

An Exploration of Diffie-Hellman Permutations

Master Thesis Defense

Tommy Pham

Temple University

Advisor: Dr. Vasily Dolgushev

October 12, 2026

Primes and their Primitive Roots

Recall that, for every prime p , the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of units of the ring $\mathbb{Z}/p\mathbb{Z}$ is a cyclic group of order $p - 1$.

Definition (Primitive Root)

Given a prime p , a positive integer b is a primitive root relative to p if its residue class modulo p , $b + p\mathbb{Z}$, generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$.

Notation: For a positive integer n and an integer a , we will denote by $\text{rem}(a, n)$ the nonnegative remainder of division of a by n .

Further,

$$\underline{\text{rem}}(a, n) = \begin{cases} \text{rem}(a, n), & \text{if } n \nmid a, \\ n, & \text{if } n \mid a. \end{cases}$$

The Discrete Logarithm Problem for $(\mathbb{Z}/p\mathbb{Z})^\times$

Consider a "large" prime p (e.g. p has ≈ 100 decimal digits).

Let b be a primitive root relative to p . Then

$$\langle b + p\mathbb{Z} \rangle = (\mathbb{Z}/p\mathbb{Z})^\times.$$

So for an integer $1 \leq y \leq p-1$, $\exists!$ integer $1 \leq x \leq p-1$ such that

$$b^x \equiv y \pmod{p}.$$

Given y , it is computationally challenging to solve for x . The task of solving for an integer x that satisfies the congruence above is called the Discrete Logarithm Problem (DLP) for the group $(\mathbb{Z}/p\mathbb{Z})^\times$.

For example:

Let $p = 10^9 + 7$ and then 5 is a primitive root modulo p . We are interested in solving for the congruence

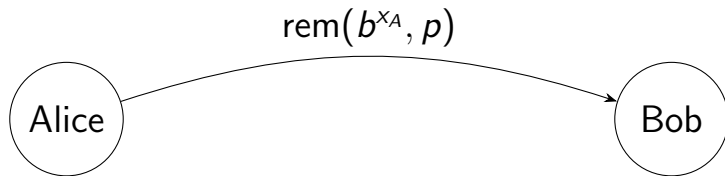
$$5^x \equiv 23 \pmod{p}.$$

It took my computer (with the Apple M1 Pro chip and 16 GB RAM) 14.15 minutes to solve for $x = 82047235$.

Diffie-Hellman Key Exchange Protocol

Alice and Bob agree on a pair (p, b) , where p is a large prime and b is a primitive root modulo p .

Alice then chooses an integer $1 < x_A < p - 1$ and Bob then also chooses an integer $1 < x_B < p - 1$.



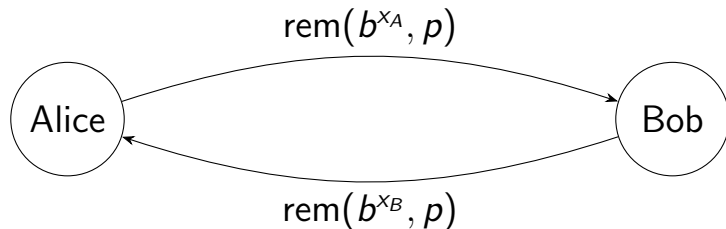
Alice then computes the residue class $(\bar{b}^{x_B})^{x_A}$ and Bob computes the residue class $(\bar{b}^{x_A})^{x_B}$. Note that

$$(\bar{b}^{x_B})^{x_A} = \bar{b}^{x_B x_A} = (\bar{b}^{x_A})^{x_B} \implies \text{This is their shared secret key.}$$

Diffie-Hellman Key Exchange Protocol

Alice and Bob agree on a pair (p, b) , where p is a large prime and b is a primitive root modulo p .

Alice then chooses an integer $1 < x_A < p - 1$ and Bob then also chooses an integer $1 < x_B < p - 1$.



Alice then computes the residue class $(\bar{b}^{x_B})^{x_A}$ and Bob computes the residue class $(\bar{b}^{x_A})^{x_B}$. Note that

$$(\bar{b}^{x_B})^{x_A} = \bar{b}^{x_B x_A} = (\bar{b}^{x_A})^{x_B} \implies \text{This is their shared secret key.}$$

Baby-Step Giant-Step

Let $G = \langle g \rangle$ be a cyclic group of order t and consider the DLP

$$g^x = y.$$

Set $s = \lceil \sqrt{t} \rceil$.

$$x = a_0 + a_1 s,$$

where $0 \leq a_0 < s$ and $0 \leq a_1 < s$.

