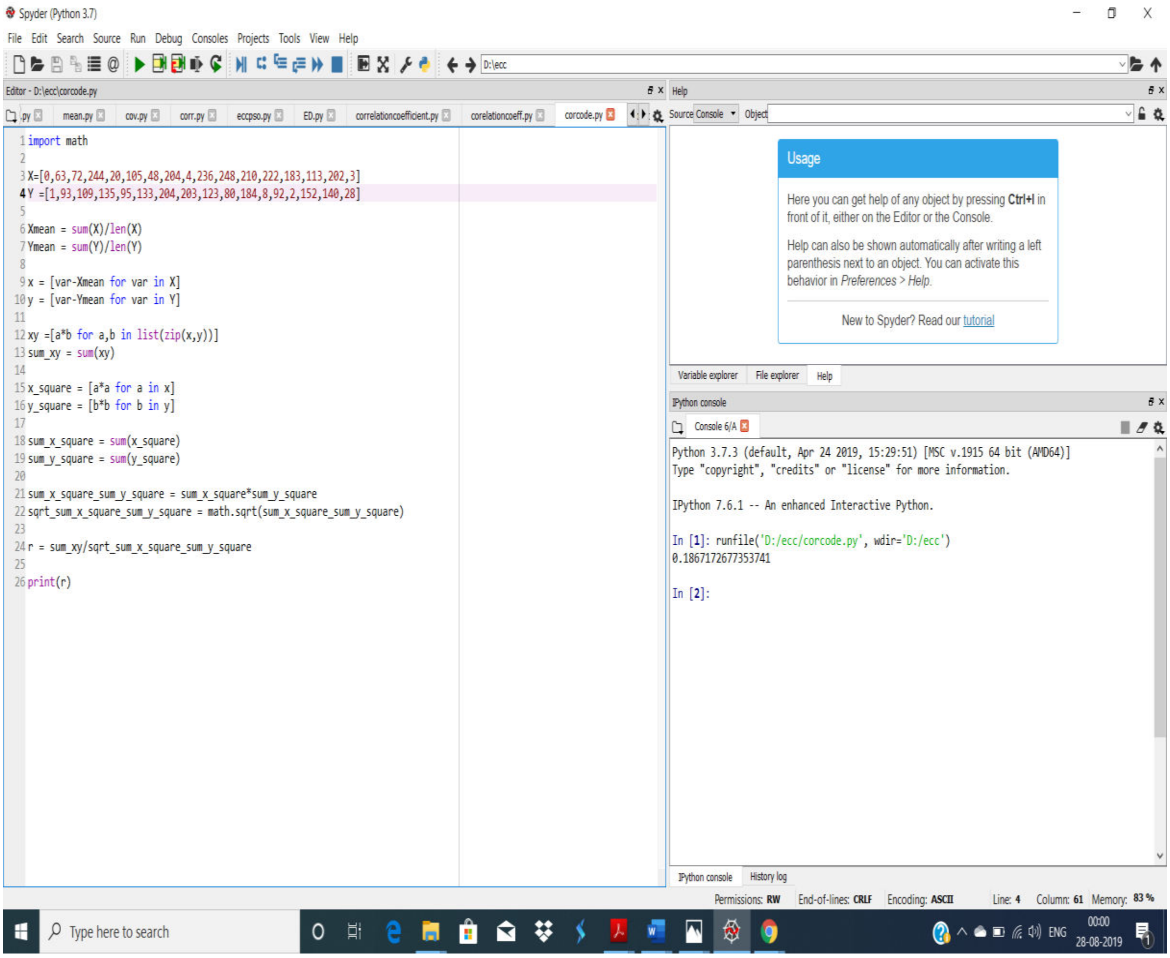


Fig.4.1.2.7 Python code for calculating correlation coefficient with P=251

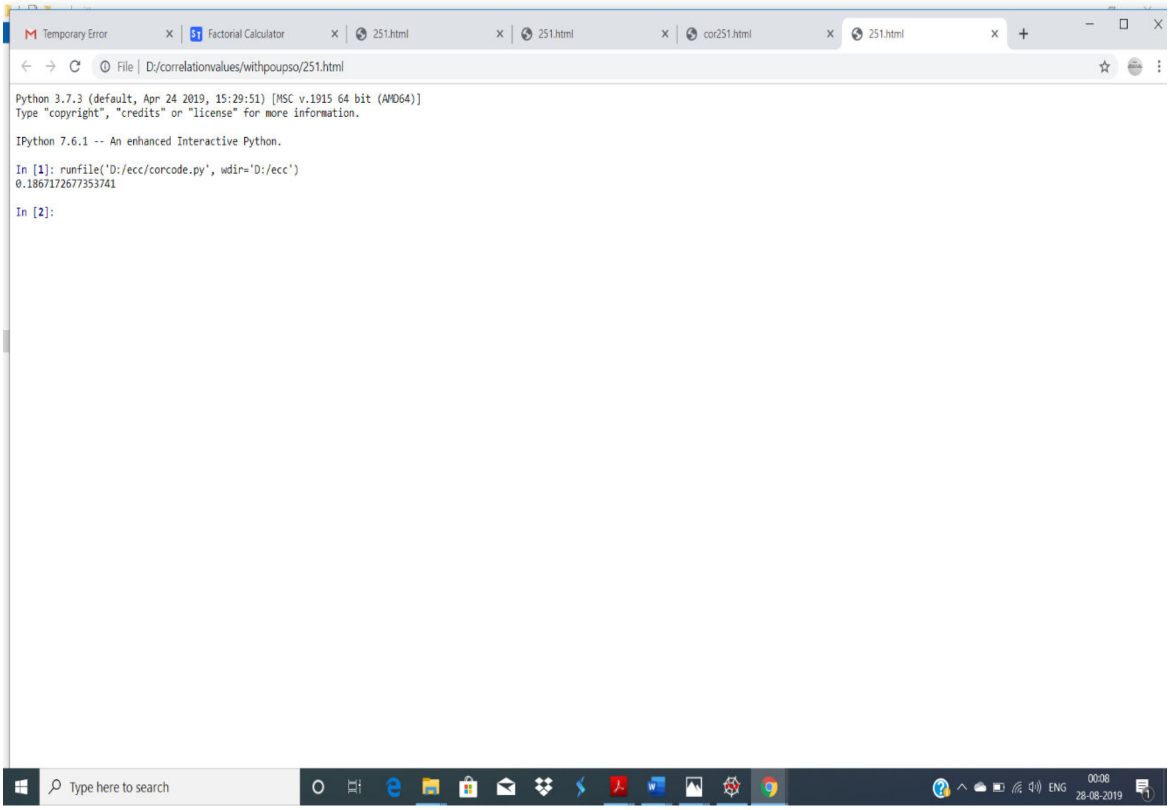


Fig.4.1.2.8 Correlation Coefficient output with P=251

b)P=457

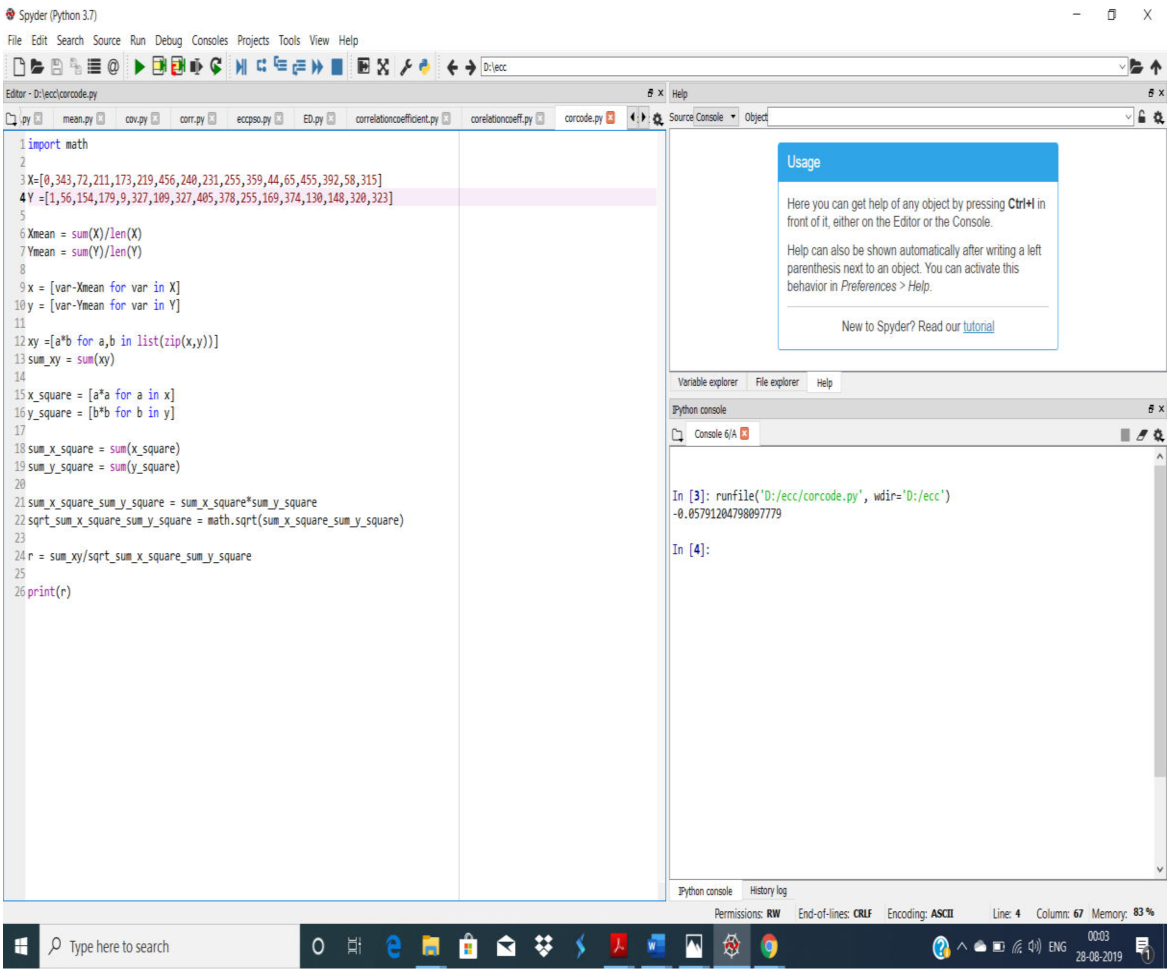


Fig.4.1.2.9 Python code for calculating correlation coefficient with P=457

