Interdisciplinary Information Sciences Vol. 24, No. 1 (2018) 87–90
©Graduate School of Information Sciences, Tohoku University
ISSN 1340-9050 print/1347-6157 online
DOI 10.4036/iis.2018.S.01

SHORT COMMUNICATION

On the Fixed Points of an Elliptic-Curve Version of Self-Power Map

Hiroki SHIZUYA*

*Center for Information Technology in Education & Graduate School of Information Sciences,
Tohoku University, Sendai 980-8576, Japan*

Fixed points of the self-power map over a finite field have been studied in cryptology as a special case of modular exponentiation. In this note, we define an elliptic-curve version of the self-power map, enumerate the number of curves that contain at least one fixed point, and give its upper and lower bounds. Our result is a partial solution to the open question raised by Glebsky and Shparlinski in 2010.

KEYWORDS: fixed point, cryptographic primitive, elliptic curve, self-power map

1. Introduction

For p prime, define the modular exponentiation as $f_g(x) = g^x$ over the finite field $\mathbb{F}_p$. An h is said to be a fixed point of f_g if $f_g(h) = h$. For example, if $h \in \mathbb{F}_p^\times$ generates $\mathbb{F}_p^\times$ and h is also in $(\mathbb{Z}/(p-1)\mathbb{Z})^\times$, then we may define f_g so that h can be a fixed point by putting $g = h^{\bar{h}}$, where $h\bar{h} \equiv 1 \pmod{p-1}$. The number of such pairs (g, h) and other properties have been well studied [4–6] because too many fixed points could affect the security of cryptosystems based on the difficulty of discrete logarithm problem, which is the problem to compute f_g^{-1}. As a variant of f_g, we can define the self-power map modulo a prime: $f_s(x) = x^x \bmod p$. The fixed points of f_s have been explored also from a cryptographic viewpoint [1, 3].

In 2010, Glebsky and Shparlinski [4] improved the result on the fixed points of f_g and proposed to extend the discussion to cover elliptic curves. Let $E(\mathbb{F}_p)$ be an elliptic curve defined over a finite field $\mathbb{F}_p$ with p prime, and let N be the order of the group, namely $N = \#E(\mathbb{F}_p)$. They defined the map

$$f_{gs} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{F}_p, \quad t \mapsto x(tG),$$

where $G \in E(\mathbb{F}_p)$ is a base point and for $P = (u, v) \in E(\mathbb{F}_p)$, $x(P) = u$. Their interests were in the property of pairs (G, t) leading to fixed points such that $f_{gs}(t) = t$, but they left it as an open question.

In this note, we will tackle this open question in a restricted setting. Namely, we define

$$f : E(\mathbb{F}_p) \to E(\mathbb{F}_p), \quad G \mapsto x(G)G,$$

which is obtained by replacing t-multiple in f_{gs} above with $x(G)$-multiple. We investigate the fixed point P such that $f(P) = P$. Clearly, if P is a fixed point of f, such P leads to a fixed point of f_{gs} by putting $G = P$ and $t = x(P)$, i.e. for such (G, t), $f_{gs}(t) = t$. Note that our f can be regarded as an elliptic-curve version of f_s.

We will enumerate the number of elliptic curves that contain at least one fixed point of f and estimate its lower and upper bounds.

2. Preliminaries

In this section we will give notions and notations used in this note, and then mention our key idea to investigate the fixed points.

Throughout this note we assume that p is a prime >3. This enables us to keep discussion based on the same Wierstrass form $E : y^2 = x^3 + ax + b$ where (a, b) is in $\mathbb{F}_p \times \mathbb{F}_p$ but is excluded if the discriminant $\Delta(E) = 4a^3 + 27b^2 = 0$, i.e. the curve becomes singular for such (a, b). The elliptic curve defined over $\mathbb{F}_p$, denoted by $E(\mathbb{F}_p)$, is formed as the union of $\mathbb{F}_p$-rational points of E and $\{O\}$, where O is the identity of the elliptic-curve group $E(\mathbb{F}_p)$. Concerning the order of $E(\mathbb{F}_p)$, denoted by N, we have $N = \#E(\mathbb{F}_p) = p + 1 - a_p$ where $|a_p| \leq 2\sqrt{p}$. If we disregard isomorphisms among the curves, the number of elliptic curves defined over $\mathbb{F}_p$, denoted by N_c is given as $N_c = \#\{(a, b) \in \mathbb{F}_p^2\} - \#\{(a, b) \in \mathbb{F}_p^2 | \Delta(E) = 0\} = p^2 - p$.

