STATISTICS FOR FIXED POINTS OF THE SELF-POWER MAP

MATTHEW FRIEDRICHSEN AND JOSHUA HOLDEN

The "self-power map" $x \mapsto x^x$ modulo p is related to a variation of the ElGamal digital signature scheme. It is similar in this way to the discrete exponentiation map, but it has received much less study. In particular, an individual wishing to forge a signature for a selected message must solve the congruence

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

for r and s, given m, g, y, and p but not knowing the discrete logarithm of y modulo p to the base g. (See, e.g., [12, Note 11.71] for this variation. We assume for the moment the security of the hash function $H(m)$.) It is generally expected that the best way to solve this congruence 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".

The self-power map and self-power equations have been studied in various forms in [1–4, 6–11, 13]. We investigate, both theoretically and experimentally, the number of fixed points of the map, i.e., solutions to

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

between 1 and $p-1$. In particular, we would like to know whether the distribution across various primes behaves as we would expect if the self-power map were a "random map". We do this by creating a model in which values of a map are assumed to occur uniformly randomly except as forced by the structure of the self-power map. The model uses the following heuristic, which is related to those in [9, Section 6]:

Heuristic 1. *The map $x \mapsto x^x \bmod p$ is a random map in the sense that for all p, if x, y are chosen uniformly at random from $\{1, \dots, p-1\}$ with $\operatorname{ord}_p x = d$, then*

$$\Pr[x^x \equiv y \pmod{p}] \approx \begin{cases} \frac{1}{d} & \textit{if } \operatorname{ord}_p y \mid d, \\ 0 & \textit{otherwise.} \end{cases}$$

We can then predict the distribution of the number of fixed points of this random map and compare it statistically to the actual self-power map. Let $F_d(p)$ be the number of solutions to (2) with $1 \le x \le p-1$ and $\operatorname{ord}_p x = d$. A binomial model then predicts (see [5] for more details):

Prediction 1. $\Pr[F_d(p) = k] = \binom{\phi(d)}{k} \left(\frac{1}{d}\right)^k \left(\frac{d-1}{d}\right)^{\phi(d)-k}$

Data was collected for 238 primes starting at 100,000 and 599 primes starting at 1,000,000. A chi-squared goodness-of-fit test gave a p-value of 0.198, so we do not see statistical evidence that our predictions are incorrect. However, a sliding window imposed on the data indicated that strong divergence from the predictions occurs with particularly small and particularly large values of d. This led us to augment our model with specific predictions in the cases $d = 3$, $d = 4$, $d = 6$, $d = (p-1)/3$, and $d = (p-4)/4$, which take into account the lack of independence in the fixed points for these orders. Chi-squared tests suggest that the new models account for the deviations from the original model in these cases. Furthermore, chi-squared tests were done using the original model for $d = 5$ and $d = 7$ which indicated that corrections were not necessary in those cases. Likewise orders in the range $(p-1)/5$ to $(p-1)/13$ do not appear to be showing significant deviation from the original model. However, the sliding window chi-squared test shows evidence of possible divergence from the predictions in the neighborhood of $(p-1)/16$. It is not clear yet whether this is a true problem with the model, or just a "random" consequence of the particular primes that we picked.

So far, these results do not clearly indicate any "nonrandom" structure in the self-power map when the lack of independence is accounted for. We continue to search for such structure in the distribution of fixed points and also in larger cycles. If nonrandom structure does exist, it may be possible to exploit it to break the signature scheme mentioned above or others like it.

References

[1] Catalina Voichita Anghel, *The Self Power Map and its Image Modulo a Prime*, PhD Thesis, University of Toronto, 2013.

[2] 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.

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

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

[5] Matthew Friedrichsen and Joshua Holden, *Bounds and Statistics for Fixed Points of the Self-Power Map*, arXiv:1403.5548 [math] (2014).

[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] Joshua Holden, *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 **92** (2012), 163–178.

[11] Pär Kurlberg, Florian Luca, and Igor Shparlinski, *On the Fixed Points of the Map $x \mapsto x^x$ Modulo a Prime*, arXiv:1402.4464 [math] (2014). To appear in Mathematical Research Letters.

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

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

Madison, WI, USA
E-mail address: `friedrichsenm@gmail.com`

Department of Mathematics, Rose-Hulman Institute of Technology, 5500 Wabash Avenue, Terre Haute, IN 47803-3999, USA
E-mail address: `holden@rose-hulman.edu`