Applied Mathematics and Computing
Vol. 1, No.1, (June, 2023)

A Note on Prime Elliptic Curve

Shubham Agarwal*

Department of Mathematics
New Delhi Institute of Management
New Delhi-110062 (India)
meshubhamagarwal@gmail.com
*Corresponding author

Abstract: Elliptic curves are smooth, projective algebraic curves of the first genus with a designated point O. (EC). On an elliptic curve, which makes it a commutative group by necessity, the multiplication operation is defined algebraically where point O acts as the identity element, satisfying the axioms of the abelian group. Without mentioning the point O, the curve is referred to as an elliptic curve. There are numerous ways to create elliptic curves, and by using these curves, several advanced writing and computing techniques have been developed. In elliptic curve encryption, creating a prime elliptic curve is essential. There is a need of an elliptic curve to increase security, but for increasing the scope of safety, prime elliptic curve has been introduced. In this paper, prime points on elliptic curves, prime elliptic curves, their characteristics has been described and also the relationship between prime elliptic curve coefficients has been established.

Keywords: Elliptic Curve; Prime Points on Elliptic Curve; Prime Elliptic Curve.

Reference:

Biographical notes: Shubham Agarwal is an Associate Professor with a demonstrated history of working in the education industry having more than 14 years of experience of teaching PG and UG courses, skilled in Research and Lecturing. Strong education professional with a Doctor of Philosophy (Ph.D.) focused in Number Theory and Cryptography from Kumaun University, Nainital, India. Written 4 books, having more than 30 National and International publications to his credit and has also organized and attended various seminars and conferences. He is a member of the editorial board of several Journals of National and International repute. He is also a member of the Ramanujan Mathematical Society and a reviewer of Springer Nature. His areas of interest are Cryptography, Number Theory, Operation Research, Numerical Analysis, Discrete Mathematics, Real Analysis, and Statistics.

1 Introduction

Any elliptic curve can be expressed as a function specified by or a plane algebraic curve as,

$$y^2 = x^3 + ax + b \tag{1}$$

is shown in Figure 1.

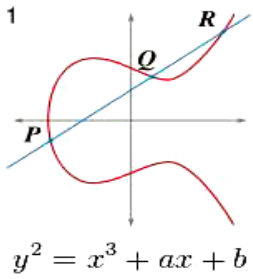

Figure 1: Elliptic curve

where a and b are real numbers. This type of equation is known as Weierstrass equation. The curve must also not be singular in order to meet the description of an elliptic curve, which means that its graph must not contain cusps or self-intersections. Elliptic curves are important in number theory and are the subject of much recent study. They also have uses in integer factorization and elliptic curve encryption (ECC).

The elliptic curve cryptosystem, which was based on elliptic curves, was developed by Miller, V. (1985), and Koblitz, N. (1987), who also described how elliptic curves are used in cryptography. Algorithms based on elliptic curve cryptography were widely used in cryptographic systems for security in 2004 and 2005, and the National Institute of Standards and Technology accepted and authorised these algorithms in 2006.

2 Review of Literature

Broker, R. (et al., 2007) developed an effective algorithm to create an elliptic curve E and a finite field F where the order of the point group E(F) is a given prime integer N. It's interesting that this method only requires polynomial time O((log N)3) and is so quick that it can be effectively applied to the related problem of finding elliptic curves with point groups of specified order.

The comparison between elliptic curve encryption and other cryptography algorithms was covered by Shanmugalakshmi, R. (et al, 2009). They have emerged as the rapidly evolving cryptography researchers in the area of information security.

Like RSA, ECC provides the highest strength-per-key-bit of any first generation public key system, according to research by Agarwal, S. (et al., 2015). ECC has performed better compared to RSA because fewer bits are needed to provide the same protection.

Agrawal, H. (et.al, 2016), presented a survey paper on an RFID authentication method based on elliptic curve cryptography. The plan was practical and applicable in circumstances where security is a top concern. The paper also discussed how the ECC authentication scheme greatly increases data security for a given key size. Because it uses less energy and generates less heat when the key size is smaller, it can be used to provide a certain degree of security. Smaller key sizes have the primary benefit of requiring less data, more compact software, and smaller chips to carry out quick cryptographic operations.

Based on a mod 4 congruence of 2-adic logarithms of Heegner points for specific elliptic curves E/Q with E(Q)[2] = Z/2Z, Kriz, D. (et al., 2017) proved a condition for prime twists of E to have analytic rank 0 or 1.

3 Prime Points on Elliptic Curve

If $y = ax^3 + bx^2 + cx + d$ is an elliptic curve then a point P(p,q) is said to be prime point if p and q both are primes.

Further, if $P(p_1,q_1)$ and $Q(p_2,q_2)$ are two prime points on elliptic curve such that P+Q is also a prime point then such an elliptic curve is called prime elliptic curve.

