Fixed Points of Diffie-Hellman Permutations

Sophia V. Breslavets
Yulia's Dream Program
Saint Bernard School, Uncasville CT, USA
Mentor: Vasily A. Dolgushev

Abstract

In this paper, we explored the Discrete Logarithm Problem (DLP) through introducing Diffie-Hellman (DH) permutations. For every prime integer $p > 7$, we also introduced the concept of vulnerable exponents and this concept is motivated by the question of existence of fixed points of DH permutations. We proved a criterion of vulnerability for exponents relative to a given prime $p > 7$. We established a lower bound on the percentage of vulnerable exponents for every safe prime $p > 7$. For large safe primes, this bound is very close to 25%. This paper is accompanied by a GitHub repository with a SageMath script for working with DH permutations, their fixed points and vulnerable exponents. In this paper, we also listed selected open questions motivated by our exploration.

1 Introduction

There are several challenging problems related to primitive roots modulo a prime integer p. These problems include Artin's conjecture [1], [7], [11], exploration of the upper bound [2], [5] for the least primitive root modulo p, and the Discrete Logarithm Problem (DLP) [9], [10].

For a prime p and its primitive root b, we introduce a bijection

$$\tau_{p,b} : \{1, 2, \ldots, p-2\} \xrightarrow{\simeq} \{1, 2, \ldots, p-2\}$$

that plays the key role in the Diffie-Hellman key exchange protocol [3]. For this reason, we call $\tau_{p,b}$ the **Diffie-Hellman (DH) permutation** corresponding to the pair (p, b). The presence of fixed points of DH permutations is a serious weakness of the Diffie-Hellman protocol and, in this paper, we explore natural concepts related to DH permutations and their fixed points.

For a pair (p, b), a prime p and its primitive root b, we call integers $1 \leq x \leq p-2$ **exponents**. We say that an exponent x is **vulnerable relative to** p, if there exists at least one primitive root b modulo p such that $\tau_{p,b}(x) = x$.

For a prime p and an exponent $1 \leq x \leq p-2$, we denote by $\Omega_{x,p}$ the set of primitive roots modulo p such that $\tau_{p,b}(x) = x$. Elements of $\Omega_{x,p}$ are called **distinguished primitive roots** for the pair (x, p). Clearly, an exponent $1 \leq x \leq p-2$ is vulnerable relative to p if and only if the set $\Omega_{x,p}$ is non-empty.

For a prime p, we denote by $\mu(p)$ the maximum of the following set:

$$\{\mathrm{nfp}(\tau_{p,b}) \mid b \in \text{ the set of prim. roots mod } p\},$$

where $\mathrm{nfp}(\tau_{p,b})$ is the number of fixed points of $\tau_{p,b}$. We call primitive roots b modulo p for which $\mathrm{nfp}(\tau_{p,b}) = \mu(p)$ **vulnerable**.

Some information about $\mu(p)$ and vulnerable primitive roots for a given prime p can be extracted from computer experiments using [4]. In this paper, we present selected results of such computer experiments.

Theoretical results of this paper include the criterion of vulnerability of an exponent $1 \leq x \leq p-2$ for every prime $p \geq 11$ (see Theorem 2.3) and a lower bound for the number of vulnerable exponents relative to a safe prime $p \geq 11$ (see Theorem 3.5).

According to Theorem 2.3, an exponent x is vulnerable (relative to a prime $p \geq 11$) if and only if

$$\frac{p-1}{\gcd(x, p-1)} = \mathrm{ord}_p(x+1),$$

where gcd denotes the greatest common divisor and $\mathrm{ord}_p(x+1)$ is the order of the residues class of $(x+1)$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Theorem 2.3 also contains the formula for the number of distinguished primitive roots for a pair (x, p), where x is a vulnerable exponent relative to a prime p.

According to Theorem 3.5, the number of vulnerable exponents relative to a safe prime $p = 2q+1 \geq 11$ is greater or equal to

$$\frac{q-5}{2}.$$

In particular, for large safe primes p, the ratio of the number of vulnerable exponents to the total number of exponents is greater or equal to a number that is very close to $1/4$.

In our proofs, we mostly use tools of elementary number theory and a couple of facts from basic undergraduate algebra.

Organization of the paper. The introduction has two additional subsections. In Subsection 1.1, we establish the notational conventions and, in Subsection 1.2, we give a brief reminder of the Diffie-Hellman key exchange protocol. In Section 2, we introduce the DH permutations and develop terminology related to our work. We introduce the concept of vulnerable exponents, prove a criterion of vulnerability for an exponent $1 \leq x \leq p-2$, where p is a prime ≥ 11 (see Theorem 2.3). Given a vulnerable exponent x relative to a prime $p \geq 11$, we describe the set of distinguished primitive roots for a pair (x, p). In Section 2, we also present selected results of computer experiments. In Section 3, our focus is on safe primes. In this section, we prove an interesting corollary of Theorem 2.3 (see Corollary 3.2 and Question 4.4 motivated by this result) and establish a lower bound on the number of vulnerable exponents for every safe prime $p \geq 11$ (see Theorem 3.5). In Section 4, we present several open questions motivated by our exploration. Section 4 also features new integers sequences related to our work. Finally, in Appendix A, we collect useful information about GitHub repository [4] that accompanies this paper.

1.1 Notational conventions

For a finite set X, the notation $\#X$ is reserved for the size of X.

For a positive integer d, we denote by S_d the symmetric group on d letters, i.e. S_d is the group of bijections $\{1, 2, \ldots, d\} \xrightarrow{\simeq} \{1, 2, \ldots, d\}$. For a permutation τ, the notation $\mathrm{nfp}(\tau)$ is reserved for the number of fixed points of τ.

For a positive integer n and an integer a, we denote by $\mathrm{rem}(a, n)$ the (non-negative) remainder of division of a by n.

For an integer $n \geq 2$ and an integer a coprime to n, the notation $\mathrm{ord}_n(a)$ is reserved for the order of the residue class

$$a + n\mathbb{Z}$$

in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. For example, let p be prime and b be an integer with $p \nmid b$. Then b is a primitive root modulo p if and only if $\mathrm{ord}_p(b) = p-1$.

When a modulus n is clear from the context, $\overline{a}$ denotes the residue class of a modulo n.

The notation ϕ is reserved for Euler's ϕ-function (a.k.a. the totient function).

For positive integers d, m, we denote by $\mathrm{gcpd}(d, m)$ the greatest divisor of d that is coprime to m. For instance $\mathrm{gcpd}(180, 21) = 20$ and $\mathrm{gcpd}(21, 180) = 7$.

1.2 A reminder of the Diffie-Hellman key exchange protocol

The Diffie-Hellman key exchange protocol [3] allows two parties (say, Alice and Bob) to agree on the secrete encryption key using a public channel. This can be done in such way that, computationally, it is very hard for an eavesdropper who monitors the public channel to get the resulting secret encryption key.

Let p be a large prime[1] and b be a primitive root modulo p. The pair (p, b) is the **public part** of the key. Alice and Bob place this information in a public channel.