We then compute the baby step list

$$1, g, g^2, \dots, g^{s-1}.$$

Baby-Step Giant-Step Continued

The giant step list consists of elements

$$y, yg^{-s}, yg^{-2s}, \dots, yg^{-(s-1)s}.$$

If $x = a_0 + a_1s$, then

$$g^x = g^{a_0 + a_1s} = g^{a_0}(g^s)^{a_1}.$$

Since $y = g^x$, so

$$g^{a_0} = yg^{-a_1s}.$$

So there must exist indices p, q such that

$$g^p = yg^{-qs}$$

with $0 \leq p, q < s$.

Comparing exponents, we conclude

$$x \equiv p + qs \pmod{t}.$$

Time Complexity of BSGS

- Computing the baby list takes $s - 1$ operations.
- Computing the giant list takes another $s - 1$ operations.
- Creating a dictionary to store the baby list takes $s - 1$ steps.

Thus, the total runtime is

$$O(s - 1) + O(s - 1) + O(s - 1) = O(s) = O(\sqrt{t}).$$

Suppose we know a non-trivial factorization of $t = ab$, where $\gcd(a, b) = 1$.

- Reduction method
 - Runtime: $O(\log(t) + \sqrt{a} + \sqrt{b})$.
- Index Calculus
 - Runtime: $O(\exp((c + o(1))\sqrt{\ln t \ln \ln t}))$.

Motivation

Let $X := \{1, 2, \dots, p-1\}$ be the set of *exponents*.

Definition (The Key DH Permutation)

For a prime $p \geq 7$, let g_p be the smallest positive primitive root modulo p , then

$$\tau_p(x) := \text{rem}(g_p^x, p), \quad x \in X.$$

For example,

$$\tau_7 = (1, 3, 6) \quad \text{and} \quad \tau_{11} = (1, 2, 4, 5, 10)(6, 9).$$

For a given prime p and an integer $1 \leq y \leq p-1$, solving the equation

$$\tau_p(x) = y \iff \text{Solving the discrete log of } y \text{ w.r.t the base } g_p \text{ modulo } p.$$

Motivation (Continued)

- We explore new ways to solve the DLP for $(\mathbb{Z}/p\mathbb{Z})^\times$
- We seek a suitable composition of permutations such that the permutation

$$(h_1 \circ h_2 \circ \dots \circ h_n) \circ \tau_p$$

has one of the following properties:

- A relatively large number of fixed points
- A relatively long cycle type
- The length of the longest cycle is relatively short

For the first property, we may then be more likely to recover the exponent x in the equation $\tau_p(x) = y$.

The last two properties are useful for cycle attacks.

Motivation (Continued)

- We also would like to propose an authentication protocol that we think is secure
- Elliptic curves are useful, but often harder to implement
- For those smaller companies that lack resources, we would like to propose a simpler protocol that is still secure

What Are Diffie-Hellman(DH) Permutations?

Recall that $X := \{1, 2, \dots, p-1\}$ is the set of exponents. Consider a prime $p \geq 7$. Let g_p be the smallest integer such that

$$\langle g_p + p\mathbb{Z} \rangle = (\mathbb{Z}/p\mathbb{Z})^\times.$$

We identify X with the ring $\mathbb{Z}/(p-1)\mathbb{Z}$ and the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ via the following bijections

$$x \mapsto x + (p-1)\mathbb{Z} \quad \text{and} \quad x \mapsto x + p\mathbb{Z},$$

respectively.

