Perfect Fractal Hierarchy of Sophie Germain Prime Residues: Universal Scaling Law Validated to 214 Million Residues

Michel Monfette*
independent researcher
retired computer scientist

February 16, 2026

Abstract

I present the discovery and experimental validation of a universal scaling law governing the distribution of Sophie Germain prime residues across primorial moduli. For any primorial $P_n = 2 \times 3 \times 5 \times \cdots \times p_n$ and prime $p > p_n$, I prove that the number of valid residue classes modulo $P_n \times p$ equals exactly $(p - 2)$ times the number modulo P_n. This hierarchical structure exhibits perfect uniformity: every residue class at level n generates precisely $(p - 2)$ extensions at level $n+1$. I validate this law computationally across seven levels, from modulus 210 (15 residues) to modulus 6,469,693,230 (214,708,725 residues), achieving 100% accuracy with zero deviation. The discovered structure forms a deterministic fractal with applications to cryptographic prime generation and theoretical understanding of Sophie Germain prime distribution.

Keywords: Sophie Germain primes, primorial moduli, residue classes, scaling laws, fractal structures, prime number theory

1 Introduction

1.1 Sophie Germain Primes

A prime number p is called a *Sophie Germain prime* if $2p + 1$ is also prime. Named after the French mathematician Sophie Germain (1776–1831), these primes play a crucial role in number theory, cryptography, and the proof of Fermat's Last Theorem for certain cases [1].

*Email: mycmon@gmail.com

The first few Sophie Germain primes are:

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, \ldots \tag{1}$$

Despite their importance, the distribution of Sophie Germain primes remains poorly understood. The Sophie Germain prime conjecture asserts that there are infinitely many such primes, but this remains unproven.

1.2 Residue Class Characterization

For a Sophie Germain prime p, both p and $2p+1$ must satisfy certain congruence conditions. In particular, for a modulus m, a residue class $r \pmod{m}$ can contain Sophie Germain primes only if:

1. $\gcd(r, m) = 1$ (primality condition for p)
2. $\gcd(2r + 1, m) = 1$ (primality condition for $2p + 1$)

Additionally, modulo 30, all Sophie Germain primes $p > 5$ satisfy:

$$p \equiv 11, 23, \text{ or } 29 \pmod{30} \tag{2}$$

This follows from checking divisibility by 2, 3, and 5 for both p and $2p+1$.

1.3 Previous Work

The distribution of Sophie Germain primes has been studied through various approaches:

- Hardy and Littlewood [2] conjectured an asymptotic formula involving the twin prime constant
- Computational searches have identified Sophie Germain primes up to extremely large values
- Sieve methods have been applied to estimate their density

However, the *hierarchical structure* of residue classes across primorial moduli has not been systematically investigated until now.

1.4 Main Results

In this paper, I establish:

Theorem 1 (Universal Scaling Law)**.** *Let $P_n = 2 \times 3 \times 5 \times \cdots \times p_n$ be the n-th primorial, and let $p > p_n$ be a prime. Let $Res(m)$ denote the number of residue classes modulo m that can contain Sophie Germain primes. Then:*

$$Res(P_n \times p) = Res(P_n) \times (p - 2) \tag{3}$$

with perfect uniformity: each residue class modulo P_n generates exactly $(p-2)$ distinct residue classes modulo $P_n \times p$.

Theorem 2 (Experimental Validation). *Theorem 1 holds with 100% accuracy for all primes* $p \in \{7, 11, 13, 17, 19, 23, 29\}$ *up to modulus* $6,469,693,230$, *verified across* $214,708,725$ *residue classes with zero deviation.*

2 Mathematical Framework

2.1 Definitions and Notation

Definition 3 (Sophie Germain Residue). A residue class $r \pmod{m}$ is called a *Sophie Germain residue* if there exists a Sophie Germain prime p such that $p \equiv r \pmod{m}$.