Alice chooses an exponent $1 < x_A < p-1$ and Bob chooses an exponent $1 < x_B < p-1$. The pair (x_A, x_B) is the **private part** of the key. Alice and Bob make sure that the pair (x_A, x_B) is not publicly available. Then Alice (resp. Bob) uses a public channel to send to Bob (resp. to Alice) the remainder $\mathrm{rem}(b^{x_A}, p)$ of division of b^{x_A} by p (resp. the remainder $\mathrm{rem}(b^{x_B}, p)$ of division of b^{x_B} by p).

After that, Alice can compute the residue class $\kappa_A := \left(\overline{b}^{x_B}\right)^{x_A}$ and Bob can compute the residue class $\kappa_B := \left(\overline{b}^{x_A}\right)^{x_B}$. Since

$$\left(\overline{b}^{x_B}\right)^{x_A} = \overline{b}^{x_A x_B} = \left(\overline{b}^{x_A}\right)^{x_B},$$

we have $\kappa_A = \kappa_B$.

Now Alice and Bob can use the remainder $\mathrm{rem}(b^{x_A x_B}, p)$ as their secrete encryption key. Note that, in practice, Alice and Bob use only a certain number of bits of the integer $\mathrm{rem}(b^{x_A x_B}, p)$ as their encryption key.

Suppose that Eve is monitoring the public channel that Alice and Bob use for their communication. If Eve wants to find x_A, then she needs to solve the congruence

$$b^{x_A} \equiv y_A \mod p, \tag{1}$$

where $y_A := \mathrm{rem}(b^{x_A}, p)$. This is known as the Discrete Logarithm Problem (DLP) for the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. The brute force approach of solving (1) may be time consuming.

For example, using SageMath, on a 2025 MacBook Air with the processor Apple M4 and the Random Access Memory (RAM) 24GB, it takes > 4.5 minutes to solve the congruence

$$3,405,601,951 \equiv 350,552,080^x \mod p$$

for the prime $p = 5,000,929,201$. We expect that, for the prime $p := 70,000,700,928,371$ and its primitive root $b := 57,385,944,440,573$ solving a similar congruence via the brute force search on the same device (using SageMath) may take over 170 days!

There are several tools for tackling the DLP and some of these tools are described in [10]. For example, according to [10, Section 2], there are ways to tackle the DLP for the group $(\mathbb{Z}/p\mathbb{Z})^\times$ if $p-1$ is not of the form $2q$, where q is prime. Primes of the form $2q+1$ (with q being prime) are called **safe primes**. For this reason, in Section 3 of this paper, we specifically focus on DH permutations for safe primes.

[1] In practice, we are interested in primes with at least 100 decimal digits.

Remark 1.1 Neither the author nor the mentor knew about the Brizolis conjecture [6, Section F9], [8], [9]. The DH permutation $\tau_{p,b}$ can be naturally extended to a bijection $\tau_{p,b} : \mathbb{Z}/(p-1)\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/(p-1)\mathbb{Z}$. The permutations introduced in [8] may be also identified with bijections $\mathbb{Z}/(p-1)\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/(p-1)\mathbb{Z}$. Both these bijections and the DH permutations $\tau_{p,b}$ are a part of a larger family of bijections $\tau_{p,b,\gamma} : \mathbb{Z}/(p-1)\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/(p-1)\mathbb{Z}$ defined by the formula

$$\tau_{p,b,\gamma}(\alpha) := \tau_{p,b}(\alpha) + \gamma, \qquad \alpha, \gamma \in \mathbb{Z}/(p-1)\mathbb{Z}\,.$$

It makes sense to explore this larger family of permutations parameterized by a prime p, a primitive root b modulo p and a residue class $\gamma \in \mathbb{Z}/(p-1)\mathbb{Z}$.

Acknowledgments. We are thankful to Pavel Etingof, Slava Gerovitch, and Dmytro Matvieievskyi for organizing the program "Yulia's Dream" and giving us an opportunity to connect with like-minded individuals. We are thankful to Pavel Etingof, Yury Grabovsky, Darij Grinberg, Borys Holikov, Yelena Mandelshtam, Vadym Pashkovskyi and Alex Youcis for their stimulating questions and suggestions. We are thankful to our families for their support and providing us with the conditions to work on this project.

2 Diffie-Hellman permutations and vulnerable exponents

Let p be a prime integer ≥ 11 and b be a primitive root modulo p. Since the residue class of b generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$, the assignment

$$x \mapsto \mathrm{rem}(b^x, p)$$

defines a bijection from the set $\{1, 2, \ldots, p-2\}$ to the set $\{2, 3, \ldots, p-1\}$.

Thus the formula

$$\tau_{p,b}(x) := \mathrm{rem}(b^x, p) - 1 \tag{2}$$

defines a bijection $\{1, 2, \ldots, p-2\} \xrightarrow{\simeq} \{1, 2, \ldots, p-2\}$ and we call this bijection the **Diffie-Hellman permutation** corresponding to the pair (p, b). In this set-up, an integer $x \in \{1, 2, \ldots, p-2\}$ is called an **exponent**.

The presence of fixed points of the permutation $\tau_{p,b}$ is a serious weakness of the Diffie-Hellman protocol. Indeed, if Alice's exponent x_A is a fixed point of $\tau_{p,b}$, then an eavesdropper (say, Eve) can easily get $x_A = \mathrm{rem}(b^{x_A}, p) - 1$ and hence Eve can calculate $(\overline{b}^{x_B})^{x_A} = \overline{b}^{x_A x_B}$. Similarly, if Bob's exponent x_B is a fixed point of $\tau_{p,b}$, then Eve can easily get $x_B = \mathrm{rem}(b^{x_B}, p) - 1$ and hence Eve can calculate $(\overline{b}^{x_A})^{x_B} = \overline{b}^{x_A x_B}$.

Thus, if Alice or Bob accidentally chooses a fixed point of $\tau_{p,b}$ as their exponent, then they essentially place the private part of their key into the public channel.

For a prime p, we set

$$\mu(p) := \max(\{\mathrm{nfp}(\tau_{p,b}) \mid b \in \text{ the set of prim. roots mod } p\}), \tag{3}$$

where $\mathrm{nfp}(\tau_{p,b})$ is the number of fixed points of the permutation $\tau_{p,b}$. Let us also denote by $\theta(p)$ the percentage of primitive roots b for which $\mathrm{nfp}(\tau_{p,b}) = \mu(p)$.

Using [4], one can compute values of μ and θ for various prime integers. The table below contains this information for selected primes:

prime p	$100 \cdot \mu(p)/(p-2)$	$\theta(p)$
103	4.95%	3.13%
911	0.55%	0.35%
1009	0.4%	1.04%
1823	0.27%	0.33%
3343	0.15%	0.36%
5557	0.13%	0.05%

The second column in the table features the values $100 \cdot \mu(p)/(p-2)$ for the specified prime integers p and the third column features the values of θ.