Received March 19, 2018; Accepted April 27, 2018; J-STAGE Advance published May 25, 2018
ACM Computing Classification System: Theory of Computation → Computational complexity and cryptography; Cryptographic primitives
This work was supported in part by KAKENHI Grant Number 26330150.

*Corresponding author. E-mail: shizuya@cite.tohoku.ac.jp

An elliptic-curve version of the self-power map is defined as $f : E(\mathbb{F}_p) \to E(\mathbb{F}_p)$ by $f(G) = x(G)G$. We want to enumerate the number of curves that contain at least one fixed point $P \in E(\mathbb{F}_p)$ such that $f(P) = P$. We attempt to achieve this in two ways.

One is to count curves that have an $\mathbb{F}_p$-rational point at $x = 1$. For $P = (1, v)$, we have $f(P) = x(P)P = P$. We call such point *a trivial fixed point*, and denote by N_1 the number of curves that have such trivial fixed point.

The other approach is to count curves that have points of order 2. Suppose $P \in E(\mathbb{F}_p)$ is a point of order 2, that is $2P = O$. Since this implies $P = -P$, the generic form of P is expressed as $P = (u, 0)$, which means that u is a zero of E. Further, if u is odd, then we have for some $k \geq 0$, $f(P) = uP = (2k + 1)P = k(2P) + P = P$. Therefore P is a fixed point of f if P is a point of order 2 and $x(P)$ is odd. We call such point an *order-based fixed point* and denote by N_2 the number of curves that have at least one order-based fixed point.

3. Main Result

Theorem 3.1. *For $p > 3$,*

(i) $\dfrac{p(p+1)}{2} > N_1 \geq \dfrac{p(p-1)}{2}$ *and*

(ii) $N_2 \geq \dfrac{(p-1)(p-2)}{6}$.

Proof. (i) Recall that N_1 denotes the number of elliptic curves that have a trivial fixed point, in other words an $\mathbb{F}_p$-rational point at $x = 1$. We are to enumerate $E : y^2 = x^3 + ax + b$ such that $\Delta(E) \neq 0$ and E has a point $(1, v)$, that is $v^2 = a + b + 1$ and $4a^3 + 27b^2 \neq 0$. The former condition is equivalent to that $a + b + 1$ is in $\mathrm{QR}_p \cup \{0\}$, where QR_p denotes the set of quadratic residues mod$p$. Therefore the generic form of such curves should be

$$E_1 : y^2 = x^3 + sx + t^2 - s - 1,$$

where $s, t \in \mathbb{F}_p$. Then we have

$$\begin{aligned} N_1 &= \#\{s\} \times \#\{t^2\} - \#\{\text{singular curves}\} \\ &= \#\mathbb{F}_p \times \#(\mathrm{QR}_p \cup \{0\}) - \#\{(s,t) \in \mathbb{F}_p^2 | \Delta(E_1) = 0\} \\ &= p\left(\frac{p-1}{2} + 1\right) - \#\{(s,t) \in \mathbb{F}_p^2 | \Delta(E_1) = 0\}. \end{aligned}$$

Note that

$$p \geq \#\{(s,t) \in \mathbb{F}_p^2 | \Delta(E_1) = 0\} > 0,$$

where the right inequality follows from the fact that there exists at least one (s, t) such that $\Delta(E_1) = 0$ for any $p > 3$, namely $(s, t) = (0, 1)$.

Thus,

$$p\left(\frac{p-1}{2} + 1\right) > N_1 \geq p\left(\frac{p-1}{2} + 1\right) - p,$$

and the statement follows.

(ii) Define the n-multiple map $[n] : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p)$ by $P \mapsto nP$, where $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$. We write $E[n]$ to designate the n-torsion group defined as $E[n] = \{P \in E(\overline{\mathbb{F}}_p) | nP = O\} = \mathrm{Ker}([n]) \subseteq E(\overline{\mathbb{F}}_p)$. We also use $E(\mathbb{F}_p)[n]$ to express the set of $\mathbb{F}_p$-rational points in $E[n]$, namely $E(\mathbb{F}_p)[n] = E[n] \cap E(\mathbb{F}_p)$.