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 10 | Oct -2020 ISSN: 2582-3930

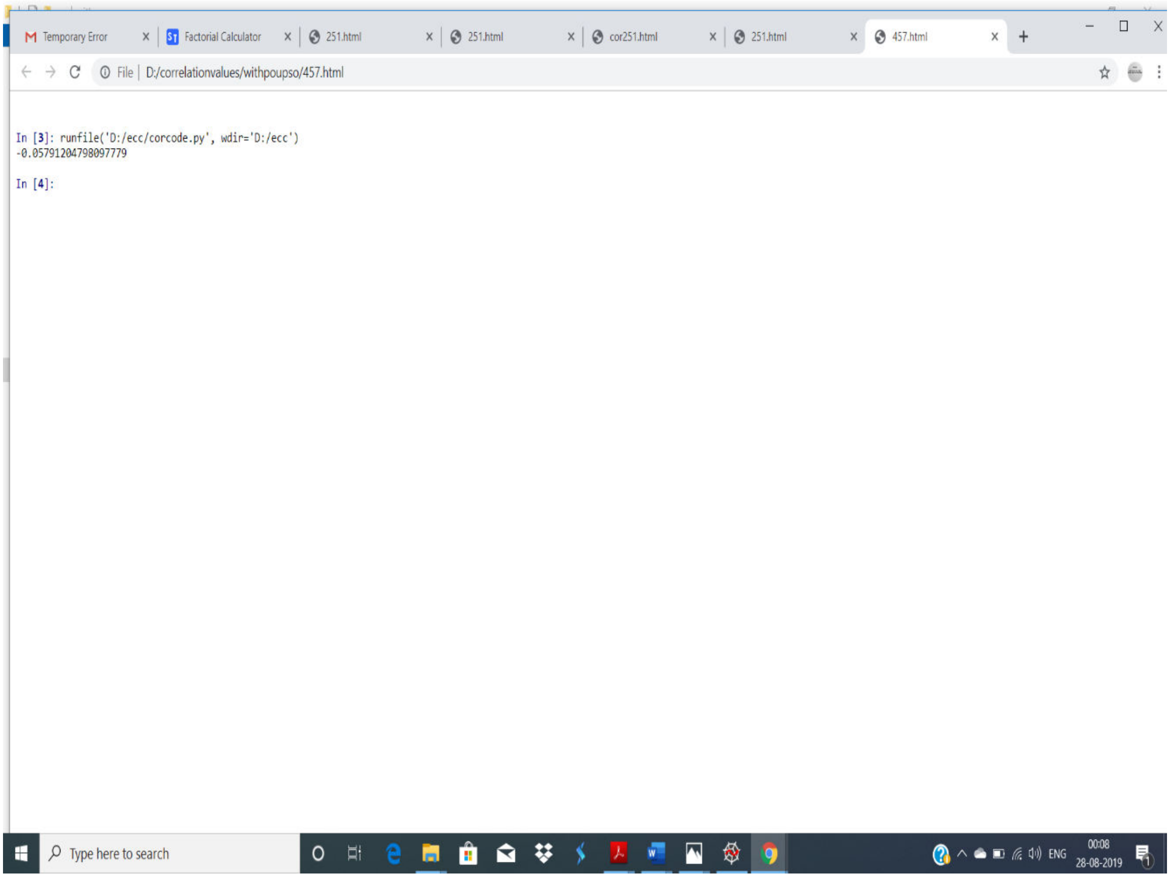


Fig.4.1.3.0 Correlation Coefficient output with P=457

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 10 | Oct -2020 ISSN: 2582-3930