Let b be a primitive root modulo p. If the number of fixed points of the permutation $\tau_{p,b}$ equals $\mu(p)$ (i.e. the worst case scenario), then we call b a **vulnerable primitive root**. The following table for primes $11 \leq p \leq 107$ and their vulnerable primitive roots is produced using [4]:

prime p	vulnerable primitive roots
11	2, 6
13	2
17	7, 10, 11, 12
19	3
23	19
29	2, 8
31	13, 21
37	22
41	26
43	20, 28
47	5, 22, 23, 44
53	2, 8, 12, 18, 19, 34, 41, 51

prime p	vulnerable primitive roots
59	11
61	2
67	31, 51
71	7, 21, 22, 28, 59, 65
73	14
79	6, 39
83	15
89	27, 41
97	59, 87
101	2
103	77
107	2, 91

Further related results of [4] are shown in Figures 1 and 2. Figure 1 shows the plot of the values

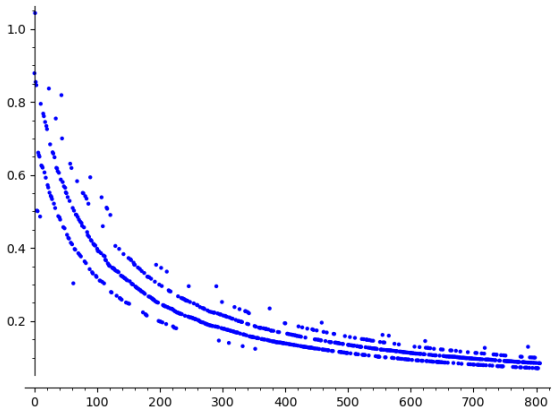

Figure 1: Percentages of fixed points for primes $571 \leq p \leq 7109$ in the worst case scenario

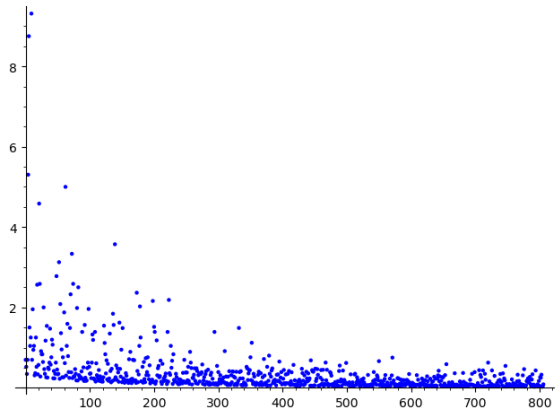

Figure 2: Percentages of vulnerable primitive roots for primes $571 \leq p \leq 7109$

$100 \cdot \mu(p)/(p-2)$ for all primes $571 \leq p \leq 7109$. Figure 2 shows the percentages of vulnerable primitive roots for primes $571 \leq p \leq 7109$. (There are 807 primes in this range.)

Definition 2.1 *Let p be a prime ≥ 11. We say that an exponent $x \in \{1, 2, \ldots, p-2\}$ is **vulnerable** relative to p if there exists a primitive root b modulo p such that*

$$\tau_{p,b}(x) = x.$$

Note that $x = 1$ is a vulnerable exponent relative to p if and only if 2 is a primitive root modulo p.

For an integer $1 \le x \le p-2$, we denote by $\Omega_{x,p}$ the set of all primitive roots $1 < b \le p-1$ such that $\tau_{p,b}(x) = x$. We call elements of $\Omega_{x,p}$ **distinguished primitive roots** for the pair (x, p). Clearly a positive integer $1 \le x \le p-2$ is a vulnerable exponent relative to p if and only if $\Omega_{x,p} \neq \emptyset$. In the next subsection, we will give an explicit description of the set $\Omega_{x,p}$ for every prime $p \ge 11$ and for every vulnerable exponent x relative to p.

Example 2.2 The integer $p := 9241$ is prime and there are 1920 primitive roots modulo p. According to [4], 777 exponents out of 9239 are vulnerable. The table below shows the distinguished primitive roots for selected pairs (x, p) (with x being vulnerable and $p = 9241$):

exponent x	disting. prim. roots for the pair $(x, 9241)$
230	2754, 4078, 1314, 7150, 6487, 5163, 7927, 2091
388	1046, 247, 8195, 8994
430	1873, 4270, 3370, 7594, 7368, 4971, 5871, 1647
679	303, 2869, 7671, 7764, 959, 7830
1250	3498, 763, 3935, 2478, 5743, 8478, 5306, 6763
1310	658, 6276, 7139, 4444, 8583, 2965, 2102, 4797
1561	6918, 2647, 6734, 5876, 5163, 4657
1841	7969, 4242, 3202, 4578, 5743, 4185
2093	4336, 5068, 3673, 4097, 4696, 3170
2116	2718, 8805, 6523, 436
2317	455, 8639, 1223, 8182, 2965, 1053

We have

$$\{\#\Omega_{x,9241} \mid 1 \le x \le 9239\} = \{1, 2, 4, 6, 8, 10, 12, 16, 20, 24, 40\}$$

and $x := 3608$ is the only exponent that has 40 distinguished primitive roots. Here is the list of the first 12 distinguished primitive roots for the pair $(3608, 9241)$:

$$129,\ 206,\ 217,\ 470,\ 537,\ 857,\ 1082,\ 1404,\ 1418,\ 1482,\ 2107,\ 2271.$$

2.1 A criterion of vulnerability

The goal of this section is to prove the following statement:

Theorem 2.3 *Let p be a prime ≥ 11. An integer $1 \le x \le p-2$ is a vulnerable exponent (relative to p) if and only if*

$$\mathrm{ord}_p(x+1) = \frac{p-1}{\gcd(x, p-1)}. \tag{4}$$

If x is a vulnerable exponent relative to p, $d := \gcd(x, p-1)$, $m := (p-1)/d$ and d_1 is the greatest divisor of d that is coprime to m, then the number of primitive roots $1 < b \le p-1$ such that $\tau_{p,b}(x) = x$ equals $\phi(d_1)d/d_1$.

Proof. Condition (4) is clearly necessary. Indeed, let β be a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ for which

$$\beta^x = (x+1) + p\mathbb{Z}.$$

Since the order of β^x in $(\mathbb{Z}/p\mathbb{Z})^\times$ is $(p-1)/\gcd(x, p-1)$, condition (4) follows.

Let us now assume that x satisfies equation (4) and let us choose a generator β_0 of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Since $2 \leq x+1 \leq p-1$ and β_0 is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, there exists a unique exponent $1 \leq t \leq p-2$ such that

$$\beta_0^t = (x+1) + p\mathbb{Z}. \tag{5}$$

Condition (4) implies that the order of β_0^t in $(\mathbb{Z}/p\mathbb{Z})^\times$ is $(p-1)/\gcd(x, p-1)$. Hence

$$\frac{p-1}{\gcd(t, p-1)} = \frac{p-1}{\gcd(x, p-1)},$$

or equivalently,

$$\gcd(t, p-1) = \gcd(x, p-1).$$

We set

$$d := \gcd(x, p-1), \quad m := (p-1)/d, \quad d_1 := \mathrm{gcpd}(d, m), \quad d_2 := d/d_1\,.$$

Since β_0 is a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$,

$$\{\beta_0^k \mid 1 \leq k \leq p-2,\ \gcd(k, p-1) = 1\}$$

is the set of all generators of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Recall that $\Omega_{x,p}$ is the set of all primitive roots b modulo p such that $\tau_{p,b}(x) = x$. Since the set $\Omega_{x,p}$ is in bijection with the set of generators β of $(\mathbb{Z}/p\mathbb{Z})^\times$ for which

$$\beta^x = (x+1) + p\mathbb{Z}$$

and $(x+1) + p\mathbb{Z} = \beta_0^t$, the above observation about generators of $(\mathbb{Z}/p\mathbb{Z})^\times$ implies that the set $\Omega_{x,p}$ is in bijection with the following set:

$$\Xi_{x,p,\beta_0} := \{k \in \{1, 2, \ldots, p-2\} \mid \gcd(k, p-1) = 1,\ \ \beta_0^{kx} = \beta_0^t\}.$$

The remainder of the proof goes as follows. First, we will show that there exists a unique integer $1 \leq k_0 \leq m-1$ such that

$$\beta_0^{k_0 x} = \beta_0^t\,. \tag{6}$$

Second, we will use the integer k_0 to construct a bijection from the set

$$(\mathbb{Z}/d_1\mathbb{Z})^\times \times \{0, 1, \ldots, d_2 - 1\}$$

to the set Ξ_{x,p,β_0}.