What Are Diffie-Hellman(DH) Permutations? (Continued)

Definition (Binary Operations on X)

For $x, y \in X$,

$$x + y := \underline{\text{rem}}(x + y, p - 1), \quad x \cdot y := \underline{\text{rem}}(xy, p - 1)$$

and

$$x * y := \text{rem}(xy, p).$$

What Are Diffie-Hellman(DH) Permutations? (Continued)

The group

$$\text{Aff}_{p-1} := \text{Aff}(\mathbb{Z}/(p-1)\mathbb{Z}) = \{f_{a,b} : x \mapsto ax + b \mid a \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times, b \in \mathbb{Z}/(p-1)\mathbb{Z}\}.$$

Aff_{p-1} acts on X via the maps

$$f_{a,b}(x) := ax + b \pmod{p-1}, \text{ where } a \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times, b \in \mathbb{Z}/(p-1)\mathbb{Z}.$$

The action of Aff_{p-1} on X induces a homomorphism

$$\begin{aligned} \Phi : \text{Aff}_{p-1} &\longmapsto S_{p-1}, \\ f_{a,b} &\longmapsto \Phi(f_{a,b}) : x \longmapsto f_{a,b}(x) = ax + b \pmod{p-1}, \forall x \in X. \end{aligned}$$

Φ is injective

What Are Diffie-Hellman(DH) Permutations? (Continued)

Another group action coming from the cyclic group $\mathcal{Z}_{p-1} = \langle \mu_{g_p} \rangle$, where

$$\mu_{g_p}(x) := g_p * x.$$

Similarly,

$$\begin{aligned}\Psi : \mathcal{Z}_{p-1} &\longmapsto S_{p-1}, \\ \mu_{g_p}^k &\longmapsto \Psi(\mu_{g_p}^k) := x \mapsto \mu_{g_p}^k(x), \forall x \in X.\end{aligned}$$

Ψ is injective; thus, we may identify $\mathcal{Z}_{p-1}$ with its images in S_{p-1} .

We consider the subgroup $R_p \leq S_{p-1}$ generated by elements of Aff_{p-1} and the permutation μ_{g_p} .

What Are Diffie-Hellman(DH) Permutations? (Continued)

Theorem

Let $p \geq 7$ be a prime number. Then the permutation μ_{g_p} and elements of Aff_{p-1} generate the symmetric group S_{p-1} .

To prove the above theorem, we need the following lemma

Lemma

Let $p \geq 7$ be a prime number,

$$\rho := (1, 2, \dots, p-1)$$

and μ_2 be the permutation in S_{p-1} defined by the formula

$$\mu_2(x) := 2 * x.$$

Then,

$$\mu_2 \circ \rho \circ \mu_2^{-1} = (1, 2) \circ \rho^2.$$

What Are Diffie-Hellman (DH) Permutations? (Continued)

A few words about the proof of the theorem.

From a quick observation, $f_{1,1} \in \text{Aff}_{p-1}$.

Then it follows that $\rho \in \text{Aff}_{p-1}$.

Further, $\mu_{x_1} \circ \mu_{x_2} = \mu_{x_1 * x_2}$. Since the residue class $g_p + p\mathbb{Z}$ generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$, there exists an integer $t \in \mathbb{Z}_{>0}$ such that

$$g_p^t \equiv 2 \pmod{p}.$$

It follows that $\mu_2 = \mu_{g_p^t} = \mu_{g_p}^t \in R_p$.

Therefore, from the lemma, we have that $(1, 2) \circ \rho^2 \in R_p$.

Thus, we have that $(1, 2) \in R_p$ and $\rho \in R_p$.

It is well-known that the symmetric group S_{p-1} is generated by the transposition $(1, 2)$ and the cycle ρ .

Thus, $R_p = S_{p-1}$.

What Are Diffie-Hellman (DH) Permutations? (Continued)

Now we are ready to define the Diffie-Hellman permutations.

Recall that

$$\tau_p(x) := \text{rem}(g_p^x, p), \quad x \in X.$$

Definition (Diffie-Hellman Permutations)

Let $p \geq 7$ be a prime number, τ_p be the key DH permutation, and R_p be the subgroup of S_{p-1} generated by elements of the groups Aff_{p-1} and $\mathcal{Z}_{p-1}$. Let L, R be non-empty subsets of R_p . Then, elements of the set

$$\{a \circ \tau_p \circ b : a \in L, b \in R\}.$$

are called *Diffie-Hellman (DH) permutations*.

Unlocking Permutations

Note that

$$\mu_{g_p}(x) := g_p * x.$$

Remark: Let $p \geq 7$ be a prime, τ_p be the key DH permutation, $\rho := (1, 2, \dots, p-1)$ and μ_{g_p} be the permutations in S_{p-1} . Then there exists a unique permutation $h_{unlock} \in \langle \rho, \mu_{g_p} \rangle$ such that

$$h_{unlock} \circ \tau_p = \text{id}_X.$$

We think that, in practice, it may be very challenging to find such a permutation h_{unlock} for a given prime p .