c)P=593

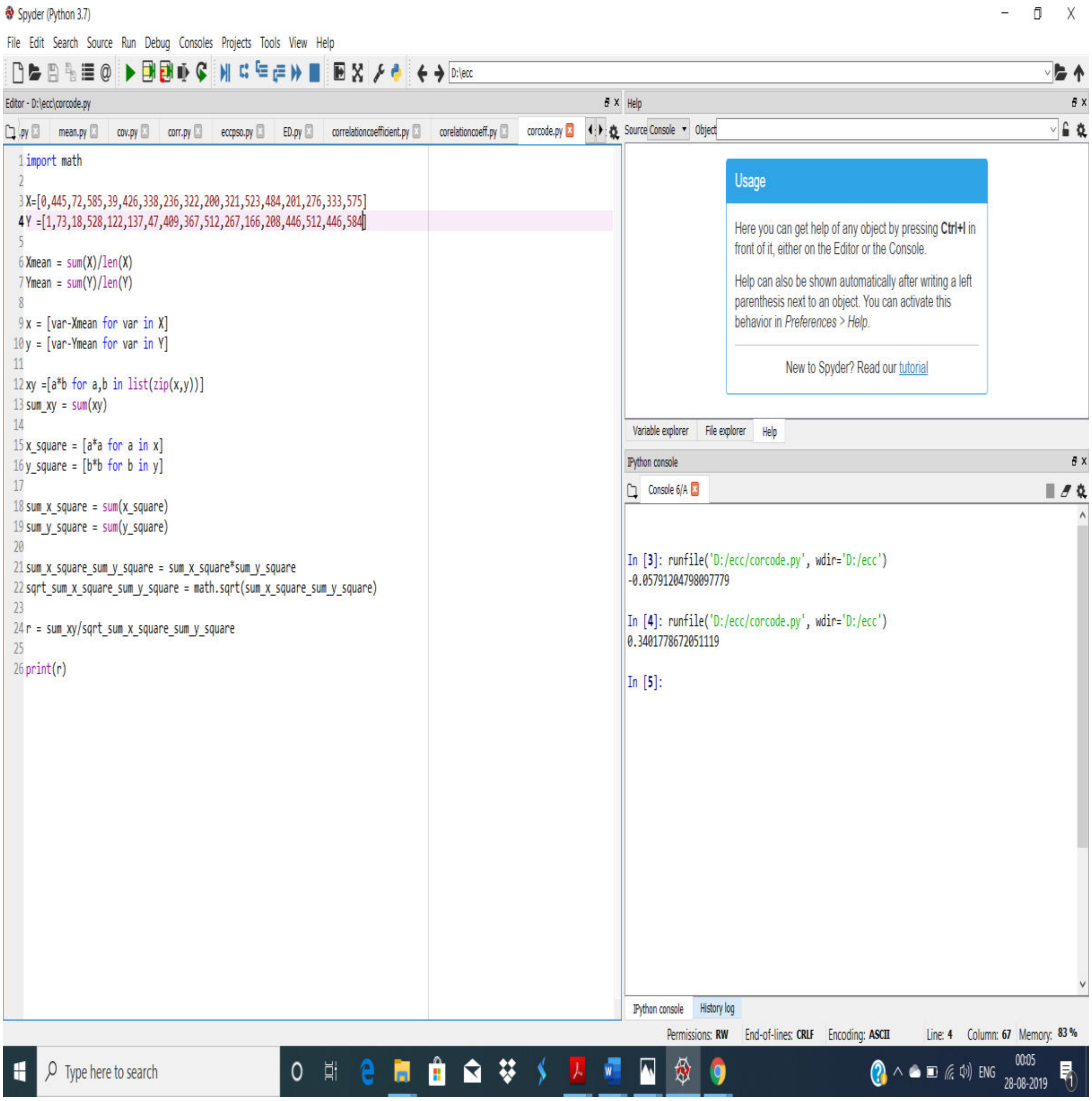


Fig.4.1.3.1 Python code for calculating correlation coefficient with P=593

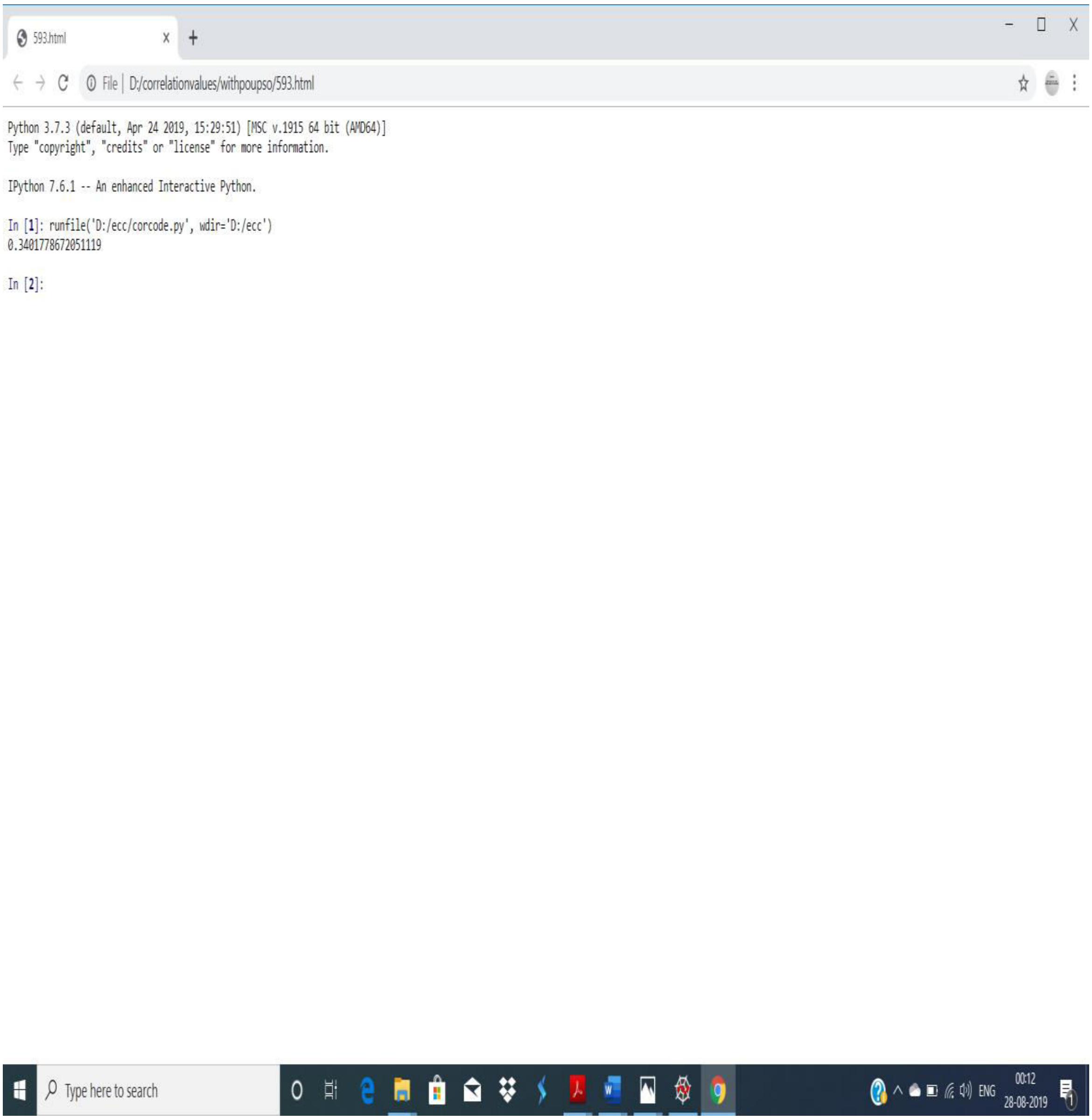


Fig.4.1.3.2 Correlation Coefficient Output with P=593

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 10 | Oct -2020 ISSN: 2582-3930

d)929

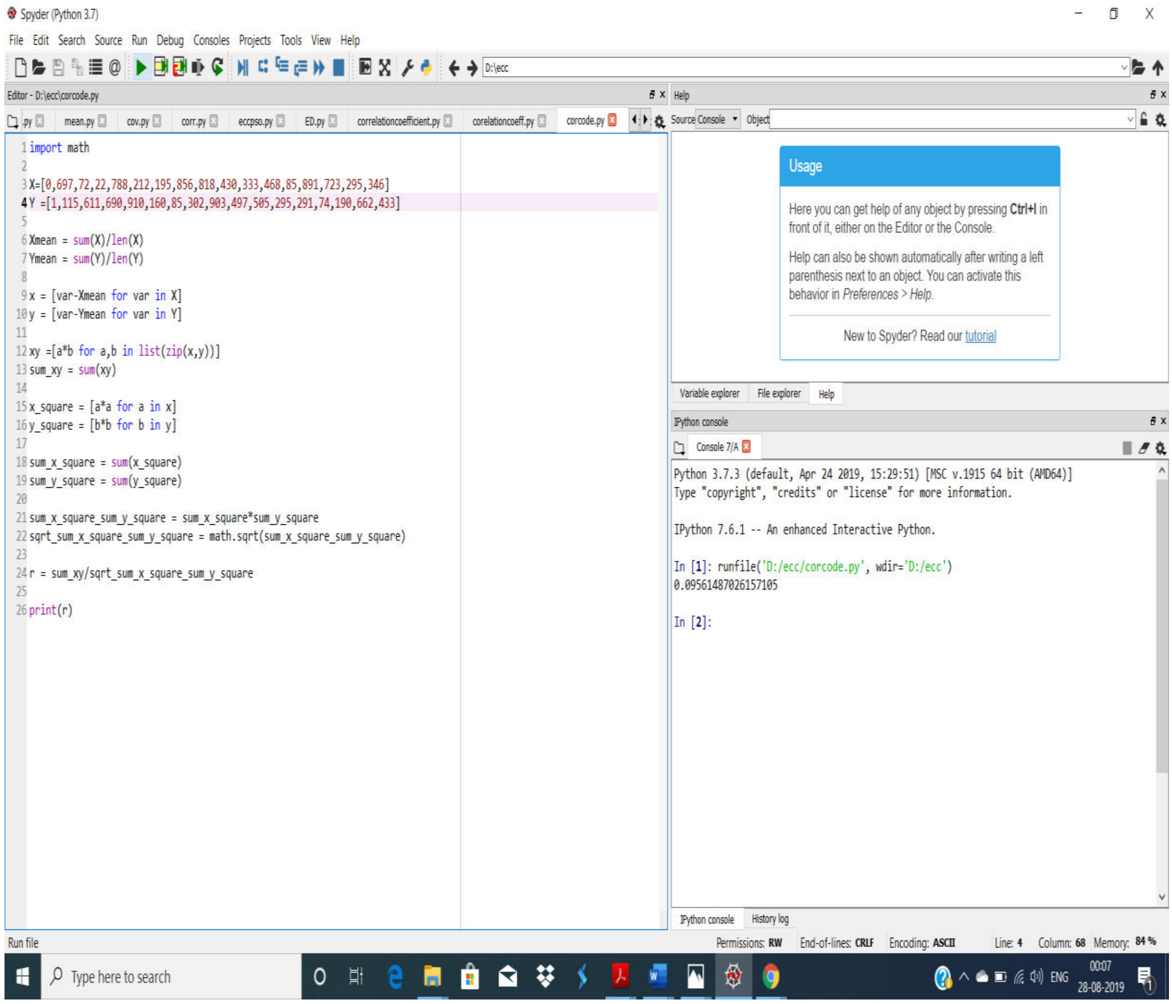


Fig.2.1.3.3 Python code for calculating correlation coefficient with P=929

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 10 | Oct -2020 ISSN: 2582-3930