By constructing such a bijection, we will achieve two goals. First, we will prove the "if" implication of the first statement of the theorem. Second, we will prove the second statement about the number of distinguished primitive roots for a pair (x, p), where x is a vulnerable exponent relative to p.

Since $\mathrm{ord}(\beta_0) = p-1$, the equation

$$\beta_0^{kx} = \beta_0^t\,. \tag{7}$$

is equivalent to

$$kx \equiv t \mod (p-1). \tag{8}$$

The congruence is equivalent to $kx - t = (p-1)r,\ r \in \mathbb{Z}$. Factoring out the greatest common divisor:

$$t = t_1 d, \quad x = x_1 d,$$

we get

$$(kx_1 - t_1)d = mrd \iff kx_1 - t_1 = mr.$$

Or going back to congruence form,

$$kx_1 \equiv t_1 \mod m \iff \overline{k}\overline{x_1} = \overline{t_1} \in (\mathbb{Z}/m\mathbb{Z})^\times .$$

Since $\overline{x}_1$ is a unit in the ring $\mathbb{Z}/m\mathbb{Z}$, there is only one integer $0 \leq k_0 < m$ that is a solution of the congruence in (8). Since $\overline{t}_1$ is also a unit in $\mathbb{Z}/m\mathbb{Z}$, we can conclude that

$$\gcd(k_0, m) = 1. \tag{9}$$

In particular, $k_0 \geq 1$.

We can also conclude that the solution set of the congruence in (8) is $\{k_0 + ms \mid s \in \mathbb{Z}\}$. Hence

$$\Xi_{x,p,\beta_0} = \{k_0 + ms \mid s \in \mathbb{Z},\ \gcd(k_0 + ms, p-1) = 1,\ 1 \leq k_0 + ms \leq (p-2)\}.$$

Note that

$$\gcd(k_0 + ms, p-1) = 1 \iff \gcd(k_0 + ms, d_1) = 1,$$

where d_1 is the greatest divisor of d that is coprime to m. Therefore

$$\Xi_{x,p,\beta_0} = \{k_0 + ms \mid s \in \mathbb{Z},\ \gcd(k_0 + ms, d_1) = 1,\ 1 \leq k_0 + ms \leq (p-2)\}. \tag{10}$$

Let us choose $\nu \in (\mathbb{Z}/d_1\mathbb{Z})^\times$ and consider the equation

$$\overline{k_0} + \overline{m}\,\overline{s} = \nu\,. \tag{11}$$

Since m is coprime to d_1, there is a unique integer $s_\nu \in \{0, 1, ..., d_1 - 1\}$ such that $\overline{k_0} + \overline{m}\,\overline{s}_\nu = \nu$. Moreover, the set of integers s satisfying (11) is

$$\{s_\nu + d_1 l \mid l \in \mathbb{Z}\}.$$

Combining this observation with (10) and the implications

$$k_0 + ms < p - 1 = md_1d_2 \iff s \leq (d_1d_2 - 1) \iff l \leq d_2 - 1,$$

we get

$$\Xi_{x,p,\beta_0} = \{k_0 + m(s_\nu + d_1 l) \mid \nu \in (\mathbb{Z}/m\mathbb{Z})^\times,\ 1 \leq l \leq d_2 - 1\}. \tag{12}$$

To complete the proof, we consider the natural map

$$\psi : (\mathbb{Z}/d_1\mathbb{Z})^\times \times \{0, 1, ..., d_2 - 1\} \to \Xi_{x,p,\beta_0}$$

defined by the formula:

$$\psi(\nu, l) := k_0 + m(s_\nu + ld_1).$$

It is clear from (12) that the map ψ is surjective. To prove that ψ is injective, we consider $(\nu_1, l_1), (\nu_2, l_2) \in (\mathbb{Z}/d_1\mathbb{Z})^\times \times \{0, 1, \ldots, d_2 - 1\}$ such that $\psi(\nu_1, l_1) = \psi(\nu_2, l_2)$. Then

$$\begin{aligned} k_0 + m(s_{\nu_1} + l_1d_1) &= k_0 + m(s_{\nu_2} + l_2d_1) \\ \iff m(s_{\nu_1} + l_1d_1) &= m(s_{\nu_2} + l_2d_1). \end{aligned} \tag{13}$$

Passing to residue classes modulo d_1, we get

$$\overline{m}\,\overline{s_{\nu_1}} = \overline{m}\,\overline{s_{\nu_2}}\,.$$

Due to equation (11), $\nu_1 = \nu_2$. Hence $s_{\nu_1} = s_{\nu_2}$ and substituting this into (13), we get $l_1 = l_2$. So

$$\psi(\nu_1, l_1) = \psi(\nu_2, l_2) \iff (\nu_1, l_1) = (\nu_2, l_2).$$

Thus we established the injectivity and the theorem is proved. □

3 Vulnerable exponents for safe primes

A prime integer q is called a **Germain prime** if the integer $2q+1$ is also prime. Primes of the form $2q+1$ (with q being prime) are called **safe**.

The goal of this section is to establish a lower bound on the number of vulnerable exponents for every safe prime $p \geq 11$.

First, let us prove that, under our assumptions, the integer q is never a vulnerable exponent:

Proposition 3.1 *If q is a prime ≥ 5 and $p := 2q+1$ is also prime, then q is not a vulnerable exponent relative to p.*

Proof. Since $\gcd(q, 2q) = q$, the integer q is a vulnerable exponent relative to p if and only if

$$\mathrm{ord}(\overline{q+1}) = 2. \tag{14}$$

We know that $\overline{-1}$ is the only element of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order 2. Thus (14) implies that $q+1 \equiv -1 \mod p$. Hence $q+1 = 2q-1$ which contradicts our assumption $q \geq 5$. □

Let us now use Theorem 2.3 and Proposition 3.1 to prove the following property of vulnerable exponents of safe primes:

Corollary 3.2 *Let p be a safe prime ≥ 11. If x is a vulnerable exponent relative to p, then there is a unique primitive root b_x modulo p such that $\tau_{p,b_x}(x) = x$.*

Proof. Let x be a vulnerable exponent relative to p, $d := \gcd(x, 2q)$, $m = 2q/d$ and $d_1 = \mathrm{gcpd}(d, m)$. Our goal is to prove that $\phi(d_1)d/d_1 = 1$.