We are interested in P such that its order is 2 and $x(P)$ is odd. A point of order 2 can be found in $E[2]$ but may not be $\mathbb{F}_p$-rational. However, if $E[2] \subseteq E(\mathbb{F}_p)[2]$, i.e., every point in $E[2]$ is $\mathbb{F}_p$-rational, then we have $E[2] = \{O, P_1, P_2, P_3\}$ such that $P_1 = (\alpha, 0)$, $P_2 = (\beta, 0)$, $P_3 = (\gamma, 0)$ with $\alpha, \beta, \gamma \in \mathbb{F}_p$. By the group law in $E(\mathbb{F}_p)$ we also have $P_3 = P_1 + P_2$. This implies that

$$\alpha + \beta + \gamma = 0.$$

Since $p > 3$, at least one of α, β, γ is odd. The order-based fixed point always exists among such P_1, P_2, and P_3.

Consider the elliptic curve of the following form:

$$E_2 : y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

with $\alpha, \beta, \gamma \in \mathbb{F}_p$. Without loss of generality, we hereafter assume $0 \leq \alpha < \beta < \gamma < p$ so that $\Delta(E_2) \neq 0$. By the discussion above, every such $E_2(\mathbb{F}_p)$ has at least one order-based fixed point $P = (u, 0)$ with odd u.

As $\alpha + \beta + \gamma \equiv 0 \,(\mathrm{mod}\, p)$, the number of elliptic curves of the form E_2 is equivalent to the number of integer partitions of p or $2p$ into three distinct parts. It is easily seen that the number of partitions of n into m distinct parts is equal to the number of partition of $n - m(m-1)/2$ into m parts. We denote by $d(k, \ell)$ the number of integer partitions of k into ℓ parts. Formulas for $\ell = 2, 3$ can be found in [2]: $d(k,2) = \lfloor k/2 \rfloor + 1$ and $d(k,3) = \{(k+3)^2/12\}$, where $\lfloor x \rfloor$ is the floor function and $\{x\}$ denotes the integer nearest to x.

We are now ready to enumerate $E_2(\mathbb{F}_p)$ to estimate the lower bound of N_2. First, consider the following set:

$$D_p = \{(\alpha, \beta.\gamma) \in \mathbb{F}_p^3 \mid (\alpha + \beta + \gamma = p) \wedge (0 \le \alpha < \beta < \gamma < p)\}.$$

It is clear that $\#D_p$ is equivalent to the number of partitions of p into three distinct parts. By the formula, we have

$$\#D_p = d(p-3,3) = \left\{\frac{(p-3+3)^2}{12}\right\}.$$

Since $p > 3$, it holds that $p \equiv \pm 1 \pmod 6$, so

$$\#D_p = \left\{\frac{p^2}{12}\right\} = \frac{p^2}{12} - \frac{1}{12}.$$

We next investigate the set

$$D_{2p} = \{(\widetilde{\alpha}, \widetilde{\beta}.\widetilde{\gamma}) \in \mathbb{F}_p^3 \mid (\widetilde{\alpha} + \widetilde{\beta} + \widetilde{\gamma} = 2p) \wedge (0 < \widetilde{\alpha} < \widetilde{\beta} < \widetilde{\gamma} < p)\},$$

where $\widetilde{\alpha}$ cannot be 0 because there exists no partition satisfying the condition if $\widetilde{\alpha} = 0$. Note that $\widetilde{\alpha} + \widetilde{\beta} + \widetilde{\gamma} = 2p$ is equivalent to $(p - \widetilde{\alpha}) + (p - \widetilde{\beta}) + (p - \widetilde{\gamma}) = p$. Therefore, if $(\alpha, \beta.\gamma)$ with $\alpha > 0$ is in D_p, then $(p-\gamma, p-\beta, p-\alpha)$ is in D_{2p}. Conversely, if $(\widetilde{\alpha}, \widetilde{\beta}.\widetilde{\gamma})$ is in D_{2p}, then $(p - \widetilde{\gamma}, p - \widetilde{\beta}, p - \widetilde{\alpha})$ is in D_p.