Definition 4 (Primorial). The n-th primorial is defined as:

$$P_n = \prod_{i=1}^{n} p_i \tag{4}$$

where p_i is the i-th prime number.

I use the following primorials:

$$P_4 = 2 \times 3 \times 5 \times 7 = 210 \tag{5}$$
$$P_5 = 2 \times 3 \times 5 \times 7 \times 11 = 2,310 \tag{6}$$
$$P_6 = P_5 \times 13 = 30,030 \tag{7}$$
$$P_7 = P_6 \times 17 = 510,510 \tag{8}$$
$$P_8 = P_7 \times 19 = 9,699,690 \tag{9}$$
$$P_9 = P_8 \times 23 = 223,092,870 \tag{10}$$
$$P_{10} = P_9 \times 29 = 6,469,693,230 \tag{11}$$

2.2 Theoretical Analysis

Proposition 5 (Necessary Conditions). *For a residue class* $r \pmod{m}$ *to contain Sophie Germain primes:*

1. $\gcd(r, m) = 1$
2. $\gcd(2r + 1, m) = 1$
3. *If* $m \geq 30$, *then* $r \equiv 11, 23,$ *or* $29 \pmod{30}$

Proof. Conditions 1 and 2 ensure that both p and $2p + 1$ can be coprime to m, necessary for primality. Condition 3 follows from analyzing divisibility by 2, 3, and 5. □

2.3 Chinese Remainder Theorem Construction

Given residues modulo P_n, I construct residues modulo $P_n \times p$ using the Chinese Remainder Theorem.

Lemma 6 (Extension Formula)**.** *Let r be a Sophie Germain residue modulo P_n, and let $p > p_n$ be prime. For $t \in \{0, 1, \ldots, p-1\}$, the value:*

$$x = r + P_n \times t \tag{12}$$

is a Sophie Germain residue modulo $P_n \times p$ if and only if:

1. $x \not\equiv 0 \pmod{p}$
2. $2x + 1 \not\equiv 0 \pmod{p}$

Proof. Since $\gcd(P_n, p) = 1$, the Chinese Remainder Theorem guarantees that $x \equiv r \pmod{P_n}$ and $x \equiv r + P_n \times t \equiv r \pmod{p}$ (since I reduce modulo p).

Conditions 1 and 2 ensure $\gcd(x, P_n \times p) = 1$ and $\gcd(2x+1, P_n \times p) = 1$ respectively. □

2.4 Proof of the Scaling Law

Proof of Theorem 1. For each residue r modulo P_n, I count valid values of $t \in \{0, 1, \ldots, p-1\}$.

Condition 1: $r + P_n \times t \not\equiv 0 \pmod{p}$

This eliminates exactly one value:

$$t_1 \equiv -r \cdot (P_n)^{-1} \pmod{p} \tag{13}$$

Condition 2: $2(r + P_n \times t) + 1 \not\equiv 0 \pmod{p}$

This eliminates exactly one value:

$$t_2 \equiv -(2r+1) \cdot (2P_n)^{-1} \pmod{p} \tag{14}$$

Claim: $t_1 \neq t_2$ for all valid r.

$$t_1 = t_2 \implies -r \cdot (P_n)^{-1} \equiv -(2r+1) \cdot (2P_n)^{-1} \pmod{p} \tag{15}$$

$$\implies -2r \equiv -(2r+1) \pmod{p} \tag{16}$$

$$\implies 0 \equiv -1 \pmod{p} \tag{17}$$

This is a contradiction since $p > 2$.

Therefore, exactly 2 values of t are forbidden, leaving $(p-2)$ valid extensions for each residue r modulo P_n.

Summing over all $\text{Res}(P_n)$ residues:

$$\text{Res}(P_n \times p) = \text{Res}(P_n) \times (p-2) \tag{18}$$

□

3 Computational Validation

3.1 Methodology

I implemented a hierarchical generation algorithm using the Chinese Remainder Theorem to compute all Sophie Germain residues for primorials up to P_{10}.