Since $1 \leq x < 2q$ and $x \neq q$, d either equals 1 or 2. In the first case ($d = 1$), $d_1 = 1$ and $\phi(d_1)d/d_1 = 1$. In the second case ($d = 2$), we have $m = q$, $d_1 = 2$ and $d/d_1 = 2$. Thus $\phi(d_1)d/d_1 = \phi(2) = 1$.

Since $\phi(d_1)d/d_1 = 1$, the second statement in Theorem 2.3 implies that, modulo p, there is only one primitive root b_x such that $\tau_{p,b_x}(x) = x$. □

Our next goal is to prove two auxiliary statements that will be used in establishing a lower bound for the number of vulnerable exponents for every safe prime $p \geq 11$.

Claim 3.3 *An element $\gamma \in (\mathbb{Z}/p\mathbb{Z})^\times$ has order q if and only if*

$$\gamma = \overline{u}^2$$

for an integer $2 \leq u \leq p-2$. If $\mathrm{ord}(\gamma) = q$, then the equation $\alpha^2 = \gamma$ has exactly two solutions in $(\mathbb{Z}/p\mathbb{Z})^\times$. More precisely, if $\overline{u}^2 = \gamma$, then $\alpha = \overline{p-u}$ is the second solution of $\alpha^2 = \gamma$.

Proof. To prove the direct implication, we choose a generator β of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $\gamma = \beta^t$ for exactly one integer $0 \leq t \leq p-2$. Since $\mathrm{ord}(\gamma) = q$, we have:

$$q = \mathrm{ord}(\beta^t) = \frac{2q}{\gcd(t, 2q)}\,.$$

Thus, $\gcd(t, 2q) = 2$, which means that t is even. If $t = 2t_1$, then

$$\gamma = \beta^{2t_1} = (\beta^{t_1})^2 = \overline{u}^2\,.$$

It is obvious that $u \notin \{0, 1, p-1\}$. So we conclude that $2 \leq u \leq p-2$. Now, let us prove the opposite implication. We know that $\gamma = \overline{u}^2$ for an integer $2 \leq u \leq p-2$. Due to Lagrange's Theorem, $\mathrm{ord}(\overline{u}) \in \{1, 2, q, 2q\}$. However, the order of $\overline{u}$ cannot be 2, because than $\overline{u}^2 = 1$ and $\overline{u} = \overline{1}$ or $\overline{u} = \overline{p-1}$, but $2 \leq u \leq p-2$. Then, $\mathrm{ord}(\overline{u}) = q$ or $\mathrm{ord}(\overline{u}) = 2q$. If the order of $\overline{u}$ is $2q$, $\mathrm{ord}(\overline{u}^2) = \dfrac{2q}{\gcd(2, 2q)} = q$, because q is odd and $\gcd(2, 2q) = 2$. If $\mathrm{ord}(\overline{u}) = q$, then $\mathrm{ord}(\overline{u}^2) = q$, because q is odd. Hence, we proved that, if $\gamma = \overline{u}^2$ for an integer $2 \leq u \leq p-2$, the element $\gamma := \overline{u}^2$ has order q.

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, the equation $\alpha^2 = \gamma$ cannot have more than two solutions. Thus, if $\overline{u}^2 = \gamma$, then $\{\overline{u}, \overline{p-u}\}$ is clearly the solution set of $\alpha^2 = \gamma$. It remains to prove that $\overline{u} \neq \overline{p-u}$.

We may assume, without loss of generality, that $2 \leq u \leq p-2$ (recall that $\mathrm{ord}(\gamma) = q$). Then $2 \leq p-u \leq p-2$.

Since p is odd, $u \neq p-u$. Combining this observation with $u, p-u \in \{0, 1, \ldots, p-1\}$, we conclude that $\overline{u} \neq \overline{p-u}$. □

Claim 3.4 *If $q \in \mathbb{Z}_{\geq 5}$, $p = 2q+1$ and $m_0 = (q-1)/2$, then q is the only integer that belongs to the interval $(\sqrt{m_0 p}, \sqrt{(m_0+1)p})$.*

Proof. The statement follows from the inequalities

$$q - 1 < \sqrt{m_0 p} < q < \sqrt{(m_0+1)p}) < q + 1. \tag{15}$$

Let us prove the second inequality and the fourth inequality in (15).

Since $q^2 - q/2 - 1/2 < q^2$ and $q^2 - q/2 - 1/2 = (q + 1/2)(q-1)$, we have

$$\sqrt{m_0 p} = \sqrt{(q+1/2)(q-1)} < q.$$

Since $\sqrt{(m_0+1)p)} = \sqrt{(q+1)(q+1/2)}$, the inequality $\sqrt{(m_0+1)p)} < q+1$ follows easily from the inequality $(q+1/2)(q+1) < (q+1)^2$.

We leave the proofs of the remaining two inequalities to the reader. □

We can now formulate and prove the second result of this research paper:

Theorem 3.5 *Let $p = 2q+1$ be a safe prime ≥ 11. Then the ratio of the number of vulnerable exponents to the total number of exponents (relative to p) is greater or equal to*

$$\frac{q-5}{4q-2}. \tag{16}$$

For $p = 11$, 5 out of 9 exponents are vulnerable.

Proof. Let us denote by X the set of all exponents relative to $p = 2q+1$, i.e. $X := \{1, 2, ..., 2q-1\}$.

Since $\{2, q, 2q\}$ is the set of all divisors t of $2q$ with $t > 1$, we have

$$X = X_2 \sqcup X_q \sqcup X_{2q}\,,$$

where $X_t = \left\{\, x \in X \mid \dfrac{2q}{\gcd(x, 2q)} = t \,\right\}$.

It is easy to see that

$$X_2 = \{q\}, \qquad X_q = \{2, 4, ..., 2q-2\}, \qquad X_{2q} = \{1, 3, ..., 2q-1\} - \{q\}. \tag{17}$$

Since q is not a vulnerable exponent (see Proposition 3.1), we only have to look at vulnerable exponents in X_q and X_{2q}.

Let us denote the set of vulnerable exponents in X_q (resp. X_{2q}) as X_q^{vul} (resp. as X_{2q}^{vul}).

To prove the first statement of the theorem, we will show that

$$\#X_q^{vul} \geq \frac{q-3}{4}, \qquad \#X_{2q}^{vul} \geq \#X_q^{vul} - 1. \tag{18}$$

To prove the first inequality in (18), we introduce two auxiliary sets:

$$Y = \{y \mid y \text{ is odd},\ 3 \leq y \leq 2q-1,\ \mathrm{ord}(\overline{y}) = q\}, \tag{19}$$

$$U := \{2 \leq u \leq q \mid \mathrm{rem}(u^2, p) \text{ is odd}\}. \tag{20}$$

It is easy to see that the assignment $x \mapsto y := x + 1$ defines a bijection from X_q^{vul} to Y.

