https://utilitasmathematicapublishing.com

Journal of AI-Augmented Mathematics (JAAM)

Vol: 1, ISSUE: 1, 2025

Pg No: 47-49

Regarding Prime-Preserving Bijections and Their Rigidity

S. Parvathi[1]

*[1] Department of Mathematics and Statistics, Faculty of Science and Humanities, SRM Institute of Science and Technology Kattankulathur, Tamilnadu, India

Abstract

Bijections f: N → N that preserve primes are considered multiplicatively. We demonstrate that if this function f is uniformly gapped on primes p such that f(p) /= p and if the set of these primes that are shifted has a divergent reciprocal sum, then there is a limited number of primes that f may permute. These bijections may nontrivially permute an infinite number of composites linked to a limited number of moving primes, contrary to previous assertions. Our outcome strengthens earlier claims, thereby resolving a complex issue regarding mathematical systems' rigidity.

Keywords: Number Theory, Prime Number Theorem, Prime-Preserving Bijections

1. Introduction

Existence of non-trivial automorphisms of N maintaining arithmetic structure is a basic subject in number theory [2]. We show that prime-preserving bijections often let primes to be rearranged in any way, but that this restriction is reduced to a limited number when a uniform gap condition is applied to the movement of primes. Composites, on the other hand, allow for an endless number of nontrivial reorganizations. Applications to permutation-based encryption are made possible by this duality, which refines the "structure vs. randomness" paradigm in arithmetic systems [3].

Context.. The bijections $f : \mathbb{N} \to \mathbb{N}$ considered here are multiplicative and prime-preserving. Such functions arise from a permutation of the primes extended multiplicatively. We show that if there is a fixed constant $c > 0$ such that for every prime p with $f(p) \neq p$ one has

$$\frac{f(p)}{p} \geq 1 + c \quad \text{or} \quad \frac{f(p)}{p} \leq \frac{1}{1+c},$$

and if the set of moved primes has divergent reciprocal sum, then f may move only finitely many primes.

2. Preliminaries

Definition 2.1 (Prime-Preserving Bijection [1])**.** A bijection $f : \mathbb{N} \to \mathbb{N}$ is *prime-preserving* if

$$n \text{ is prime} \quad \Rightarrow \quad f(n) \text{ is prime.}$$

Journal of AI-Augmented Mathematics (JAAM)
Vol: 1, ISSUE: 1, 2025
Pg No: 47-49

Definition 2.2 (Multiplicative Function [1]). A function $f : \mathbb{N} \to \mathbb{N}$ is *multiplicative* if $f(1) = 1$ and

$$f(ab) = f(a)f(b) \quad \text{whenever } \gcd(a, b) = 1.$$

If this holds for all a, b, it is *completely multiplicative*.

Remark 2.3 (Scope of Bijections Considered). A completely multiplicative prime-preserving bijection f corresponds to a permutation σ of the primes: if $n = \prod_i p_i^{k_i}$, then

$$f(n) = \prod_i \sigma(p_i)^{k_i}.$$

Theorem 2.4 (Prime Number Theorem [1]). *Let $\pi(x)$ be the number of primes $\le x$. Then*

$$\pi(x) \sim \frac{x}{\log x}, \qquad \vartheta(x) = \sum_{p \le x} \log p \sim x.$$

3. Main Results

Lemma 3.1 (Finiteness of Moved Primes under a Gap Condition). *Let $f : \mathbb{N} \to \mathbb{N}$ be a completely multiplicative, prime-preserving bijection inducing a permutation σ on $\mathbb{P}$. Suppose there exists $c > 0$ such that for every prime p with $f(p) \neq p$,*

$$\frac{f(p)}{p} \ge 1 + c \quad \text{or} \quad \frac{f(p)}{p} \le \frac{1}{1+c},$$

and that $\sum_{p : f(p) \neq p} \frac{1}{p} = \infty$. Then only finitely many primes are moved by f.

Proof. Let $S = \{p \in \mathbb{P} : f(p) \neq p\}$ be the set of moved primes. For each prime p, define $r(p) = \frac{f(p)}{p}$. If $p \notin S$, then $r(p) = 1$ and $\log r(p) = 0$.

Consider

$$L = \sum_{p \in \mathbb{P}} \log r(p) = \sum_{p \in S} \log r(p).$$

Case 1: S is finite. Since f permutes S onto itself, $\prod_{p \in S} r(p) = 1$ and hence $\sum_{p \in S} \log r(p) = 0$. Thus $L = 0$.

Case 2: S is infinite. By hypothesis $\sum_{p \in S} 1/p = \infty$. The gap condition gives $\log r(p) \ge \delta > 0$ for all $p \in S$ (where $\delta = \log(1 + c)$). Hence $\sum_{p \in S} \log r(p)$ diverges by the term test, so L cannot be zero.

In either case, consistency of f as a permutation requires $L = 0$. The only resolution is that S must be finite. □

Theorem 3.2 (Structure of Composite Permutations). *Let f be as in Lemma 3.1, and let $S = \{p_1, \ldots, p_k\}$ be the finite set of moved primes. Then:*

1. *f fixes every prime $p \notin S$.*
2. *f permutes infinitely many composites. Indeed, if $n = p_j^m K$ with $p_j \in S$, $m \ge 1$, and $\gcd(K, p_j) = 1$, then*

$$f(n) = f(p_j)^m f(K) = f(p_j)^m K \neq n,$$

and varying m, K yields infinitely many such n.

Proof. **(1)** Immediate from Lemma 3.1.

(2) Write $n = \prod_{p \in S} p^{\alpha_p} \prod_{q \in /S} q^{\beta_q}$. Then

$$f(n) = \prod_{p \in S} f(p)^{\alpha_p} \times \prod_{q \in /S} q^{\beta_q}.$$

Choosing $n = p_j^m K$ with K supported on primes not in S gives $f(n) = f(p_j)^m K \neq n$, and infinitely many choices of m, K produce infinitely many non-fixed composites. □

https://utilitasmathematicapublishing.com
Vol: 1, ISSUE: 1, 2025
Pg No: 47-49
Journal of AI-Augmented Mathematics (JAAM)

4. Application to Cryptographic Permutations

The duality between prime rigidity and composite flexibility enables novel permutation constructions. For instance, in pseudorandom number generation, finite prime swaps can seed format-preserving encryption schemes [3].

5. Conclusion

A multiplicative prime-preserving bijection may permute an unlimited number of composites associated with primes, but it can only fix a finite number of primes under the uniform gap requirement and divergent-reciprocal-sum hypothesis.

> Any multiplicative, prime-preserving bijection $f : \mathbb{N} \to \mathbb{N}$ satisfying a uniform gap condition (with the moved primes having divergent reciprocal sum) fixes all but finitely many primes, but may permute infinitely many composites associated with those finitely many moved primes.

References

[1] Hardy, G. H., & Wright, E. M. (1979). An introduction to the theory of numbers. Oxford university press. 2.1, 2.2, 2.4
[2] Erd˝os, P. (1935). On arithmetic properties of integers.Acta Arithmetica, 1, 23–56. 1
[3] Katz, J., & Lindell, Y. (2020). Introduction to modern cryptography crc press. Taylor & Francis. DOI, 10, 9781351133036. 1, 4