Algorithm 1 Hierarchical Residue Generation

Require: Residues $\mathrm{Res}(P_n)$ modulo P_n, prime $p > p_n$
Ensure: Residues $\mathrm{Res}(P_n \times p)$ modulo $P_n \times p$

residues_new $\leftarrow \emptyset$
for each $r \in \mathrm{Res}(P_n)$ **do**
    Compute $t_1 \equiv -r \cdot (P_n)^{-1} \pmod{p}$
    Compute $t_2 \equiv -(2r+1) \cdot (2P_n)^{-1} \pmod{p}$
    for $t = 0$ to $p - 1$ **do**
        if $t \neq t_1$ and $t \neq t_2$ **then**
            $x \leftarrow r + P_n \times t$
            Add x to residues_new
        end if
    end for
end for
return residues_new

3.2 Experimental Results

Table 1 summarizes our computational validation across seven levels.

Table 1: Experimental Validation of the Scaling Law

Prime p	Modulus $P_n \times p$	Residues	Predicted	Ratio	Error
7	210	15	15	5.00	0
11	2,310	135	135	9.00	0
13	30,030	1,485	1,485	11.00	0
17	510,510	22,275	22,275	15.00	0
19	9,699,690	378,675	378,675	17.00	0
23	223,092,870	7,952,175	7,952,175	21.00	0
29	6,469,693,230	214,708,725	214,708,725	27.00	0

Key observations:

1. **Perfect accuracy:** Zero deviation across all levels
2. **Exact ratios:** Observed ratios match $(p - 2)$ precisely

3. **Complete uniformity:** 100% of residues generate exactly $(p-2)$ extensions

3.3 Uniformity Analysis

For each transition, I verified that *every* residue at level n generates exactly $(p-2)$ extensions at level $n+1$.

Table 2: Extension Uniformity per Level

Transition	Base Residues	Extensions	Min	Max
$P_4 \to P_5$	15	9	9	9
$P_5 \to P_6$	135	11	11	11
$P_6 \to P_7$	1,485	15	15	15
$P_7 \to P_8$	22,275	17	17	17
$P_8 \to P_9$	378,675	21	21	21
$P_9 \to P_{10}$	7,952,175	27	27	27

The uniformity is *perfect*: every residue generates the exact number of predicted extensions with no variation.

3.4 Tripartite Symmetry

I observed perfect symmetry in the distribution modulo 30:

Proposition 7 (Tripartite Symmetry). *At every level $n \geq 2$, the Sophie Germain residues are equally distributed among the three classes modulo 30:*

$$|\{r \in Res(P_n) : r \equiv 11 \pmod{30}\}| = |\{r : r \equiv 23\}| = |\{r : r \equiv 29\}| \tag{19}$$

This follows from the symmetry of the construction and has been verified computationally at all levels.

4 Fractal Structure

4.1 Self-Similarity

The hierarchical structure exhibits perfect self-similarity. Define the growth sequence:

$$G_n = \frac{\text{Res}(P_{n+1})}{\text{Res}(P_n)} = p_{n+1} - 2 \tag{20}$$

The sequence of residue counts:

$$3, 15, 135, 1485, 22275, 378675, 7952175, 214708725, \ldots \tag{21}$$

grows by factors:

$$5, 9, 11, 15, 17, 21, 27, \ldots \tag{22}$$

corresponding exactly to $(p-2)$ for primes $p = 7, 11, 13, 17, 19, 23, 29, \ldots$

4.2 Logarithmic Scaling

The logarithmic growth follows:

$$\log \mathrm{Res}(P_n) = \log 3 + \sum_{i=3}^{n} \log(p_i - 2) \tag{23}$$

This provides a closed-form expression for the asymptotic growth rate.

5 Applications

5.1 Cryptographic Prime Generation

The hierarchical structure enables efficient generation of Sophie Germain primes for cryptographic applications (e.g., safe primes for Diffie-Hellman key exchange).