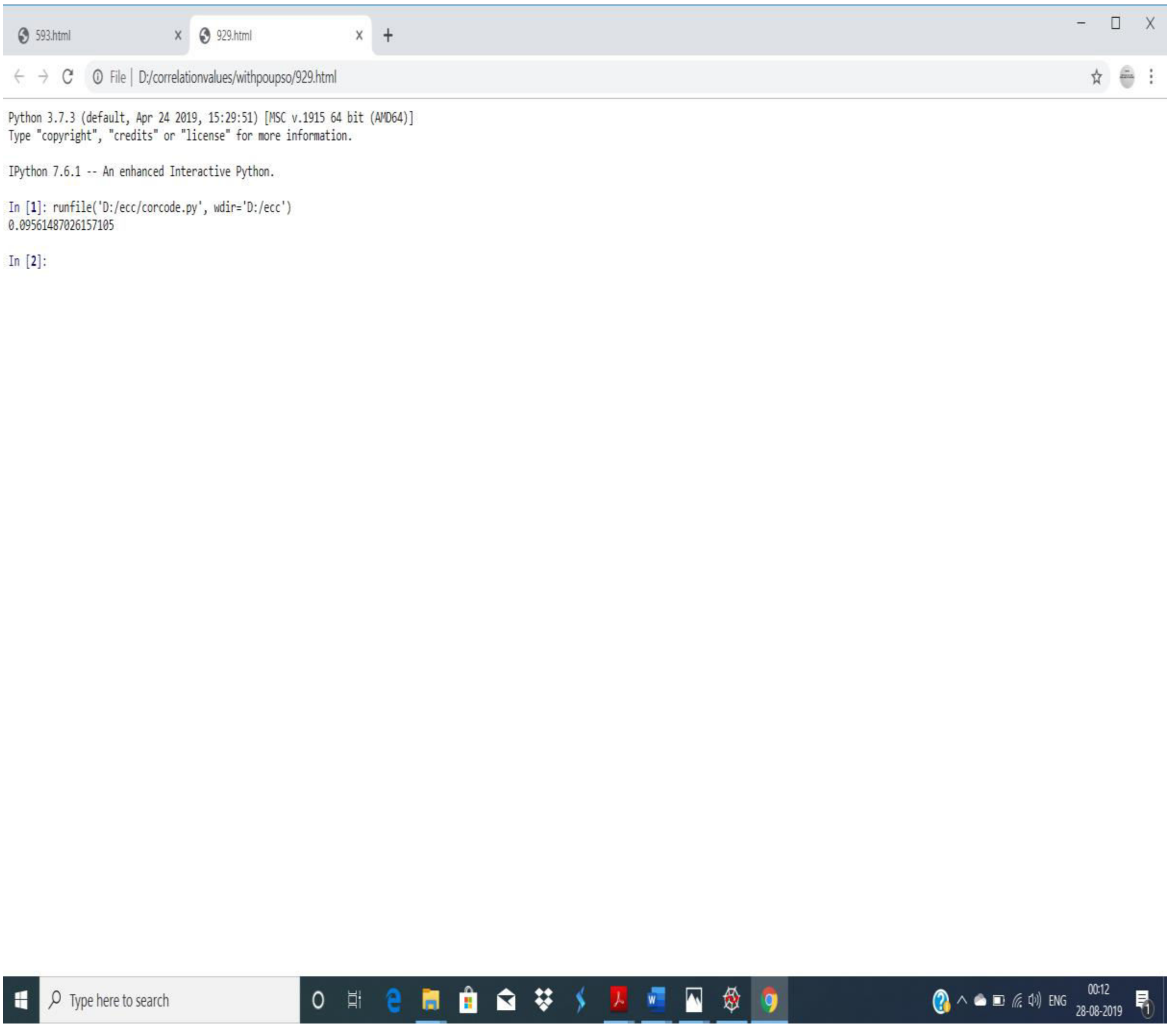


Fig.4.1.3.4 Correlation Coefficient output with P=929

4.4.2 WITH PSO

a)P=251

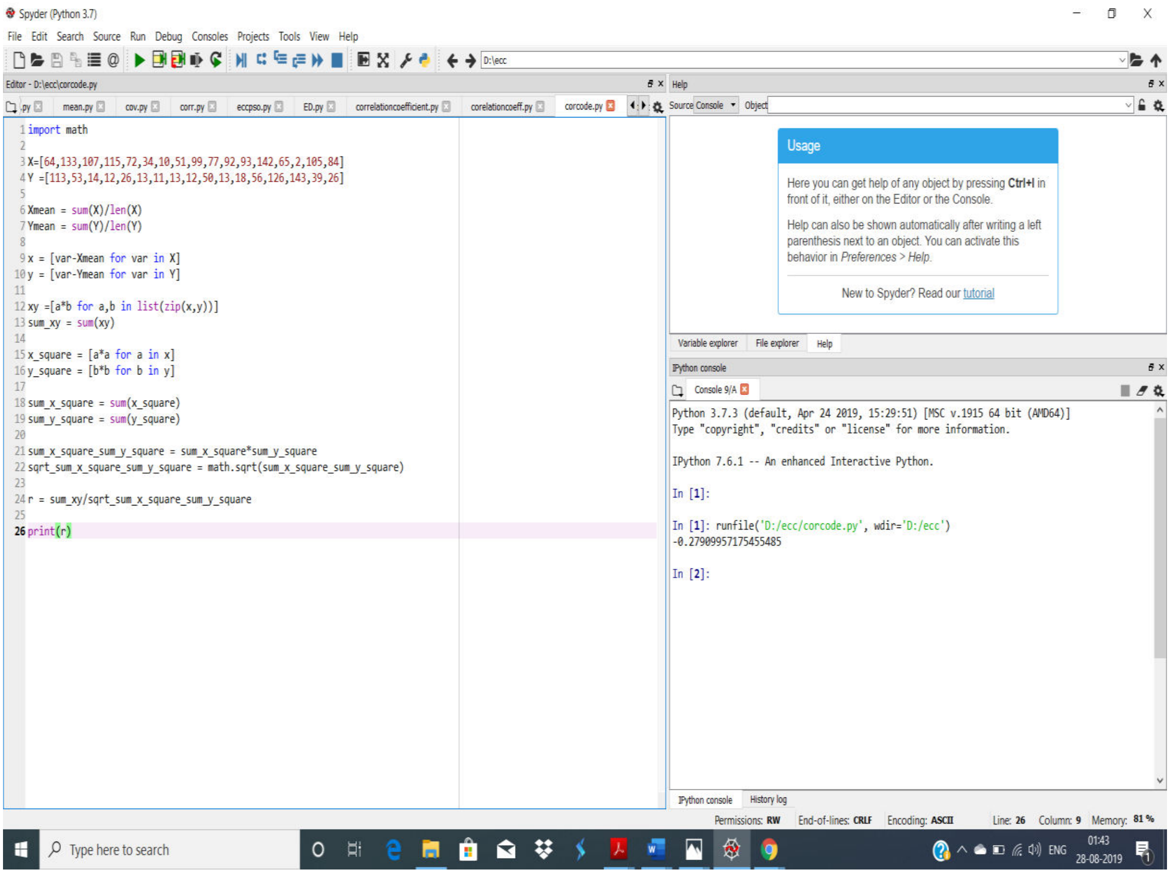


Fig.4.1.3.5 Python code for calculating correlation coefficient of obtained PSO points with P=251