Hence,

$$\begin{aligned}\#D_{2p} &= \#D_p - \#\{(0, \beta, \gamma) \in D_p\} \\ &= \frac{p^2 - 1}{12} - d(p-3, 2) \\ &= \frac{p^2-1}{12} - \left(\left\lfloor \frac{p-3}{2} \right\rfloor + 1\right) \\ &= \frac{p^2-1}{12} - \frac{p-1}{2}.\end{aligned}$$

We finally get

$$N_2 \ge \#D_p + \#D_{2p} = \frac{(p-1)(p-2)}{6}.$$

□

We now return to the open question raised by Glebsky and Shparlinski. Recall that they considered a map f_{gs} sending $t \in \mathbb{Z}/N\mathbb{Z}$ to $x(tG) \in \mathbb{F}_p$, where $N = \#E(\mathbb{F}_p)$, $G \in E(\mathbb{F}_p)$ is a base point and for $P = (u, v) \in E(\mathbb{F}_p)$, $x(P) = u$. Their interests are in the pairs (G, t) leading to fixed points such that $f_{gs}(t) = t$.

Assume that P is a fixed point of f. Then we can define $f_{gs}(t) = x(tP)$, and for $t = x(P)$, it holds that $f_{gs}(t) = t$. In other words, for every fixed point P of f, $(P, x(P))$ is a pair for a fixed point of f_{gs}. Hence an immediate corollary to Theorem 3.1 follows.

Corollary 3.2. *For $f_{gs}(t) = x(tG)$ defined over $E(\mathbb{F}_p)$ with $p > 3$, the following statements hold.*

(i) *If the base point G is of the form $G = (1, v)$, then $t = 1$ is a fixed point of f_{gs}, i.e., $f_{gs}(1) = x(1 \cdot G) = x(G) = 1$. The number of elliptic curves containing such G is at least $p(p-1)/2$, a half of elliptic curves defined over $\mathbb{F}_p$.*

(ii) *If the base point G is of the form $G = (u, 0)$ with $u = 2k + 1$ for some $k \ge 0$, then $t = u$ is a fixed point of f_{gs}, i.e., $f_{gs}(u) = x(uG) = x(G) = u$. The number of elliptic curves containing such G is at least $(p-1)(p-2)/6$.*

4. Concluding Remarks

We have explored the fixed points of f, an elliptic-curve version of the self-power map defined over $\mathbb{F}_p$ with $p > 3$, and estimated as mentioned in Theorem 3.1 the number of elliptic curves containing at least one fixed point in two ways. Those fixed points can also be the fixed points of f_{gs} that Glebsky and Shparlinski [4] left as an open question, so our result gives a partial solution to it, but is clearly far from the expected complete solution. Therefore we have a lot of things to do: for example, is there an efficient way to recognize that $E(\mathbb{F}_p)[n]$ contains a point P such that $x(P) = kn + 1$ for some k? and further, is there an elliptic curve that contains no fixed point of f or f_{gs} for any $p > 3$?

Acknowledgments

The author would like to thank Masahiro Mambo and an anonymous reviewer for their helpful comments to improve an earlier version of this paper.

REFERENCES

[1] Anghel, C. V., “The self-power map and collecting all residue classes,” *Mathematics of Computation*, **85**: 379–399 (2015).

[2] Andrews, G., and Eriksson, K., Integer Partitions, Cambridge University Press (2004).

[3] Friedrichsen, M., and Holden, J., “Statistics for fixed points of the self-power map,” arXiv:1403.5548v2 [math.NT] (2015).

[4] Glebsky, L., and Shparlinski, I., “Short cycles in repeated exponentiation modulo a prime,” *Design, Codes and Cryptography*, **56**: 35–42 (2010).

[5] Holden, J., “Fixed Points and Two-Cycles of the Discrete Logarithm,” *Algorithmic Number Theory Symposium (ANTS-V)*, LNCS 2369, Springer: 405–415 (2002).

[6] Holden, J., and Robinson, M. M., “Counting fixed points, two-cycles, and collisions of the discrete exponential function using p-adic methods,” *J. Australian Math. Soc.*, **92**: 163–178 (2012).