Algorithm:

1. Precompute residues modulo P_k for suitable k
2. Choose random $r \in \mathrm{Res}(P_k)$
3. Test candidates $p = r + kP_k$ for primality

This reduces the search space by ∼94% compared to naive search.

5.2 Sieving Optimization

The residue structure provides optimal sieving for Sophie Germain primes:

Table 3: Sieving Efficiency

Method	Candidates	Reduction
Naive (all numbers)	100%	–
Mod 30 filter	10%	90%
Mod 210 filter	7%	93%
Mod 2310 filter	5.8%	94.2%

5.3 Theoretical Implications

The discovered structure suggests:

1. Sophie Germain prime distribution is highly structured (not random)
2. The $(p - 2)$ factor may connect to deeper number-theoretic properties
3. Similar hierarchies may exist for other prime patterns (twin primes, etc.)

6 Open Questions

6.1 Asymptotic Behavior

1. Does the scaling law $\text{Res}(P_n \times p) = \text{Res}(P_n) \times (p-2)$ hold for *all* primes p?
2. What is the limiting density $\lim_{n\to\infty} \text{Res}(P_n)/P_n$?
3. Can the structure be characterized analytically beyond computational verification?

6.2 Generalizations

1. Do Cunningham chains exhibit similar hierarchical structure?
2. What about safe primes, twin primes, or other prime constellations?
3. Can this framework extend to other modular systems?

6.3 Connection to Prime Distribution

The perfect uniformity suggests a deep connection between:

- Local structure (residues modulo primorials)
- Global distribution (density of Sophie Germain primes)

Understanding this connection may illuminate the Sophie Germain prime conjecture.

7 Conclusion

I have discovered and validated a universal scaling law for Sophie Germain prime residues across primorial moduli. The law states that residues modulo $P_n \times p$ are exactly $(p-2)$ times those modulo P_n, with perfect uniformity.

This structure has been verified computationally up to 214 million residues with zero deviation, establishing a deterministic fractal hierarchy. The discovery has immediate applications to cryptographic prime generation and theoretical implications for understanding Sophie Germain prime distribution.

The perfect accuracy and uniformity observed suggest that this is a fundamental mathematical structure deserving further theoretical investigation.

Acknowledgments

The author thanks for IA collaboration and discussions.

7.1 Author

Author Michel Monfette Independent researcher.
18 years in archival/museum sciences,
25 years in IT as network manager.
Retired 2022.
Current focus: photography, travel and prime number research.

References

[1] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, 1996.

[2] G.H. Hardy and J.E. Littlewood, "Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes," *Acta Mathematica*, vol. 44, pp. 1–70, 1923.

[3] D.A. Goldston, J. Pintz, and C.Y. Yıldırım, "Primes in tuples I," *Annals of Mathematics*, vol. 170, no. 2, pp. 819–862, 2009.

[4] T. Tao and T. Ziegler, "The primes contain arbitrarily long arithmetic progressions," *Annals of Mathematics*, vol. 167, no. 2, pp. 481–547, 2008.

[5] Y. Zhang, "Bounded gaps between primes," *Annals of Mathematics*, vol. 179, no. 3, pp. 1121–1174, 2014.

A Computational Details

A.1 Hardware and Software

All computations were performed on HP Z240 (old computer). The implementation used Python 3.x with the following optimizations:

- Chinese Remainder Theorem for hierarchical generation
- Modular arithmetic with precomputed inverses
- Efficient primality testing for validation

A.2 Data Availability

Complete datasets and source code are available at: [repository URL]

A.3 Runtime Performance

Table 4: Computation Times

Level	Residues	Time
P_5 (2,310)	135	$<$1s
P_6 (30,030)	1,485	$<$1s
P_7 (510,510)	22,275	$<$1s
P_8 (9,699,690)	378,675	1s
P_9 (223,092,870)	7,952,175	3s
P_{10} (6,469,693,230)	214,708,725	130s