Due to Claim 3.3, the assignment

$$u \mapsto \mathrm{rem}(u^2, p)$$

defines a bijection from U to Y. Thus $\#U = \#X_q^{vul}$ and our goal is to prove that

$$\#U \geq \frac{q-3}{4}. \tag{21}$$

Let $m_0 := (q-1)/2$. Due to Claim 3.4, every integer $2 \leq u \leq q$ belongs to exactly one interval $(\sqrt{mp}, \sqrt{(m+1)p})$, where m is an integer

$$0 \leq m \leq m_0\,.$$

Moreover, $u \in U \cap (\sqrt{mp}, \sqrt{(m+1)p})$ if and only if u is odd and m is even or u is even and m is odd.

Let $E_m := (\sqrt{mp}, \sqrt{(m+1)p}) \cap 2\mathbb{Z}$ and $I_m := (\sqrt{mp}, \sqrt{(m+1)p}) \cap (2\mathbb{Z}+1)$.

Combining the above observation with $1 \notin U$, we conclude that:

$$\#U \ = \ (\#I_0 - 1) \ + \sum_{2 \leq m \leq m_0}^{m \text{ is even}} \#I_m \ + \sum_{1 \leq m \leq m_0}^{m \text{ is odd}} \#E_m\,.$$

Since $(q-1)$ is even, there are exactly $(q-1)/2$ odd integers in the range $2 \leq u \leq q$. Hence

$$\#U \ = \ \frac{q-1}{2} \ + \sum_{0 < m \leq m_0}^{m \text{ is odd}} (\#E_m - \#I_m). \tag{22}$$

For every $1 \leq m \leq m_0$, $\#E_m - \#I_m \geq -1$. It is also easy to see that the number of odd integers $1 \leq m \leq m_0$ is $\leq \frac{m_0+1}{2} = \frac{q+1}{4}$. Combining these observations with (22), we arrive at the desired inequality:

$$\#U \geq \frac{q-1}{2} - \frac{q+1}{4} = \frac{q-3}{4}.$$

Since we proved the inequality in (21), the first inequality in (18) is also proved.

To prove the second inequality in (18), we notice that

$$\{x+1 \mid x \in X_{2q}\} = \{s \in 2\mathbb{Z} \mid 2 \leq s \leq p-1,\ s \neq q+1\}.$$

Thus X_{2q}^{vul} is in bijection with the set $S := \{s \in 2\mathbb{Z} \mid 2 \le s \le p-1,\ s \neq q+1,\ \mathrm{ord}(\overline{s}) = 2q\}$.

Since $\mathrm{ord}(\overline{p-1}) = 2 \neq 2q$, we conclude that

$$S = \{s \in 2\mathbb{Z} \mid 2 \le s \le p-3,\ s \neq q+1,\ \mathrm{ord}(\overline{s}) = 2q\}. \tag{23}$$

We also claim that the assignment $y \mapsto p - y$ defines a bijection from the set Y (see (19)) to the set

$$\tilde{S} := \{s \in 2\mathbb{Z} \mid 2 \le s \le p-3,\ \mathrm{ord}(\overline{s}) = 2q\}. \tag{24}$$

Indeed, since $\overline{y}^q = \overline{1}$ and q is odd, $(-\overline{y})^q = -\overline{1} \neq \overline{1}$. Since $-\overline{y} \neq \overline{1}$, $(-\overline{y})^2 = \overline{y}^2 \neq \overline{1}$ and q is prime, we conclude that $\mathrm{ord}(-\overline{y}) = 2q$.

Vice versa, let $s \in \tilde{S}$. Since $\overline{s}^q \neq \overline{1}$ and $(\overline{s}^q)^2 = \overline{1}$, we conclude that $\overline{s}^q = -\overline{1}$. Hence $(-\overline{s})^q = \overline{1}$. Since $-\overline{s} \neq \overline{1}$ and q is prime, we conclude that $\mathrm{ord}(-\overline{s}) = q$.

We proved that the assignment $y \mapsto s := p - y$ defines a bijection from the set Y to the set $\tilde{S}$.

It is clear that $S \subset \tilde{S}$ and

$$\#S = \begin{cases} \#\tilde{S} & \text{if } \mathrm{ord}(\overline{q+1}) \neq 2q \\ \#\tilde{S} - 1 & \text{if } \mathrm{ord}(\overline{q+1}) = 2q. \end{cases} \tag{25}$$

Combining the above arguments, we conclude that

$$\#X_{2q}^{vul} = \#S \ge \#\tilde{S} - 1 = \#Y - 1 = \#X_q^{vul} - 1.$$

Thus the second inequality in (18) is also proved.

Since the number of vulnerable exponents relative to p equals $\#X_q^{vul} + \#X_{2q}^{vul}$, the inequalities in (18) imply that the number of vulnerable exponents relative to p is greater or equal to

$$\frac{q-3}{4} + \frac{q-3}{4} - 1 = \frac{q-5}{2}.$$

The first statement of the theorem follows.

The statement about $p = 11$ is proved by a direct calculation or using [4]. □

Remark 3.6 Note that, when the Germain prime q is large, the ratio in (16) is close to $1/4$. Please see Question 4.3 in the next section.

Remark 3.7 There are examples of safe primes $p = 2q + 1$ for which $q + 1$ is a primitive root modulo p. Thus the set S in the proof of Theorem 3.5 may be a proper subset of $\tilde{S}$ (see (23) and (24)). In fact, using [4], one can show that the number of safe primes $11 \le p = 2q+1 \le 50,000,747$ for which $q+1$ is a primitive root equals $62,323$. In other words, approximately, 0.499% of safe primes in the range $11 \le p \le 50,000,747$ satisfy this property.

The following statement is an obvious consequence of Theorem 3.5:

Corollary 3.8 *For every safe prime $p \ge 11$, there exists a primitive root b modulo p such that the DH permutation $\tau_{p,b}$ has a fixed point.* □

4 Open questions

Corollary 3.8 motivates the following question:

Question 4.1 *Let p be a prime ≥ 11. Is this true that p has a primitive root b such that the DH permutation $\tau_{p,b}$ has a fixed point?*

We encourage the reader to compare this question to the Brizolis conjecture [6, Section F9], [9].

Clearly, if every prime $p \geq 11$ has a vulnerable exponent, then the answer to Question 4.1 is "yes".

Question 4.2 *Let p be a prime ≥ 11. Is this true that the percentage of vulnerable exponents relative to p is $> 5\%$?*

Our computer experiments [4] showed that, for all primes $11 \leq p < 180181$, the percentage of vulnerable exponents is $> 7\%$. However, for $p = 180181$, this number is 6.99%. Due to these results every prime $11 \leq p \leq 180181$ has a primitive root b such that the DH permutation $\tau_{p,b}$ has a fixed point.

According to our computer experiments [4], safe primes typically have a large percentage of vulnerable exponents. For example, for every safe primes $59 \leq p \leq 1,276,103$, the percentage of vulnerable exponents relative to p is $> 42\%$.

Question 4.3 *Is this true that for every safe prime $p \geq 59$, the percentage of vulnerable exponents is $> 42\%$?*

Figure 3 shows the plot of the percentages of vulnerable exponents for all safe primes $59 \leq p \leq 165,059$. (There are 997 safe primes in this range.)

