A Metric on the Set of Elliptic Curves over $\mathbf{F}_p$

Pradeep Kumar Mishra[1] and Kishan Chand Gupta[2]

[1] Centre for Information Security and Cryptography,
University of Calgary,
CANADA

[2] Cryptographic Research Group,
Indian Statistical Institute,
Kolkata,
INDIA.

Abstract

Elliptic Curves over finite field have found application in many areas including cryptography. In the current article we define a metric on the set of elliptic curves defined over a prime field $\mathbf{F}_p, p > 3$.

Keywords: Elliptic Curves, Elliptic Curve Cryptosystems, Metric, Isomorphism Classes of Elliptic Curves.

1 Introduction

Elliptic curves are beautiful geometric entities which have fascinated mathematicians for more than a century. The curves have been studied at length and many of their interesting properties have been unearthed. In last two decades, the study of the curves received a new impetus when many of their applications were discovered. Particularly elliptic curve cryptosystems (ECC) (proposed jointly by Koblitz [2] and Miller [3] in 1985) built on the strength of elliptic curve discrete logarithm problem (ECDLP) integrated the study of the curves to the mainstream of cryptographic research. In the current article we propose a simple metric on the set of elliptic curves over a prime field $\mathbf{F}_p, p > 3$. For details about elliptic curve or elliptic curve cryptography the readers can refer to [1].

2 The Metric

The metric we propose is based on the concept of isomorphic classes of elliptic curves. Two curves on the same isomorphic class will have a finite distance between them. The distance of a curve from all the curves in an isomorphism class different than its own will be defined to be infinity.

Elliptic Curves Over Prime Fields $\mathbf{F}_p, p > 3$:, an elliptic curve is represented by an equation of the form

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

where $a, b \in \mathbf{F}_p$ and $4a^3 + 27b^2 \neq 0$. The set of rational points over $\mathbf{F}_p$ are the set of all points over $\mathbf{F}_p \times \mathbf{F}_p$ which satisfy this equation together with a special point, called the point at infinity.

Isomorphism on the set of elliptic curves over $\mathbf{F}_p$ is an equivalence relation defined as follows.

Isomorphic Curves: Let

$$C_i : y^2 = x^3 + a_i x + b_i, i = 1, 2$$

be two curves over $\mathbf{F}_p, p > 3$. C_1 is said to be isomorphic to C_2 if there exists a $t \in \mathbf{F}_p$ such that $a_2 = t^4 a_1$ and $b_2 = t^6 b_1$.

Let g be a generator of the field $\mathbf{F}_p$. Then, given any non-zero element $z \in \mathbf{F}_p$ there exists an integer $k \in \{0, 1, \cdots, p-2\}$ such that $z = g^k$. We will refer to the set $\{0, 1, \cdots, p-2\}$ as an index set of g. Note that the index set of g is not unique. Any residue class of $p-1$ can act as an index set. For defining the metric we will always use the index set $\{-\frac{p-1}{2}+1, -\frac{p-1}{2}+2, \cdots, -1, 0, 1, \cdots, \frac{p-1}{2}\}$. We will refer to this index set of a generator g as the *standard* index set of g.

Let C_1 and C_2 be any two curves over the $\mathbf{F}_p$. If C_1 and C_2 are not isomorphic we define the distance between them to be infinite. Otherwise let $t \in \mathbf{F}_p$ be the field element which transforms the parameter of C_1 to those of C_2 (or parameters of C_2 to those of C_1) (see the definition of isomorphic curve). Let $t = g^r$, where r is in the standard index set of g. Then we define the distance between C_1 and C_2 to be $|r|$[1]. That is

$d_g(C_1, C_2) = |r|$ if C_1 and C_2 are isomorphic and $t = g^r$,
$d_g(C_1, C_2) = \infty$ otherwise.

Now we claim that d_g as defined above is a metric.

Clearly, $d_g \geq 0$. Also, if C_1 and C_2 are the same curve, then they are isomorphic and for them $t = 1$ and $r = 0$. Hence it follows that $d_g(C_1, C_2) = 0$ if $C_1 = C_2$. To prove the converse is equally simple.

Next we will show that $d_g(C_1, C_2) = d_g(C_2, C_1)$. If these curves are not isomorphic then there is nothing to prove as both of these distances are ∞. So let us assume that they are isomorphic. Let $t = g^r$ be the element in $\mathbf{F}_p$ which transforms parameters of C_1 to those of C_2 (i.e. $a_2 = t^4 a_1, b_2 = t^6 b_1$). Then $t^{-1} = g^{-r}$ transforms parameters of C_2 to those of C_1 (i.e. $a_1 = {t^{-1}}^4 a_1, b_2 = {t^{-1}}^6 b_1$). Hence $d_g(C_1, C_2) = |r|$ and $d_g(C_1, C_2) = |-r|$, which are the same.

Finally, we have to prove the *triangle inequality*, i.e. we have to show that for any three curves $C_i, i = 1, 2, 3$,

$$d_g(C_1, C_2) + d_g(C_2, C_3) \geq d_g(C_1, C_3).$$

[1]there may be several t's which define the same isomorphism. Let $t_1, \ldots, t_l$ 'define' the same isomorphism. Write $t_i = g^{\alpha_i}; 1 \leq i \leq l$. Choose that i for which α_i is minimum.

Clearly, this is obvious if C_1 is not isomorphic to C_2 or C_2 is not isomorphic to C_3. In that case both sides of the inequality are ∞.

So let us assume that C_1 is isomorphic to C_2 and C_2 is isomorphic to C_3. As isomorphism is an equivalence relation C_1 is also isomorphic to C_3. Let

$$C_i : y^2 = x^3 + a_i x + b_i$$

$i = 1, 2, 3$. Then there exist $t_1, t_2 \in F_p$ and indices r_1, r_2 in the standard index set of g such that

$$a_2 = t_1^4 a_1, b_2 = t_1^6 b_1, t_1 = g^{r_1}$$

and

$$a_3 = t_2^4 a_2, b_3 = t_2^6 b_2, t_2 = g^{r_2}$$

Now

$$a_3 = (t_1 t_2)^4 a_1, b_3 = (t_1 t_2)^6 b_1$$

Let $t_1 t_2 = t_3 = g^{r_3}$. Then $r_3 = r_1 + r_2 (mod\ (p-1))$. Hence $r_3 \leq r_1 + r_2$. We have now,

$$d_g(C_1, C_2) = r_1,$$
$$d_g(C_2, C_3) = r_2,$$
$$d_g(C_1, C_3) = r_3,$$

Hence

$$d_g(C_1, C_2) + d_g(C_2, C_3) \geq d_g(C_1, C_3).$$

This etablishes the triangle inequality.

3 Conclusion

In this article, we have defined a metric on the set of elliptic curves over $\mathbf{F}_p$. The metric is dependent on the choice of the generator of the underlying field. A better metric will be the one which is independent over all generators. A candidate for such a metric can be $d(C_1, C_2) = \Sigma_g d_g(C_1, C_2)$ or we can take the average over all the generator dependent distances. One interesting open question is: does there exist one generator whose metric agrees with the average metric? Or is there a special class of fields for which there exist a generator whose corresponding metric agrees with the average metric?

References

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

[2] N. Koblitz. *Elliptic Curve Cryptosystems*, Mathematics of Computations, 48:203-209, 1987.

[3] V. S. Miller. Use of Elliptic Curves in Cryptography. In *CRYPTO'85*, LNCS 218, pp. 417-426, Springer-Verlag, 1985.