Int. Jr. of Engineering, Contemporary Mathematics and Sciences
Vol. 1, No. 1, January-June 2015
Copyright: MUK Publications
ISSN No: 2250-3099

Metrics on the set of elliptic curves over F_p

Francesca Vetro

Via Archirafi 34, 90123 Palermo, Italy
fvetro@math.unipa.it

Abstract. Let $p > 3$ be a prime number and let F_p be a finite field with p elements. In this note we define metrics on the set of elliptic curves over F_p. These metrics are independent on the choice of a generator of the multiplicative group of F_p.

Keywords: Metric, Elliptic curves, Finite fields, Isomorphism classes of elliptic curves, Elliptic curve cryptosystems.
2000 Mathematics Subject Classification: 94B27, 94A60.

1 Introduction

The study of elliptic curves over finite fields has received new impetus from the recent application of elliptic curves in cryptography. Today the elliptic curve cryptosystems are the more used. The security of such cryptosystems is connected to the difficulty of elliptic curve discrete logarithm problem (see for example [2, 4]). At present, in fact, it is not known an efficacious algorithm for the resolution of this problem.

In [5] was defined a metric on the set of elliptic curves over F_p that can have potential applications in resisting fixed table attack. The metric proposed in [5] is connected at the choice of a generator g of the multiplicative group of F_p. In this note we define simple metrics on the set of the elliptic curves over F_p that are independent on the choice of g.

2 Elliptic curves over F_p

Let $p > 3$ be a prime number and let F_p be a finite field with p elements. An elliptic curve E over F_p is defined by an equation of the form $y^2 = x^3 + ax + b$ where $a, b \in F_p$ and $4\ a^3 + 27\ b^2 \neq 0$. The points of E are all $(x, y) \in F_p \times F_p$ that satisfy this equation together with a *point at infinity*. The points of E form an abelian group whose group operation is denoted by $+$. The operation consisting in computing the multiple of a point, $Q = kP := P + P + \cdots + P$ (k-times), is called scalar multiplication.

We say that two elliptic curves over F_p, E_1 and E_2 defined by equations $y^2 = x^3 + a_1x + b_1$ and $y^2 = x^3 + a_2x + b_2$ respectively, are isomorphic if there exists an element $t \in F_p^*$ (the multiplicative group of F_p) such that $a_2 = t^4a_1$ and $b_2 = t^6b_1$ (see for example [6]). Note that there can be several elements in F_p^* which define the same isomorphism ψ between E_1 and E_2. Moreover, fixed a generator g of F_p^*, each $t \in F_p^*$ can be written as $t = g^\alpha$ with $\alpha \in \{0, \ldots, p-2\}$. Let $g^{\alpha_1}, \ldots, g^{\alpha_s}$ be the elements of F_p^* that define ψ. From now on we will choose to define ψ by the g^{α_i} for which α_i is minimum.

3 Metrics on E_{F_p}

Let us denote by E_{F_p} the set of all elliptic curves over F_p and by $\mathcal{Z}$ the ring of integer numbers. It is well known that, up to isomorphism, there is one and only one finite field of characteristic p with p elements. So each finite field with p elements is isomorphic to the field of the rest classes module p whose elements are $\{hp \ / \ h \in \mathcal{Z}\}$, $\{hp+1 \ / \ h \in \mathcal{Z}\}, \ldots, \{hp+(p-1) \ / \ h \in \mathcal{Z}\}$. We will write $\mathcal{Z}_p$ for this field and we will denote its elements by $\bar{0}, \bar{1}, \ldots, \overline{p-1}$ respectively.

Definition 3.1. Let $\bar{z_1}$ and $\bar{z}_2$ be two classes in $\mathcal{Z}_p$. We call absolute value *of* $\bar{z_1} - \bar{z}_2$ *the absolute value of* $z_1 - z_2$. *We denote the absolute value of* $\bar{z_1} - \bar{z}_2$ *by* $|\bar{z_1} - \bar{z}_2|$.

Remark 3.2. $|\bar{z_1} - \bar{z}_2| = 0$ if and only if $z_1 = z_2$. As $0 \leq z_1, z_2 \leq p-1$, we can affirm that $|\bar{z_1} - \bar{z}_2| = 0$ if and only if $\bar{z_1} = \bar{z}_2$. Hence if $\bar{z_1} \neq \bar{z}_2$ one has $|\bar{z_1} - \bar{z}_2| > 0$.

Let $\varphi : F_p \to \mathcal{Z}_p$ be an isomorphism. Let us denote by $d_\varphi : E_{F_p} \times E_{F_p} \to \mathbb{R}$ the map defined as:

$$d_\varphi(E_1, E_2) = |\varphi(a_1) - \varphi(a_2)| + |\varphi(b_1) - \varphi(b_2)|.$$

We affirm that d_φ *is a metric over* E_{F_p}. In fact $|\varphi(a_1) - \varphi(a_2)| + |\varphi(b_1) - \varphi(b_2)| \geq 0$ for each $E_1, E_2 \in E_{F_p}$. Furthermore $|\varphi(a_1) - \varphi(a_2)| + |\varphi(b_1) - \varphi(b_2)| = 0$ if and only if $\varphi(a_1) = \varphi(a_2)$ and $\varphi(b_1) = \varphi(b_2)$, i.e., if and only if $a_1 = a_2$ and $b_1 = b_2$ (see Remark 1). Because it is obvious that $d_\varphi(E_1, E_2) = d_\varphi(E_2, E_1)$, in order to prove that d_φ is a metric on E_{F_p} it is sufficient to show that

$$d_\varphi(E_1, E_3) \leq d_\varphi(E_1, E_2) + d_\varphi(E_2, E_3)$$

where $E_3 \in E_{F_p}$ is defined by the equation $y^2 = x^3 + a_3 x + b_3$.