Let p be a large safe prime. Due to Theorem 3.5, roughly a quarter of exponents relative to p or more[2] are vulnerable. Due to Corollary 3.2, for every vulnerable exponent x (relative to p), there is a unique primitive root b_x modulo p such that

$$(b_x)^x \equiv (x+1) \mod p. \tag{26}$$

The description of the set $\Omega_{x,p}$ of distinguished primitive roots for a pair (x,p) presented in the proof of Theorem 2.3 shows that, given a vulnerable exponent x, one can find the primitive root b_x relatively fast. However, given the primitive root $b := b_x$, solving the congruence $b^x \equiv (x+1) \mod p$ is probably very challenging.

Question 4.4 *Let p be a safe prime and σ be the function from the set of vulnerable primitive roots (relative to p) to the set of primitive roots modulo p given by the formula*

$$\sigma(x) := b_x,$$

where b_x is the unique primitive root modulo p for which equation (26) holds. Is σ a pre-image resistant function?

The ability to factor large integers fast does not seem to help finding the pre-image of this function. So, if σ is indeed pre-image resistant, it may be very useful in cryptographic applications.

[2] According to Figure 3, the situation may be even more encouraging.

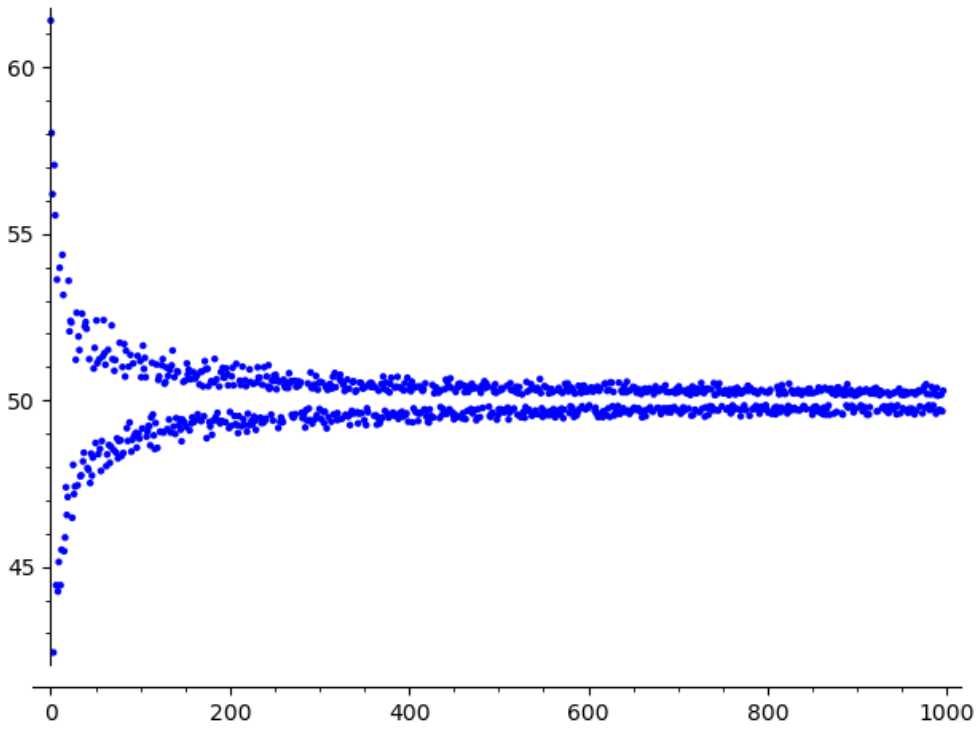

Figure 3: Percentages of vulnerable exponents for 997 safe primes $59 \leq p \leq 165,059$

4.1 Selected integer sequences

Ideas presented in this paper allow us to generate numerous integer sequences and, at the time of writing, according to [13], all these sequences[3] are new:

- Here is the sequence of numbers $\mathrm{nfp}(\tau_{p,g_p})$ for primes $7 \leq p \leq 107$:

  $$0,\ 2,\ 3,\ 0,\ 3,\ 0,\ 2,\ 0,\ 2,\ 0,\ 0,\ 2,\ 2,\ 2,\ 2,\ 2,\ 2,\ 2,\ 1,\ 3,\ 0,\ 0,\ 3,\ 0,\ 4.$$

  For comparison, here is the sequence of numbers $\mathrm{nfp}(\tau_{p,g_p})$ for primes $55,579 \leq p \leq 55,813$:

  $$3,\ 2,\ 3,\ 0,\ 2,\ 2,\ 1,\ 0,\ 2,\ 3,\ 0,\ 2,\ 1,\ 0,\ 4,\ 1,\ 1,\ 3,\ 0,\ 4,\ 4,\ 3,\ 1,\ 0,\ 2,\ 2.$$

- There are 1228 primes $3 \leq p < 10,000$ and, for 286 primes in this range, the permutation τ_{p,g_p} has no fixed points. Here is the list of the first 12 primes that satisfy this property:

  $$7,\ 17,\ 23,\ 31,\ 41,\ 43,\ 89,\ 97,\ 103,\ 127,\ 137,\ 167.$$

- Recall that, for a prime p, $\mu(p)$ denotes the number of fixed points of a DH permutation for p in the worst case scenario (see (3)). Here is the sequence of values of μ for primes $7 \leq p \leq 107$:

  $$0,\ 2,\ 3,\ 2,\ 4,\ 2,\ 2,\ 3,\ 3,\ 2,\ 2,\ 2,\ 2,\ 4,\ 2,\ 3,\ 2,\ 3,\ 2,\ 4,\ 3,\ 3,\ 3,\ 5,\ 4.$$

  For comparison, here is the sequence of values of μ for the primes $10559 \leq p \leq 10789$:

  $$5,\ 6,\ 7,\ 7,\ 7,\ 7,\ 6,\ 6,\ 5,\ 7,\ 6,\ 7,\ 5,\ 6,\ 7,\ 7,\ 6,\ 6,\ 6,\ 6,\ 6,\ 5,\ 5,\ 6,\ 6,\ 7.$$

[3]Recall that g_p is the smallest primitive root modulo a prime p.

- Here is the list of numbers of vulnerable primitive roots for all primes $1009 \leq p \leq 1171$:

$$3,\ 7,\ 4,\ 1,\ 1,\ 5,\ 8,\ 2,\ 8,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 1,\ 10,\ 1,\ 9,\ 1,\ 1,\ 1,\ 1,\ 2,\ 4.$$

- Here is the list of orders of the DH permutations τ_{p,g_p} for all primes $7 \leq p \leq 107$:

$$6,\ 10,\ 6,\ 26,\ 8,\ 84,\ 46,\ 182,\ 340,\ 60,\ 310,\ 204,\ 4950,\ 240,\ 126,814,\ 150,\ 828,$$
$$2820,\ 3068,\ 992,\ 27336,\ 240,\ 1998,\ 840.$$

- For a prime p, we denote by $\kappa(p)$ the number of cycles of the permutations τ_{p,g_p}. Here is the list of values of κ for all primes $7 \leq p \leq 107$:

$$2,\ 4,\ 5,\ 2,\ 6,\ 3,\ 4,\ 3,\ 6,\ 5,\ 2,\ 6,\ 7,\ 5,\ 10,\ 6,\ 5,\ 6,\ 8,\ 7,\ 4,\ 4,\ 11,\ 6,\ 9.$$

A Comments about the GitHub repository [4]

GitHub repository [4] accompanies this research paper. At the time of writing, it consists of the SageMath script 'FixedPoints_DH.sage', the file 'README.md', and several image files.