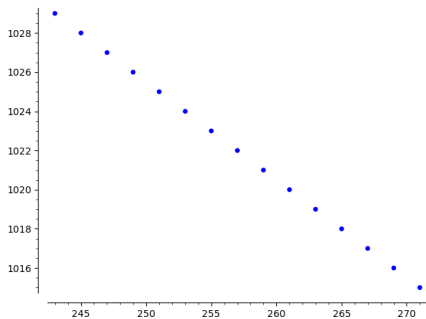
Therefore, we call a permutation h an *unlocking permutation* if $h \circ \tau_p$ has one of the properties that I mentioned earlier:

- A relatively large number of fixed points
- A relatively long cycle type
- The length of the longest cycle is relatively short

What Did We Try & See?

For a prime $p \geq 7$, we considered the permutations

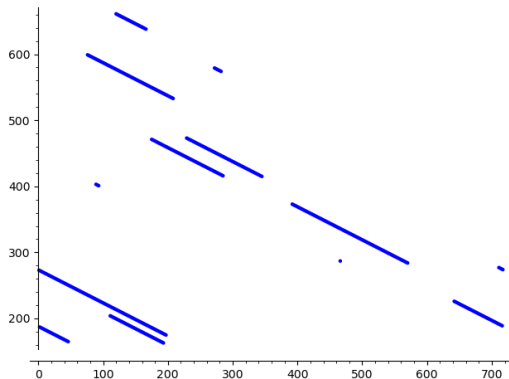
$$\rho^j \circ \mu_2 \circ \rho^k \circ \tau_p, \text{ where } 1 \leq j, k < p - 1.$$



For a prime $p = 1307$ and pair (j, k) in the plot above, the number of fixed points of the permutation $\rho^j \circ \mu_2 \circ \rho^k \circ \tau_p$ is the greatest among all pairs (j, k) with $1 \leq j, k < p - 1$. However, the number of fixed points is only 7 out of 1306, which is $\frac{7 \times 100}{1306} = 0.5355\%$.

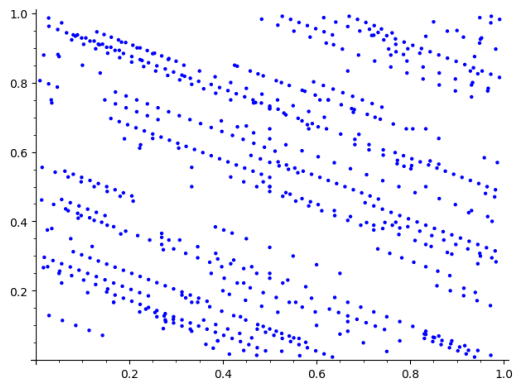
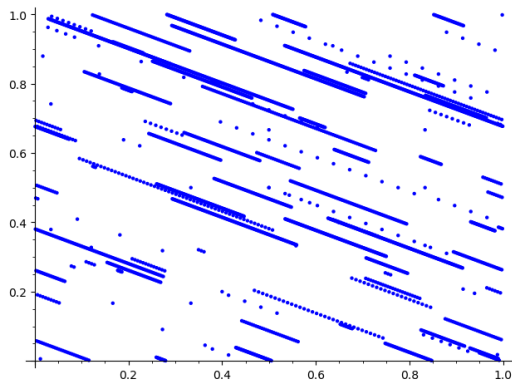
What Did We See?

Similarly, for prime $p = 719$, we get the following plot



The for a pair (j, k) in the plot above, the number of fixed points of the permutation $\rho^j \circ \mu_2 \circ \rho^k \circ \tau_p$ is the greatest among all pairs (j, k) with $1 \leq j, k < p - 1$. However, the number of fixed points is only 5 out of 718, which is $\frac{5 \times 100}{718} = 0.6963\%$.