Let $\varphi(a_i) = \bar{z}_i$ and $\varphi(b_i) = \bar{v}_i$ with $i = 1, 2, 3$. Note that

$$d_\varphi(E_1, E_3) = |\varphi(a_1) - \varphi(a_3)| + |\varphi(b_1) - \varphi(b_3)| = |\bar{z_1} - \bar{z_3}| + |\bar{v_1} - \bar{v_3}|.$$

Seeing that

$$|\bar{z_1} - \bar{z_3}| = |z_1 - z_3| = |z_1 - z_2 + z_2 - z_3| \leq |z_1 - z_2| + |z_2 - z_3| = |\bar{z}_1 - \bar{z}_2| + |\bar{z}_2 - \bar{z}_3|$$

and analogously $|\bar{v_1} - \bar{v_3}| \leq |\bar{v}_1 - \bar{v}_2| + |\bar{v}_2 - \bar{v}_3|$, one has

$$d_\varphi(E_1, E_3) \leq (|\bar{z}_1 - \bar{z}_2| + |\bar{v}_1 - \bar{v}_2|) + (|\bar{z}_2 - \bar{z}_3| + |\bar{v}_2 - \bar{v}_3|) = d_\varphi(E_1, E_2) + d_\varphi(E_2, E_3).$$

This assures that d_φ is a metric over E_{F_p}. Let $\varphi_1, \ \varphi_2, \ldots, \varphi_n$ be all the possible isomorphisms between F_p and $\mathcal{Z}_p$. The map $d_{\sum \varphi_i} : E_{F_p} \times E_{F_p} \to \mathbb{R}$ defined by

$$d_{\sum \varphi_i}(E_1, E_2) = \sum_{i=1}^{n} d_{\varphi_i}(E_1, E_2)$$

is clearly a metric over E_{F_p}. Moreover $d_{\sum \varphi_i}$ is independent on the choice of a particular isomorphism between F_p and $\mathcal{Z}_p$ and then $d_{\sum \varphi_i}$ is independent on the choice of a generator g of F_p^*.

As observed earlier, in [5], Mishra and Gupta defined a metric d_g on E_{F_p} and such metric is connected to the choice of a generator g of F_p^*. The metric d_g is based on the concept of isomorphism among elliptic curves and it is defined as:

$$\begin{aligned} d_g(E_1, E_2) &= |r| \text{ if } E_1 \text{ and } E_2 \text{ are isomorphic and } t = g^r, \\ d_g(E_1, E_2) &= \infty \text{ if } E_1 \text{ and } E_2 \text{ are not isomorphic.} \end{aligned}$$

By using d_g it is possible to define on E_{F_p} a new metric independent on the choice of g. In order to do this it is necessary to determine all the generators $g_1, \ldots, g_n$ of F_p^*. Once determined such generators, one can define a map $d_{\sum_{g_i}} : E_{F_p} \times E_{F_p} \to \mathbb{R}$ as follows:

$$\begin{aligned} d_{\sum_{g_i}}(E_1, E_2) &= \sum_{i=1}^{n} d_{g_i}(E_1, E_2) \text{ if } E_1 \text{ and } E_2 \text{ are isomorphic,} \\ d_{\sum_{g_i}}(E_1, E_2) &= \infty \text{ if } E_1 \text{ and } E_2 \text{ are not isomorphic.} \end{aligned}$$

This map is a metric on E_{F_p} with the request property.

Remark 3.3. Note that $d_{\sum_{g_i}}(E_1, E_2)$ is finite if and only if E_1 and E_2 are curves isomorphic, while $d_{\sum_{\varphi_i}}(E_1, E_2)$ is always finite. So $d_{\sum_{g_i}}$ is a metric different from $d_{\sum_{\varphi_i}}$.

A possible application

To protect the scalar multiplication on an elliptic curve $E_1 \in E_{F_p}$ against differential analysis (see [3]) it is recommended to randomize the base-point P and the multiplier k in the computation of $k\,P$. In order to do this one can transform the curve E_1 through various random morphisms. In particular, Joye and Tymen propose in [1] to perform the scalar multiplication on a random isomorphic elliptic curve and then to come back to the original elliptic curve. Otherwise they propose to compute the scalar multiplication on $\varphi(E_1)$ where $\varphi : F_p \to F_p'$ is an isomorphism (note that the isomorphism φ transforms the equation of an elliptic curve over F_p into the equation of an elliptic curve over F_p').

For way of this, one can decide to work on $\varphi(E_2)$ where $\varphi : F_p \to \mathcal{Z}_p$ is an isomorphism of fields and E_2 is an elliptic curve isomorphic to E_1. Then to return back to E_1 one can use φ and the distance $d_\varphi(E_1, E_2) = |\varphi(a_1) - \varphi(a_2)| + |\varphi(b_1) - \varphi(b_2)|$.

References

[1] M. Joye M and C. Tymen, Protections against differential analysis for elliptic curve cryptography, Cryptographic hardware and embedded systems–CHES 2001, LNCS 2162, Springer Verlag (2001) 377–390.

[2] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 48 (1987) 203–209.

[3] P. Kocher, J. Jaffe and B. Jun, Differential power analysis, Advances in cryptology–CRYPTO' 99, LNCS 1666, Springer Verlag (1999) 388–397.

[4] V.S. Miller, Use of elliptic curves in cryptography, Advances in cryptology–CRYPTO' 85, LNCS 218, Springer Verlag (1985) 417–426.

[5] P.K. Mishra and K.C. Gupta, A metric on the set of elliptic curves over F_p, Appl. Math. Lett. 21 (2008) 1330–1332.

[6] J.H. Silverman, The arithmetic of elliptic curves, Springer, GTM (1986).