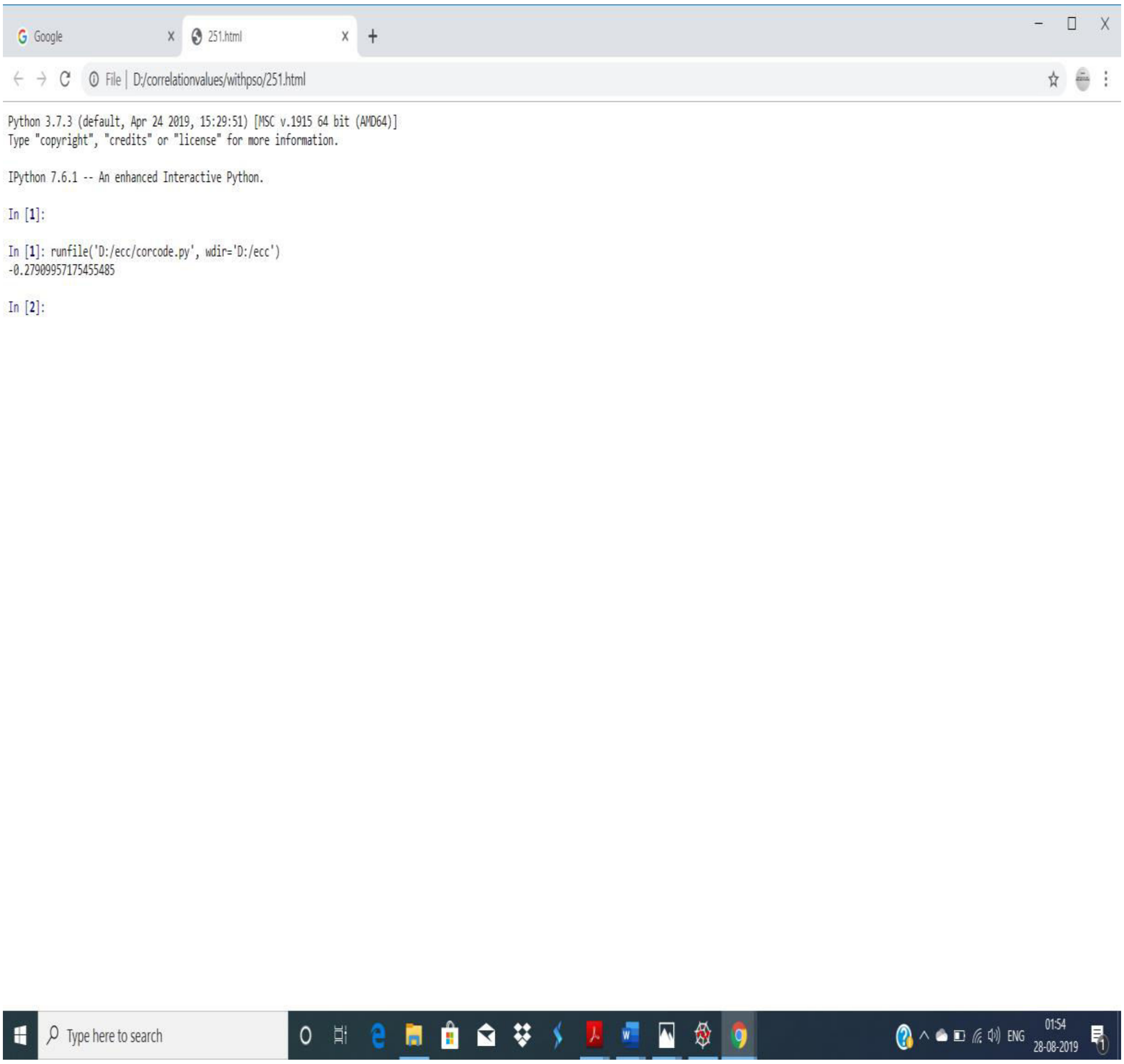


Fig.4.1.3.6 Correlation Coefficient of PSO applied elliptic points with P=251

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 10 | Oct -2020 ISSN: 2582-3930

b)P=457

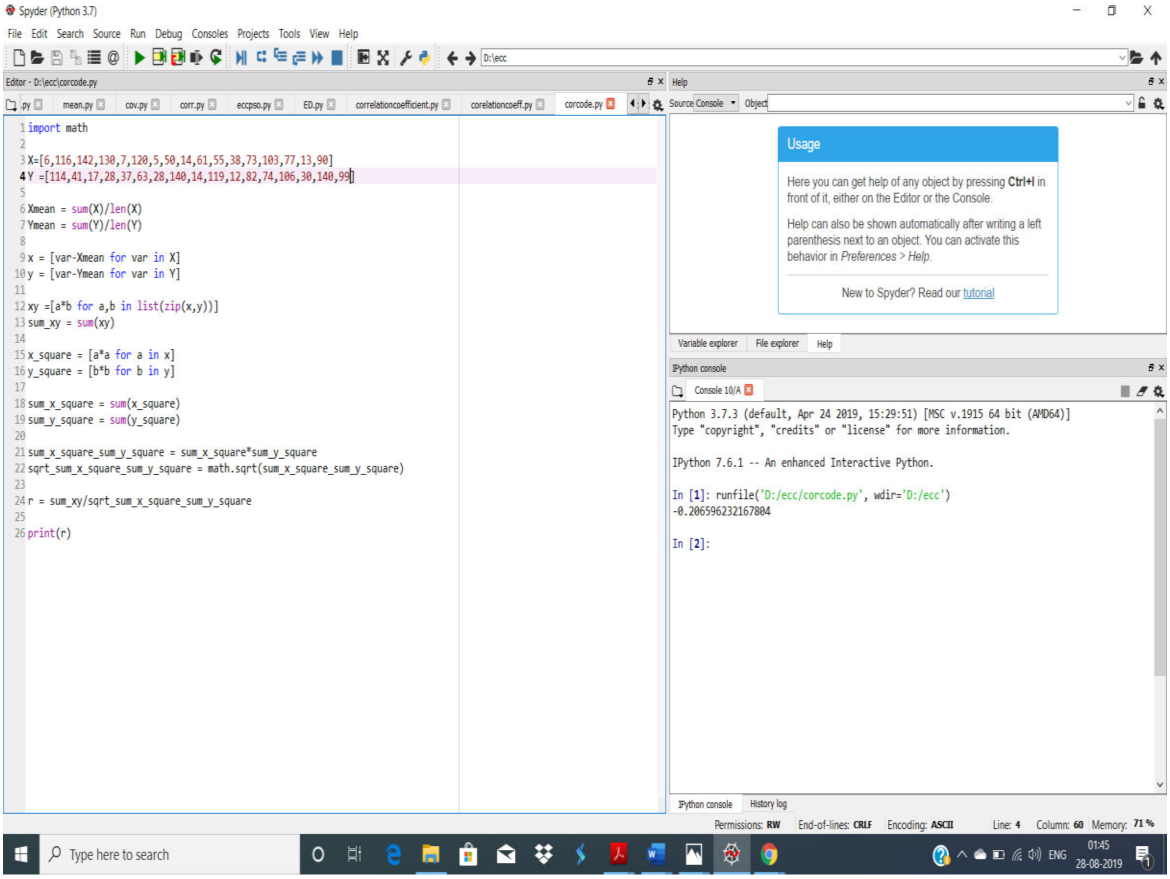


Fig.4.1.3.7 Python code for calculating correlation coefficient of obtained PSO points with P=251

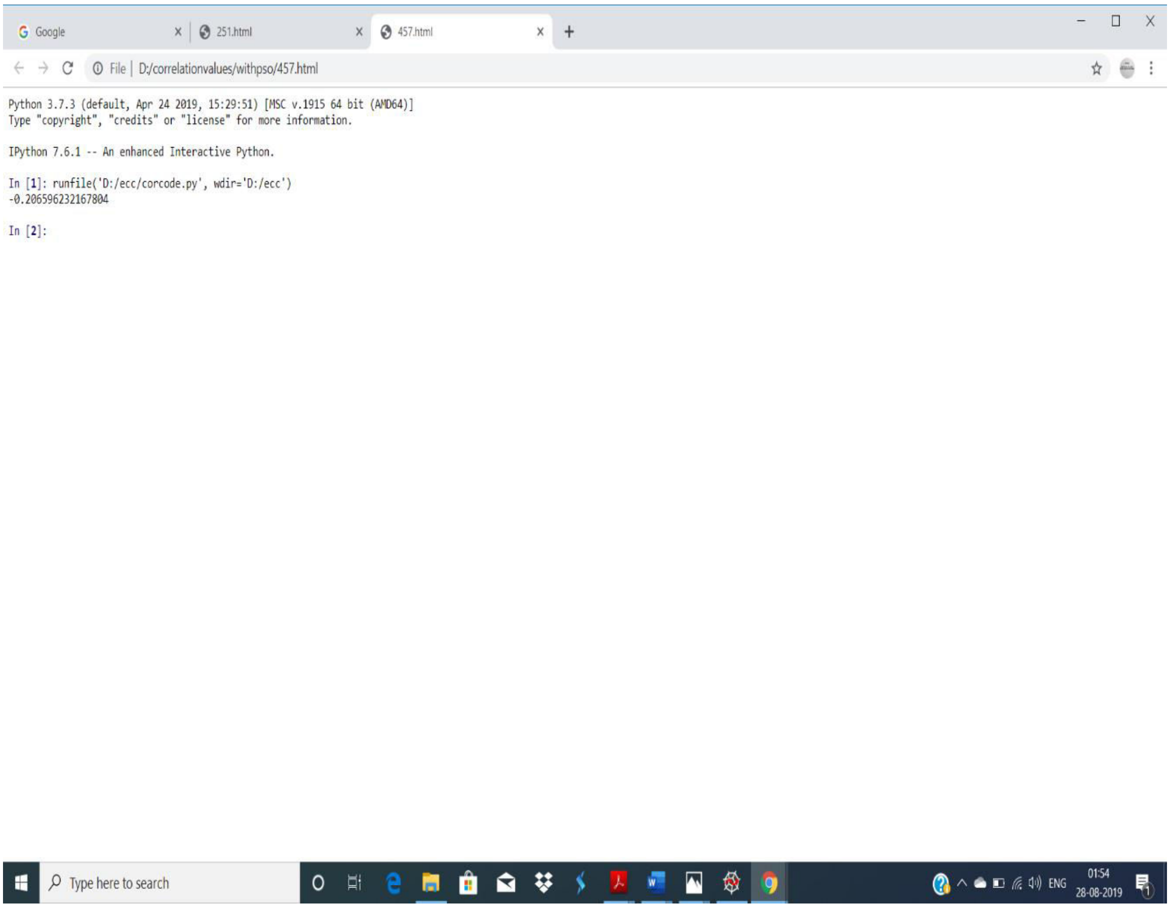


Fig.4.1.3.8 Correlation Coefficient of PSO applied elliptic points with P=457

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 10 | Oct -2020 ISSN: 2582-3930

