FIXED POINTS AND TWO-CYCLES OF THE SELF-POWER MAP

JOSHUA HOLDEN

The security of the ElGamal digital signature scheme against selective forgery relies on the difficulty of solving the congruence $g^{H(m)} \equiv y^r r^s \pmod{p}$ for r and s, given m, g, y, and p but not knowing the discrete logarithm of y modulo p to the base g. (We assume for the moment the security of the hash function $H(m)$.) Similarly, the security of a certain variation of this scheme given in, e.g., [11, Note 11.71], relies on the difficulty of solving

$$g^{H(m)} \equiv y^s r^r \pmod{p}. \tag{1}$$

It is generally expected that the best way to solve either of these congruences is to calculate the discrete logarithm of y, but this is not known to be true. In particular, another possible option would be to choose s arbitrarily and solve the relevant equation for r. In the case of (1), this boils down to solving equations of the form $x^x \equiv c \pmod{p}$. We will refer to these equations as "self-power equations", and we will call the map $x \mapsto x^x$ modulo p, or modulo p^e, the "self-power map". This map has been studied in various forms in [4–10, 12]. In this work we will investigate the number of fixed points of the map, i.e., solutions to

$$x^x \equiv x \pmod{p} \tag{2}$$

and two-cycles, or solutions to

$$h^h \equiv a \pmod{p} \quad \text{and} \quad a^a \equiv h \pmod{p}. \tag{3}$$

We will start by considering $F(p)$, the number of solutions to (2) such that $1 \leq x \leq p-1$, which lets us reduce the equation to $x^{x-1} \equiv 1 \pmod{p}$. Then we just need to consider the relationship between the order of x and of x^{x-1} modulo p and we can proceed as in [13] or [3] to prove:

Theorem 1.

$$\left| F(p) - \sum_{n \mid p-1} \frac{\phi(n)}{n} \right| \leq d(p-1)^2 \sqrt{p}(1 + \ln p),$$

where $d(p-1)$ is the number of divisors of $p-1$.

In the case of a prime power modulus we do not yet know how to extend the method to prove the corresponding result. However, if $G_e(p)$ is the number of solutions to $x^x \equiv x \pmod{p^e}$ with $1 \leq x \leq (p-1)p^e$ and $p \nmid x$, then we can use the p-adic methods of [10] to prove:

Theorem 2.

$$G_e(p) = (p-1) \left[\sum_{n \mid p-1} \frac{\phi(n)}{n} + p^{\lfloor e/2 \rfloor} - 1 \right].$$

In the case of two-cycles we have not yet finished the counting of the "singular solutions" where $ha \equiv 1 \pmod{p}$. Nevertheless if we let $T_e(p)$ be the number of pairs (h, a) such that h and $a \in \{1, 2, \ldots p(p-1)\}$, $p \nmid h$, $p \nmid a$, $ha \not\equiv 1 \pmod{p}$, and $h^h \equiv a^a \mod p^e$, then we have:

Theorem 3.

$$T_e(p) = \left[\sum_{c=1}^{p-1} \gcd(c-1, p-1) \sum_{n \mid \gcd(c, p-1)} \frac{\phi(n)}{n} \right] - \left[\sum_{d \mid p-1} d J_2\left(\frac{p-1}{d}\right) \right],$$

where J_2 is the Jordan totient function.

The first term in this equation counts all of the solutions modulo p and the second term counts the singular solutions. Each nonsingular solution lifts to a unique solution modulo p^e, whereas each singular solution may lift to more than one or none at all. Classifying these cases will result in a complete count of solutions.

References

[1] Antal Balog, Kevin A. Broughan, and Igor E. Shparlinski, *On the Number of Solutions of Exponential Congruences*, Acta Arithmetica **148** (2011), no. 1, 93–103, DOI 10.4064/aa148-1-7.

[2] Nicolas Bourbaki, *Commutative Algebra: Chapters 1-7*, 1st ed., Addison-Wesley, 1972.

[3] Cristian Cobeli and Alexandru Zaharescu, *An Exponential Congruence with Solutions in Primitive Roots*, Rev. Roumaine Math. Pures Appl. **44** (1999), no. 1, 15–22. MR2002d:11005

[4] Roger Crocker, *On a New Problem in Number Theory*, The American Mathematical Monthly **73** (1966), no. 4, 355–357.

[5] ———, *On Residues of n^n*, The American Mathematical Monthly **76** (1969), no. 9, 1028–1029.

[6] Matthew Friedrichsen, Brian Larson, and Emily McDowell, *Structure and Statistics of the Self-Power Map*, Rose-Hulman Undergraduate Mathematics Journal **11** (2010), no. 2.

[7] Joshua Holden, *Fixed Points and Two-Cycles of the Discrete Logarithm*, Algorithmic number theory (ANTS 2002), 2002, pp. 405–415.

[8] ———, *Addenda/corrigenda: Fixed Points and Two-Cycles of the Discrete Logarithm*, 2002. Unpublished, available at `http://xxx.lanl.gov/abs/math.NT/0208028`.

[9] Joshua Holden and Pieter Moree, *Some Heuristics and Results for Small Cycles of the Discrete Logarithm*, Mathematics of Computation **75** (2006), no. 253, 419–449.

[10] Joshua Holden and Margaret M. Robinson, *Counting Fixed Points, Two-Cycles, and Collisions of the Discrete Exponential Function using p-adic Methods*, Journal of the Australian Mathematical Society. special issue dedicated to Alf van der Poorten, to appear.

[11] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC, 1996.

[12] Lawrence Somer, *The Residues of n^n Modulo p*, Fibonacci Quarterly **19** (1981), no. 2, 110–117.

[13] Wen Peng Zhang, *On a Problem of Brizolis*, Pure Appl. Math. **11** (1995), no. suppl., 1–3. MR98d:11099

Department of Mathematics, Rose-Hulman Institute of Technology, Terre Haute, IN 47803, USA
E-mail address: `holden@rose-hulman.edu`