What Did We see? (Continued)



The left plot is for the first 30 safe primes and the right plot is for the first 30 primes. The x, y -axes are the normalized values of j and k that maximize the number of fixed points of the permutation $\rho^j \circ \mu_2 \circ \rho^k \circ \tau_p$. The maximum percentage of the number of fixed points for the first 30 safe primes is 0.512% for prime $p = 1367$ and the maximum percentage of the number of fixed points for the first 30 primes is 4.411% for prime $p = 137$.

An Authentication Protocol Based on DH Permutations

- Alice and Bob agree on a large prime p and a primitive root b modulo p . For example, take $b := g_p$.
- Alice chooses a random integer $1 < x < p - 1$ and calculates the following integers:

$$r_x := \text{rem}(b^x, p) \quad \text{and} \quad c := \text{rem}(x - r_x, p - 1).$$

- Alice keeps x secret and publishes the triple (p, b, c) .
- When it is time, Alice sends an important message to Bob. However, Bob does not know if the message is from Alice or an imposter.
- Alice then sends x to Bob via a secure channel. Bob then calculates

$$r_x := \text{rem}(b^x, p)$$

and checks whether $r_x \equiv x - c \pmod{p - 1}$.

The Security of the Protocol

- The security of the protocol relies on the assumption that the function

$$C_{p,b}(x) := c, \quad x \in \{1, 2, \dots, p-1\},$$

where $c := \text{rem}(x - r_x, p-1)$, is a pre-image resistant function.

- If Eve tries to impersonate Alice, she must find an integer $\tilde{x}$ such that

$$r_{\tilde{x}} \equiv \tilde{x} - c \pmod{p-1}.$$

We believe that the tools that we discussed earlier are not useful in finding such an integer $\tilde{x}$. This is because those tools are suitable for solving the congruence

$$b^x \equiv y \pmod{p}.$$

where b is a primitive root modulo p and y is a given integer. However, in our case, the RHS depends on the unknown integer x .

The Security of the Protocol (Continued)

- We also tried to implement a modified version of the BSGS algorithm to solve for $\tilde{x}$ in the congruence

$$r_{\tilde{x}} \equiv \tilde{x} - c \pmod{p-1}.$$

For a prime p , we let $r_x := \text{rem}(g_p^x, p)$. Let $N \approx \sqrt{p-1}$ and $\beta := \bar{g}_p$.

Then we compute the baby step list: $\beta, \beta^2, \dots, \beta^{N-1}$.

Then we compute the giant step list: $\beta^N, \beta^{2N}, \dots, \beta^{(N-1)N}$.

For any $1 \leq x \leq p-1$, we may write $x = x_0 + x_1 N$, where $0 \leq x_0, x_1 < N$. Then we check if

$$\beta^{x_0 + x_1 N} = \begin{cases} \overline{x_0 + x_1 N - c}, & \text{if } x \geq c, \\ \overline{x_0 + x_1 N - c - 1}, & \text{if } x < c. \end{cases}$$

The Security of the Protocol (Continued)

- We also tried to implement a modified version of the BSGS algorithm to solve for $\tilde{x}$ in the congruence

$$r_{\tilde{x}} \equiv \tilde{x} - c \pmod{p-1}.$$

For a prime p , we let $r_x := \text{rem}(g_p^x, p)$. Let $N \approx \sqrt{p-1}$ and $\beta := \bar{g}_p$.

Then we compute the baby step list: $\beta, \beta^2, \dots, \beta^{N-1}$.

Then we compute the giant step list: $\beta^N, \beta^{2N}, \dots, \beta^{(N-1)N}$.

For any $1 \leq x \leq p-1$, we may write $x = x_0 + x_1 N$, where $0 \leq x_0, x_1 < N$. Then we check if

$$\beta^{x_0+x_1 N} = \begin{cases} \overline{x_0 + x_1 N - c}, & \text{if } x \geq c, \\ \overline{x_0 + x_1 N - c - 1}, & \text{if } x < c. \end{cases}$$

This algorithm turned out to be slower than using brute-force! We also looked into quantum algorithms such as Shor's algorithm but as of now, we do not think it is helpful in solving for a desired exponent x .

Fixed points may be a vulnerability

For a prime p and its primitive root b , we set

$$\nu(p, b) := \max(\{\text{nfp}(\rho^c \circ \tau_{p,b}) \mid 1 \leq c \leq p-1\}).$$

where $\text{nfp}(h)$ denotes the number of fixed points of the permutation h .