b) P=593

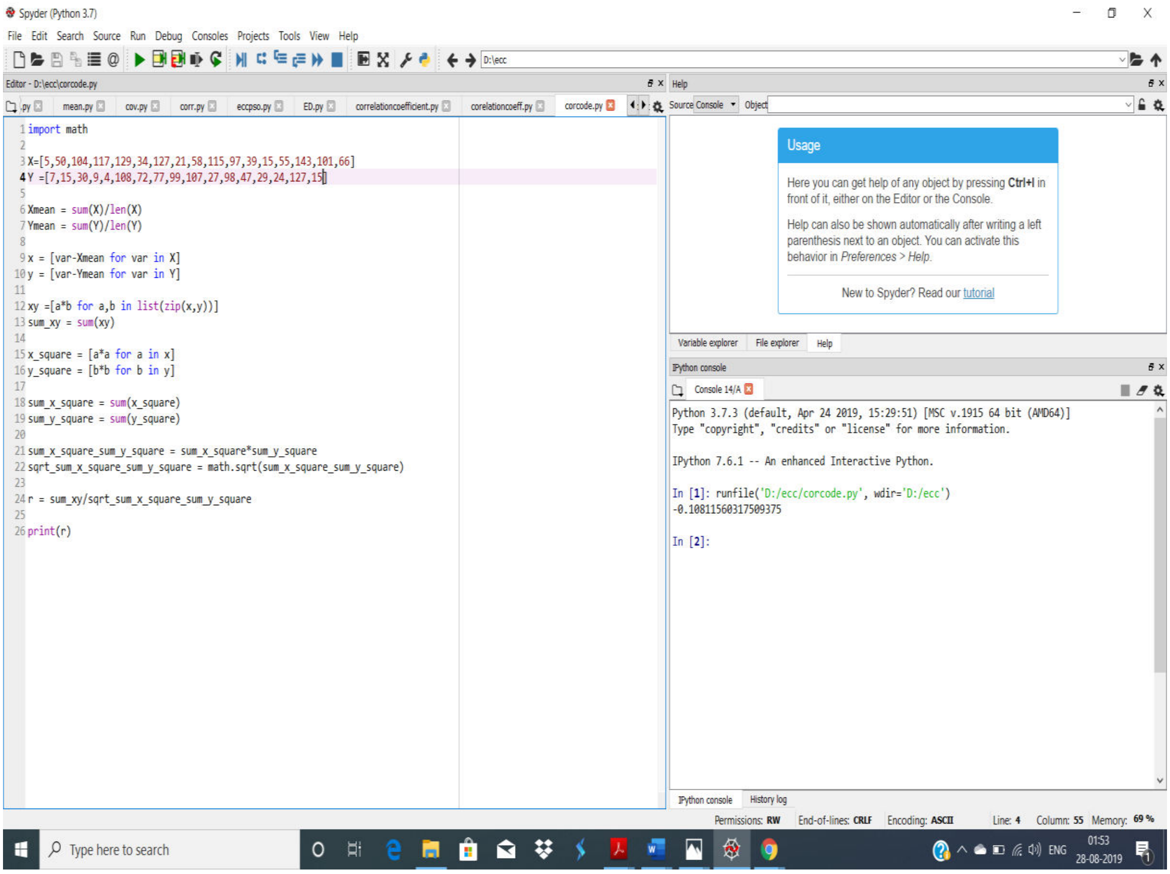


Fig.4.1.3.9 Python code for calculating correlation coefficient of obtained PSO points with P=593