4 Characteristics of Prime Elliptic Curve

Number of pairs of prime points on a prime elliptic curve is called the characteristic of a prime elliptic curve.

5 Relationship between the Coefficients of Prime Elliptic Curve

Let,
$$y = ax^3 + bx^2 + cx + d \tag{2}$$

is a prime elliptic curve and $P(p_1,q_1)$ and $Q(p_2,q_2)$ are two points on it, then they must satisfy the equation of elliptic curve

$$q_1 = ap_1^3 + bp_1^2 + cp_1 + d$$
$$q_2 = ap_2^3 + bp_2^2 + cp_2 + d$$
$$q_1 - q_2 = a(p_1^3 - p_2^3) + b(p_1^2 - p_2^2) + c(p_1 - p_2)$$
$$(q_1 - q_2) / (p_1 - p_2) = a(p_1^2 + p_1p_2 + p_2^2) + b(p_1 + p_2) + c$$

Since the curve passing through $P(p_1,q_1)$ and $Q(p_2,q_2)$ therefore,
$$y - q_1 = [(q_2 - q_1) / (p_2 - p_1)] (x - p_1)$$

Let,
$$(q_2 - q_1) / (p_2 - p_1) = \alpha \tag{3}$$

Hence,
$$y - q_1 = \alpha (x - p_1)$$
$$y = \alpha (x - p_1) + q_1$$
$$ax^3 + bx^2 + cx + d = \alpha (x - p_1) + q_1 \quad \text{(using eqn. (2))}$$
$$ax^3 + bx^2 + (c - \alpha) x + d + \alpha p_1 - q_1 = 0 \tag{4}$$

Let α_1, α_2 and α_3 be the roots of equation (4) then, we must have
$$\alpha_1 + \alpha_2 + \alpha_3 = - b/a$$
$$p_1 + p_2 + \alpha_3 = - b/a$$

If $R(p_3,q_3)$ be the third point which satisfy equation (2) then
$$p_1 + p_2 + p_3 = - b/a \tag{5}$$
and
$$q_3 = \alpha (p_3 - p_1) + q_1$$

$$q_3 - q_1 = \alpha (p_3 - p_1)$$
$$(q_3 - q_1) / (p_3 - p_1) = \alpha$$
$$(q_3 - q_1) / (p_3 - p_1) = (q_2 - q_1) / (p_2 - p_1) \quad (6)$$

also, $$p_1p_2 + p_2p_3 + p_3p_1 = (c - \alpha) / a \quad (7)$$

and $$p_1p_2p_3 = (d + \alpha p_1 - q_1) / a \quad (8)$$

from (5), (7) & (8), we have

$$\left.\begin{aligned} a &= - b/(p_1 + p_2 + p_3) \\ &= (c - \alpha) / (p_1p_2 + p_2p_3 + p_3p_1) \\ &= (d + \alpha p_1 - q_1) / (p_1p_2p_3) \end{aligned}\right\} \quad (9)$$

Equation (9) shows the relationship between the coefficients a, b, c & d of prime elliptic curve (2).

6 Conclusion

The relationship between the prime elliptic curve's coefficients will be helpful for further research into the prime elliptic curve and can also be used to design more secure encryption and decryption algorithms in cryptography. By using the relationship between the coefficients, the elliptic curve can be transformed in such a way that makes it difficult for an unauthorised user to understand, which will result in a high level of security.

References

1 Miller, V. (1985) 'Use of elliptic curves in cryptography', *CRYPTO 85*: 417–426.

2 Koblitz, N. (1987) 'Elliptic curve cryptosystems', *Mathematics of Computation*, 48 (177): pp. 203– 209. JSTOR 2007884.

3 Broker, R. & Stevenhagen, P. (2007) 'Constructing elliptic curves of prime order', *Contemporary Mathematics, American Mathematical Society*, Volume XX, pp. 1-12.

4 Shanmugalakshmi, R. & Prabu, M. (2009) 'Research Issues on Elliptic Curve Cryptography and Its Applications', *International Journal of Computer Science and Network Security (IJCSNS)*, Vol.9 No.6, pp. 19-22.

5 Agarwal, S. & Uniyal, A.S. (2015) 'Elliptic Curves: An Efficient and Secure Encryption Scheme in Modern Cryptography', *International Journal of Advance Research in Science & Engineering (IJARSE)*, (ISSN 2319-8354 (E)), Volume 04, Issue 03, pp. 134-143.

6 Agrawal, H. & Badadapure, P.R. (2016) 'A Survey Paper on Elliptic Curve Cryptography', *International Research Journal of Engineering and Technology (IRJET)*, e-ISSN: 2395 -0056, p-ISSN: 2395-0072, Volume: 03 Issue: 04, pp. 2014-2018.

7 Kriz, D. & Li, C. (2017) 'Prime Twists of Elliptic Curves', *Department of Mathematics, Columbia University*, 2990 Broadway, New York, pp. 1-6.