Set

$$r_{\tilde{x}} := \text{rem}(b^{\tilde{x}}, p).$$

Thus, if Eve chooses an integer $\tilde{x}$ uniformly at random from $\{1, 2, \dots, p-1\}$, the probability that $\tilde{x}$ satisfies

$$r_{\tilde{x}} \equiv \tilde{x} - c \pmod{p-1}$$

is at most

$$\frac{\nu(p, b)}{p-1}.$$

Note: We will suppress b and just write $\nu(p)$ from now on.

Evidence of small number of fixed points

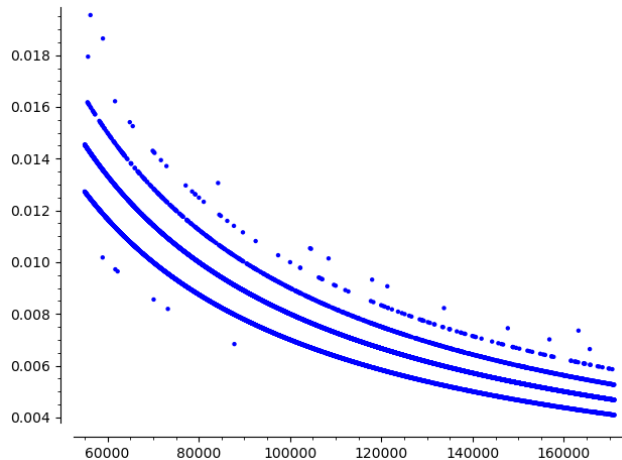


Figure: Values of $\frac{100\nu(p)}{p-1}$ for 10,000 primes in the range $55,001 \leq p \leq 171,049$.

Evidence of small number of fixed points

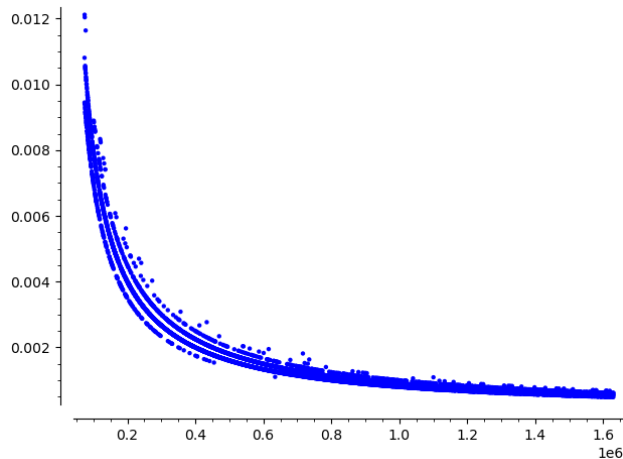


Figure: Values of $\frac{100\nu(p)}{p-1}$ for 6,000 safe primes in the range $74,027 \leq p \leq 1,629,899$.

Bound on the number of fixed points

Theorem

Let $p \geq 7$ be a prime integer. Then

$$\nu(p) \leq (p-1)^{1/2} + (p-1)^{1/4} + \frac{1}{2}.$$

We will use the following results from Javier Cilleruelo (2009) to prove the theorem.

Definition

A *Sidon set* is a subset of a semigroup G having the property that all sums of two elements are distinct. Equivalently, if $a, b, c, d \in G$ and $a - b = c - d$, then $\{a, b\} = \{c, d\}$.

Corollary (Cilleruelo)

Let $F \subseteq \{1, \dots, n\}$ be a Sidon set. Then $\#F \leq n^{1/2} + n^{1/4} + \frac{1}{2}$.

Outline of the proof of the theorem

Let p be prime. Let b be a primitive root modulo p , fix $c \in \{1, 2, \dots, p-1\}$.

Let

$$A_c := \{x \in X \mid r_x \equiv x - c \pmod{p-1}\}$$

and

$$S_{p,b,c} := \{r \in \{1, 2, \dots, p-1\} \mid b^{r+c} \equiv r \pmod{p}\}.$$

Note that A_c is just a set of fixed points of $\rho^c \circ \tau_p$. In the proof, we show that the map

$$\phi : A_c \longmapsto S_{p,b,c}, \quad x \longmapsto r_x := \text{rem}(b^x, p)$$

is a bijection.