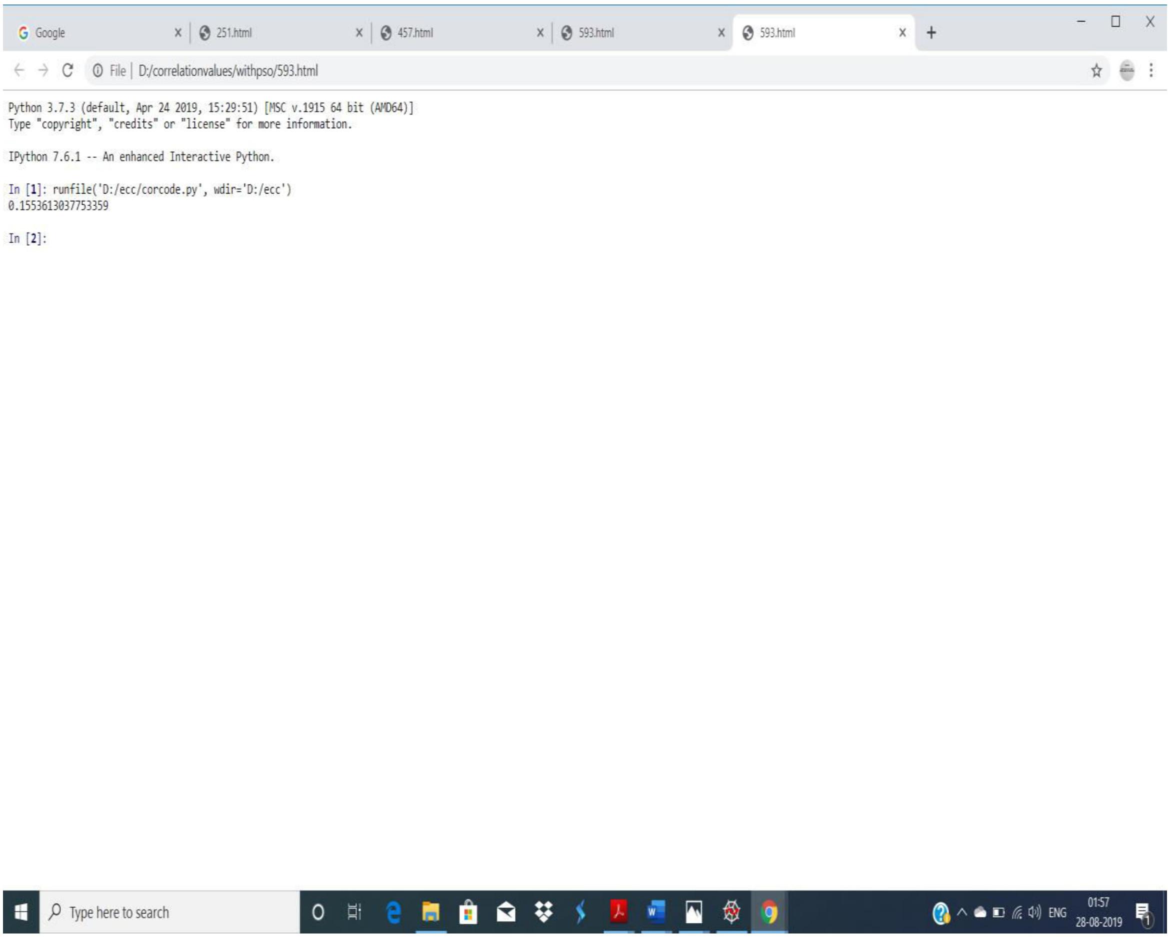


Fig.4.1.4.0 Correlation Coefficient of PSO applied elliptic points with P=593

c) P=929

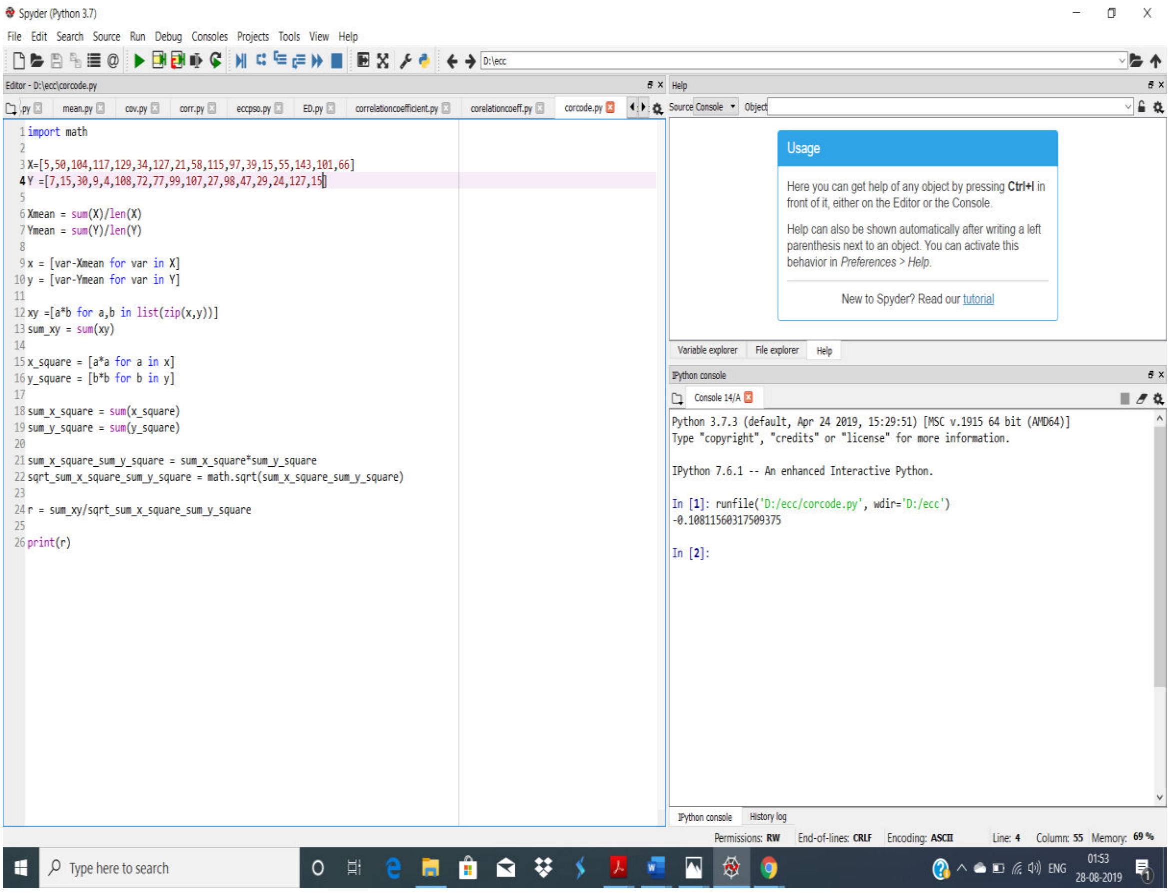


Fig.4.1.4.1 Python code for calculating correlation coefficient of obtained PSO points with P=929

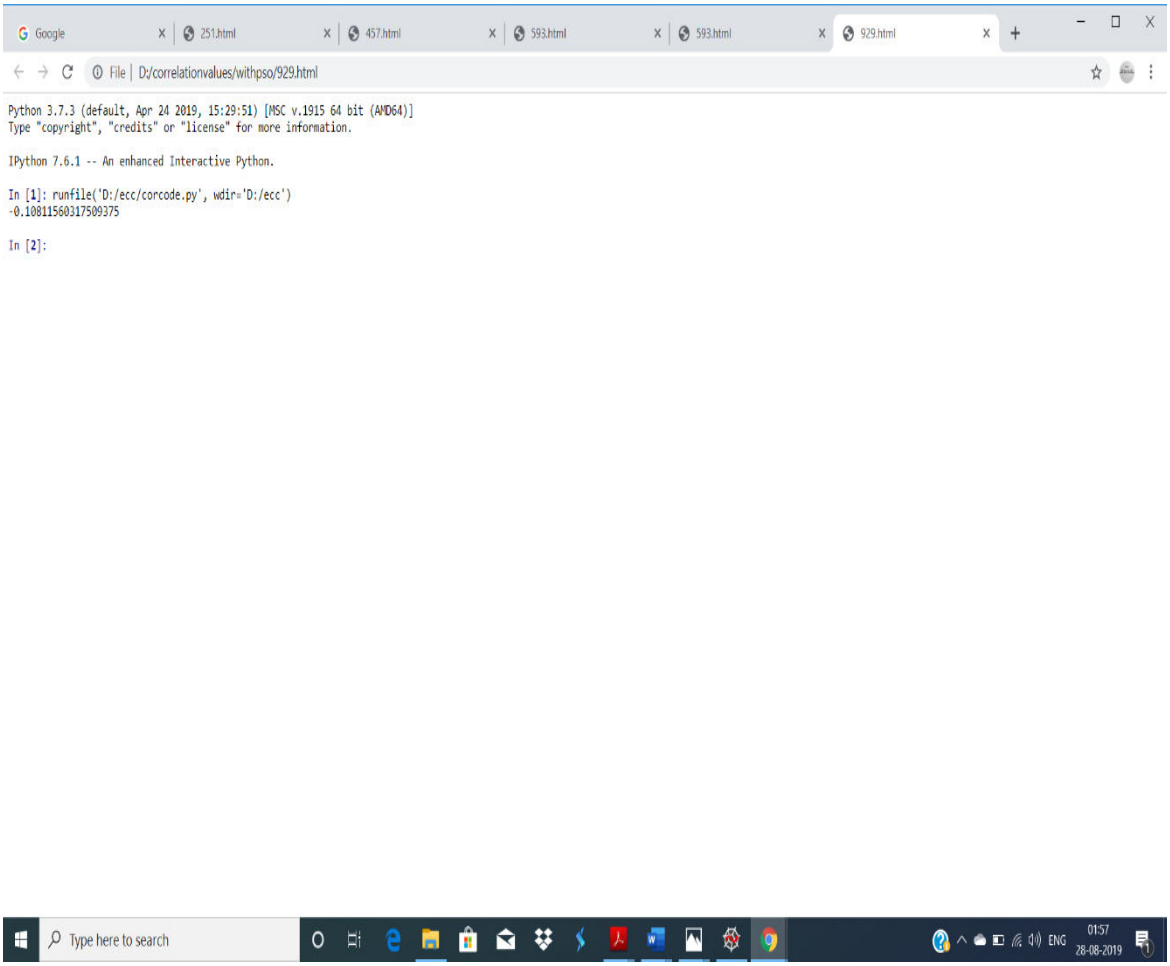


Fig.4.1.4.2 Correlation Coefficient of PSO applied elliptic points with P=929

RESULT ANALYSIS

5.1 TABLE SHOWING IMPROVEMENT OF CORRELATION AMONGST ELLIPTIC POINTS AFTER APPLYING METAHEURISTIC ALGORITHM VIZ.PSO

S No.	Prime number	Correlation coefficient between X and Y Coordinates of elliptic points	Correlation coefficient after applying Metaheuristics viz.PSO on elliptic points
1	251	0.1867172677353741	-0.27909957175455485
2	457	-0.05791204798097779	-0.206596232167804
3	593	0.3401778672051119	-0.06280917543035339
4	929	0.09561487026157105	-0.10811560317509375