Here are the descriptions of selected functions defined in the script 'FixedPoints_DH.sage':

- For a prime p and an integer b coprime to p, the command $order\_mod(b, p)$ returns the order of the residue class of b in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of units of the ring $\mathbb{Z}/p\mathbb{Z}$.
- For a prime p and an integer b coprime to p, the command $is\_primitive(b, p)$ returns $True$ if b in a primitive root modulo p; otherwise, it returns $False$.
- For a prime p, $prim\_roots(p)$ is a generator of all primitive roots modulo p, e.g. the command $list(prim\_roots(p))$ returns
$$[5,\ 10,\ 20,\ 17,\ 11,\ 21,\ 19,\ 15,\ 7,\ 14]$$
- Let p be prime, b be a primitive root modulo p and x be any integers; the command $DH\_perm(p, b, x)$ returns $\tau_{p,b}(x)$; usually, we assume that $1 \leq x \leq p - 2$.
- Let p be prime and b be a primitive root modulo p; the command $DH\_order(p, b)$ returns the order of the DH permutation $\tau_{p,b}$.
- Let p be prime and b be a primitive root modulo p; the command $DH\_cycle\_type(p, b)$ returns the cycle type of the DH permutation $\tau_{p,b}$.
- Let p be prime and b be a primitive root modulo p; the command $fixed\_points(p, b)$ returns the tuple of all fixed points of the Diffie-Hellman permutation $\tau_{p,b}$.
- For a prime p, the command $fixed\_pts4smallest\_prim\_root(p)$ returns the tuple of all fixed points of the Diffie-Hellman permutation τ_{p,g_p}, where g_p is the smallest primitive root modulo p; equivalently, one can execute the command $fixed\_points(p, primitive\_root(p))$.
- For a prime $p > 7$, the commands $vul\_exp(p)$ and $vul\_exp1(p)$ return the list of all vulnerable exponents relative to p; usually, the resulting list is not sorted; the time performance of both commands $vul\_exp(p)$ and $vul\_exp1(p)$ is comparable.
- $vul\_exp\_slow()$ is a slow version of $vul\_exp()$; it was used for testing the functions $vul\_exp()$ and $vul\_exp1()$.

- Let p be a safe prime > 7; the command $vul\_exp4safe(p)$ returns the list of all vulnerable exponents relative to p; note that, under our assumptions, q and $p-2$ are not vulnerable exponents; so we ignore them; also, $(x+1)^2$ is not congruent to 1 if $1 \leq x \leq p-4$ and x in odd; usually, the output of $vul\_exp4safe()$ is not a sorted list.

- Let p be a safe prime > 7 and b be a primitive root modulo p; the command $fixed\_points4safe(p, b)$ returns the list of all fixed points of the permutation $\tau_{p,b}$.

- For a prime $p > 7$, the command $percentage\_vul\_exp(p)$ returns the percentage of vulnerable exponents among the total number of $(p-2)$ exponents relative to p.

- For a safe prime $p > 7$, the command $percentage\_vul\_exp4safe(p)$ returns the percentage of vulnerable exponents among the total number of $(p-2)$ exponents relative to p.

- Let p be a prime and x be an integer $1 \leq x \leq p-2$; the command $disting\_prim\_roots(x, p)$ returns the tuple of primitive roots b modulo p for which $\tau_{p,b}(x) = x$.

- For a prime p and a vulnerable exponent x, the command $num\_disting\_prim\_roots(x, p)$ returns the size of the set $\Omega_{x,p}$ of distinguished primitive roots for the pair (x, p); the command should not be applied if x is not a vulnerable exponent.

- Let x be a vulnerable exponent relative to a prime p and b be a primitive root modulo p; the command $disting\_exp(x, p, b)$ returns the tuple of integers $k \in \{1, \ldots, p-2\}$ such that $\tau_{p,b^k}(x) = x$.

- For a prime p, the command $root\_profile(p, timed = None)$ returns the list L of nonnegative integers of length $p-1$; if an integer $0 \leq k \leq p-2$ is coprime to $(p-1)$, then $L[k]$ is the number of fixed points of the DH permutation τ_{p,g_p^k}, where g_p is the smallest primitive root modulo p; if k is not coprime to $(p-1)$, then $L[k] = 0$.

- For a safe prime $p = 2q+1$, the command $root\_profile4safe(p)$ returns the list L of non-negative integers of length $(p-1)$; if an integer $0 \leq k \leq p-2$ is coprime to $2q$, then $L[k]$ is the number of fixed points of the DH permutation τ_{p,g_p^k}; otherwise, $L[k] = 0$.

- For a prime $p > 7$, the command $max\_num\_fp(p)$ returns the value $\mu(p)$ of the function μ (see (3)).

- For a safe prime $p > 7$, the command $max\_num\_fp4safe(p)$ returns the value $\mu(p)$ of the function μ (see (3)).

- For a prime p, the command $vul\_prim\_roots(p)$ returns the list of vulnerable primitive roots modulo p; the output may not be sorted.

By loading the script 'FixedPoints_DH.sage', one loads the list 'SP' of all safe primes $11 \leq p \leq 50,000,747$. There are $124,849$ safe primes in this range.

References

[1] Artin's Constant, Wolfram MathWorld, `https://mathworld.wolfram.com/ArtinsConstant.html`

[2] D.A. Burgess, On character sums and primitive roots, Proc. London Math. Soc. (3) **12** (1962), 179-192.

[3] W. Diffie and M. Hellman, New Directions in Cryptography, IEEE Trans. Info. Th. **22** (1976) 644-654.

[4] V.A. Dolgushev, DiffieHellman_FixedPoints, GitHub repository, `https://github.com/Pekatom/DiffieHellman_FixedPoints`

[5] E. Grosswald, On Burgess' bound for primitive roots modulo primes and an application to $\Gamma(p)$, Amer. J. Math. **103**, 6 (1981) 1171-1183.

[6] R.K. Guy, Unsolved problems in number theory, *Probl. Books in Math.* Springer-Verlag, New York, 2004, xviii+437 pp.

[7] C. Hooley, On Artin's conjecture. J. Reine Angew. Math. **225** (1967) 209–220.

[8] P. Landrock, Power map permutations and the discrete log problem, Des. Codes Cryptogr. **77**, 2-3 (2015) 713-724.

[9] M. Levin, C. Pomerance and K. Soundararajan, Fixed points for discrete logarithms, *Algorithmic number theory,* 6–15. Lecture Notes in Comput. Sci., **6197** Springer, Berlin, 2010

[10] C. Pomerance, Elementary thoughts on discrete logarithms, *Algorithmic number theory*, J. P. Buhler and P. Stevenhagen, eds., Math. Sci. Res. Inst. Pub. **44**, Cambridge U. Press, New York, 2008, pp. 385–396.

[11] M. Ram Murty, Artin's conjecture for primitive roots. Math. Intelligencer **10**, 4 (1988) 59–67.

[12] K.H. Rosen, Elementary Number Theory and Its Applications, Addison-Wesley Publishing Company, 1984.

[13] The On-Line Encyclopedia of Integer Sequences, `https://oeis.org/`