Then we show that $S_{p,b,c}$ is a Sidon set. Therefore, by the corollary by Cilleruelo,

$$\#A_c = \#S_{p,b,c} \leq (p-1)^{1/2} + (p-1)^{1/4} + \frac{1}{2}.$$

A follow up corollary

The previous theorem motivates the following corollary:

Corollary

$$\lim_{\substack{p \rightarrow \infty \\ p \text{ prime}}} \frac{\nu(p)}{p-1} = 0.$$

From the previous theorem, we have

$$\#S_{p, g_p, c} \leq (p-1)^{1/2} + (p-1)^{1/4} + \frac{1}{2}.$$

This bound is independent of c . Therefore, by the definition of $\nu(p)$,

$$0 \leq \frac{\nu(p)}{p-1} \leq \frac{(p-1)^{1/2} + (p-1)^{1/4} + \frac{1}{2}}{p-1} = (p-1)^{-1/2} + (p-1)^{-3/4} + \frac{1}{2(p-1)}.$$

The right-hand side tends to 0 as $p \rightarrow \infty$. Thus, $\lim_{\substack{p \rightarrow \infty \\ p \text{ prime}}} \frac{\nu(p)}{p-1} = 0$.

There may be a sharper bound

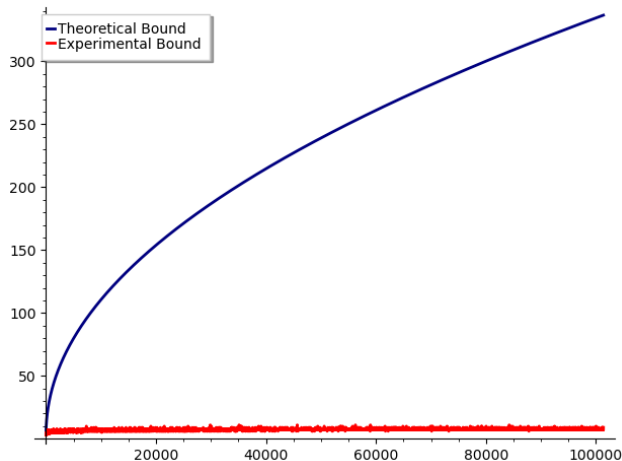


Figure: Theoretical Bound (in blue) vs Experimental Bound (in red) for the smallest positive primitive root modulo p .

A relevant piece of information

We found that people also study the congruence

$$g^h \equiv h \pmod{p},$$

where $1 \leq g, h \leq p - 1$. This may be relevant to our work! We are not sure if this would help us achieve a better bound on the number of fixed points.

Bibliography

-  S. V. Breslavets, Fixed Points of Diffie-Hellman Permutations, Research Paper, Yulia's Dream Program, August 2025, <https://math.mit.edu/research/highschool/primes/materials/2025/YD/Breslavets.pdf>
-  W. Diffie and M. Hellman, New Directions in Cryptography, IEEE Trans. Info. Th. **22** (1976) 644-654.
-  P. Landrock, Power map permutations and the discrete log problem, Des. Codes Cryptogr. **77**, 2-3 (2015) 713–724.
-  J.S. Milne, Group Theory, <https://www.jmilne.org/math/CourseNotes/gt.html>
-  K.H. Rosen, Elementary Number Theory and Its Applications, Addison-Wesley Publishing Company, 1984.
-  P.W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, <https://arxiv.org/abs/quant-ph/9508027>

Bibliography

-  The On-Line Encyclopedia of Integer Sequences, <https://oeis.org/>
-  C. Pomerance, Elementary thoughts on discrete logarithms, *Algorithmic Number Theory, MSRI Publications* **44** (2008)
-  W. Trappe and L. Washington, Introduction to Cryptography with Coding Theory, Second Edition, Pearson, 2006.
-  Wolfram MathWorld, Cayley Graph, <https://mathworld.wolfram.com/CayleyGraph.html>
-  J. Cilleruelo, Sidon Sets in $\mathbb{N}^d$, <https://www.sciencedirect.com/science/article/pii/S0097316509001848>
-  R. Granger, T. Kleinjung, J. Zumbragel, Indiscreet logarithms in finite fields of small characteristic , <https://arxiv.org/abs/1604.03837v1>

Thank you for listening! Please ask any question you may have.