TABLE 5.1 SHOWING IMPROVEMENT OF CORRELATION AMONGST ELLIPTIC POINTS AFTER APPLYING METAHEURISTIC ALGORITHM VIZ.PSO

5.2 GRAPH SHOWING CORRELATION VALUES VERSUS PRIME NUMBERS

1.CORRELATION VERSUS PRIME NUMBER WITHOUT PSO

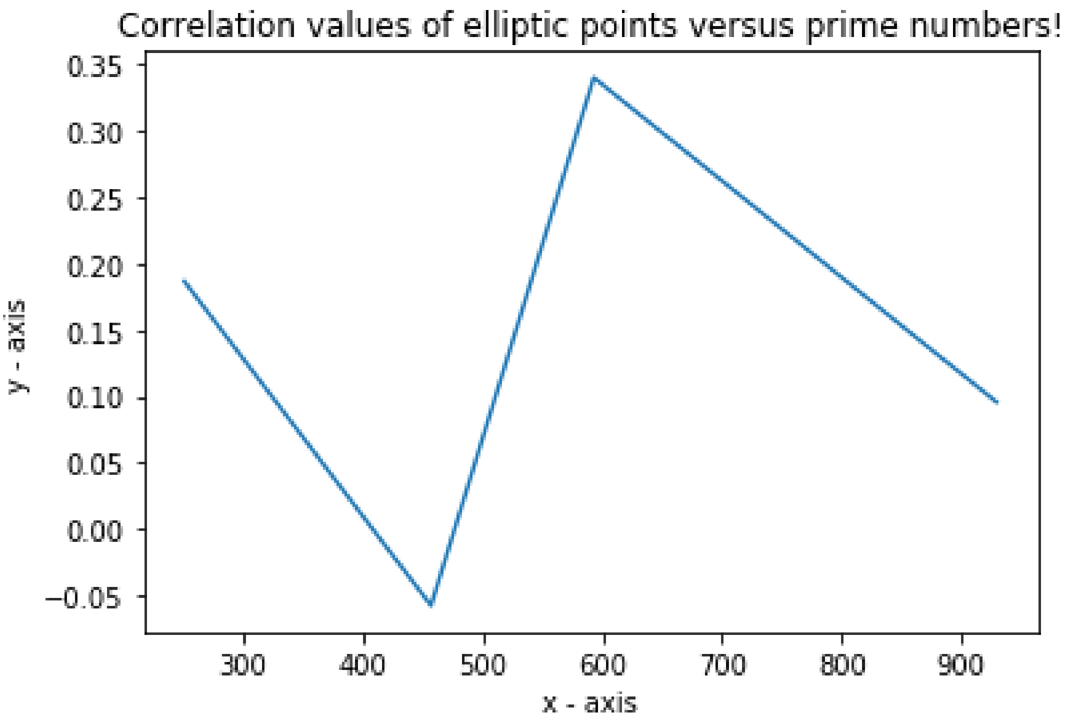


Fig.5.1.1.1 GRAPH SHOWING CORRELATION VERSUS PRIME NUMBER WITHOUT PSO

2.CORRELATION VALUES VERSUS PRIME NUMBERS AFTER APPLYING PSO

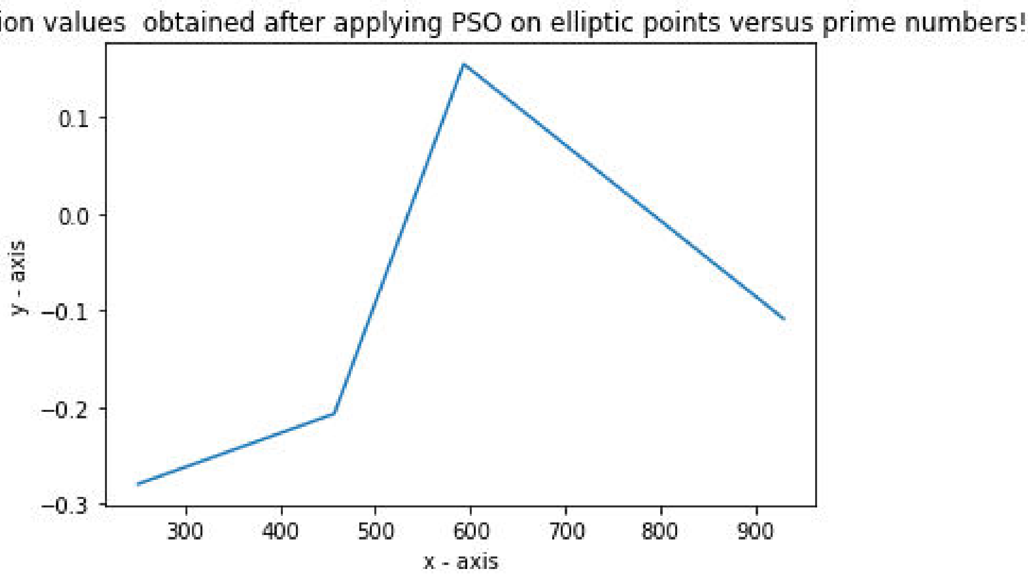


Fig.5.1.1.2 GRAPH SHOWING CORRELATION VALUES VERSUS PRIME NUMBERS AFTER APPLYING PSO

The above obtained correlation values are compared and contrasted with the earlier work of "Selection of Fittest Key Using Genetic Algorithm and Autocorrelation in Cryptography"[12] based on the following results.

Table 5.2: - Table showing autocorrelation values of different keys when Genetic Algorithm is applied on DES to find the fittest key

	Autocorrelation values
Iteration 1 Crossover set	-0.0077539468
Iteration 2 Population Generation set	0.0535485376
Iteration 3 Crossover set	-0.0111042183

It is observed that the values of correlation are much better when Elliptic Curve Cryptography is amalgamated with a metaheuristic algorithm named Particle Swarm Optimization as almost all correlation values are negative and less than Table 5.2 values

Conclusion and Future Scope

6.1 Conclusion

- Proximity of correlation value to -1 guarantees randomness in the key
- The key may be less susceptible to any adversaries attack.
- From Fig.5.1.1.2 graph, it is inferred that with large prime numbers, correlation values decrease increasing randomness in the key when PSO is applied on elliptic curve points

6.2 Future Scope

- The venture can be conveyed on asset obliged gadgets like versatile phones, IoT and so on
- The symmetric cover key offers greater security when contrasted with RSA with little key size

References

[1]D. Hankerson, A. Menezes, and S.A. Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag, 2004

[2]T.A. Feo and M.G.C. Resende (1995) Greedy randomized adaptive search procedures. Journal of Global Optimization, 6:109–133, 1995.

[3]Hansen, P.; Mladenovic, N.; Perez, J.A.M. (2010). "Variable neighborhood search: methods and applications". Annals of Operations Research. 175: 367–407doi:10.1007/s10479-009-0657-6.

[4]Mattern, Friedemann; Floerkemeier, Christian (2010). "From the Internet of Computer to the Internet of Things" (PDF). Informatik-Spektrum. 33 (2): 107–121. Bibcode:2009InfSp..32..496H. doi:10.1007/s00287-010-0417-7. Retrieved 3 February 2014.

[5]Glover, F.; Kochenberger, G.A. (2003). Handbook of metaheuristics. 57. Springer, International Series in Operations Research & Management Science. ISBN 978-1-4020-7263-5.

[6]Du, Wenliang Kevin; Deng, Jing; Han, Yunghsiang S.; and Varshney, Pramod K., "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks" (2000). Electrical Engineering and Computer Science. Paper 36. http://surface.syr.edu/eecs/36

[7]Bitcoin Exchanges Linked To Silk Road? So the FBI Thinks, retrieved fromhttps://silkroaddrugs.org/category/bitcoin/

[8]Croxton, Frederick Emory; Cowden, Dudley Johnstone; Klein, Sidney (1968) Applied General Statistics, Pitman. ISBN 9780273403159 (page 625)

[9]Dargie, W. and Poellabauer, C. (2010). Fundamentals of wireless sensor networks: theory and practice.

John Wiley and Sons. pp. 168–183, 191–192. ISBN 978-0-470-99765-9

[10]Savage, David G., LA Times, Supreme Court rules in favor of California police chief who read employee's texts

[11] Zhang, Y. (2015). "A Comprehensive Survey on Particle Swarm OptimizationAlgorithm and Its Applications". Mathematical Problems in Engineering. 2015: 931256.

[12]Sania Jawaid, AnamSaiyeda,,NabaSuroor"Selection of Fittest Key Using Genetic Algorithm and Autocorrelation in Cryptography"(2015)DOI:10.12691/jcsa-3-2-5

[13] Abdul wahab, Hala&Kadhem, Suhad&Kadhim, Estabraq. (2012). planned Approach for Elliptic curve hidden writing supported Metaheuristic Algorithms. International Journal of research. 2. 1-5. 10.15373/22778179/OCT2013/33.

[14]E. Jovanov, A. Milenkovic, C. Otto, P. C.D. Groen, "A wireless body area network of intelligent motion sensors for computer assisted physicall rehabilitation", Journal of Neuro Engineering and Rehabilitation, vol. 2, no. 6, 2005.

[15]Tebogo Kgogo, Bassey Isong, Adnan M. Abu-Mahfouz, "Software defined wireless sensor networks security challenges", AFRICON 2017 IEEE, pp. 1508-1513, 2017.

[16]A. R. Elshaz1y et al., "Synchronized Double Watermark Audio Watermarking Scheme Based on a Transform Domain for Stereo Signals", IEEE Fourth International Ja-pan-Egypt Conference on Electronics Communications and Computers, 2016.

[17] R.N. Akram, K. Markantonakis, Smart Cards: State-of-the-Art to Future Directions, IEEE, pp. 154-162, 2013.