Article

Not peer-reviewed version

Prime Pair Products Based on Prime Gaps

Ahmet F. Gocgen * , Berke Sahin , Emin M. Buyukyayla

Posted Date: 31 December 2024

doi: 10.20944/preprints202412.2542.v1

Keywords: prime pairs; prime gaps; prime products; prime distribution; number theory

Article

Prime Pair Products Based on Prime Gaps

Ahmet F. Gocgen [1,*], Berke Sahin [1] and Emin M. Buyukyayla [2]

[1] Department of Mathematics, Ordu University; berkeshn17@gmail.com; +90-535-022-49-40
[2] Independent Researcher; eminmertbuyukyayla@gmail.com; +90-543-862-25-75
* Correspondence: ahmetfgocgen@gmail.com; +90-552-750-66-35

Abstract: This paper investigates the arithmetic structure of prime pair products by analyzing the gaps between primes. Focusing on pairs, we explore patterns in the distribution of their products. We establish that prime pairs with gaps a power of 6 yield products in the form $6n + 1$, while those without power of 6 gaps result in products of the form $6n + 5$, except where 2 and 3 are found, offering a foundational understanding of their algebraic properties.

Keywords: prime pairs; prime gaps; prime products; prime distribution; number theory

MSC: 11A41

1. Introduction

Prime numbers have long been a central topic in number theory, offering deep insights into the structure of mathematics [1]. A particularly intriguing area of study involves prime pairs, where two prime numbers are closely related by a small difference, such as twin primes (with a gap of 2) or cousin primes (with a gap of 4). While these pairs have been explored extensively in terms of their distribution, less attention has been given to the products of prime pairs and how the gap between the primes may influence their behavior.

This paper seeks to investigate prime pair products by focusing on the differences (or gaps) between the primes in each pair. Specifically, we explore whether certain patterns or properties emerge when analyzing prime products based on these gaps. By examining the multiplication of prime pairs, we aim to uncover potential connections between the arithmetic structure of prime numbers and the distribution of their products.

Through this exploration, a deeper understanding of prime pairs and their unique characteristics is hoped to be contributed, with implications for both theoretical research and practical applications in cryptography, computational number theory, and beyond.

2. Methods

Prime Pair Classification: Each pair of prime numbers is divided into two categories: those whose difference is a multiple of 6 and those whose difference is not a multiple of 6. The reason for choosing this categorization can be shown in relation to the results obtained in the study titled "Dynamics and Forms of Products of Twin, Cousin and Sexy Primes".

According to Gocgen and Buyukyayla in the related study [2]:

Twin and cousin prime pairs without 2 and 3 can be expressed as $6\beta + 5$, while sexy prime pairs can be expressed as $6\beta + 1$.

Based on this study and this result in particular (since there are 6 differences between the sexy primes), this way of categorization was used.

Analytical Approach to Prime Pair Products: The goal of the analysis was to observe how the gaps between primes impact the properties of their products. The following steps outline the approach used to explore these relationships.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 December 2024 doi:10.20944/preprints202412.2542.v1

Product Computation: For each identified prime pair (p_1, p_2), the product $P = p_1 \times p_2$ was computed. The resulting values were analyzed to detect patterns in their magnitude and behavior based on the gap size between the primes. Special focus was placed on pairs fitting specific forms, such as $6n + 5$ and $6n + 7$.

Modular Behavior Exploration: The products of prime pairs were studied under modular arithmetic. Products were reduced modulo k to investigate their residue classes and potential regularities. For example, products were examined for behavior like $P \equiv r \pmod 6$, where residue patterns may correlate with specific prime gaps.

NOTATIONS

$\mathbb{Z}^+$	the set of all positive integers
$\mathbb{N}$	the set of all natural numbers
$\mathbb{N}^+$	the set of all positive natural numbers
$\mathbb{C}$	the set of all composite numbers
$\mathbb{P}$	the set of all prime numbers
$\mathbb{O}$	the set of all odd numbers
$\mathbb{E}$	the set of all even numbers
$\gcd(a, b)$	$\max\{d \in Z^+ : d \mid a \text{ and } d \mid b\}$

3. Theorems and Proofs

At the outset of the study, it will be beneficial to provide several definitions and elaborations:

Definition 1. Prime numbers are defined as follows [3,4]:

$$\forall n \in \mathbb{Z}^+, 1 < n < p,\ \gcd(p, n) = 1$$

Definition 2. Composite numbers are defined as follows [3,5]:

$$\forall n \in \mathbb{Z}^+, 1 < n < c,\ \gcd(c, n) \neq 1$$

Basis 1. Every positive integer except 1 is classified as either a prime number or a composite number [6].

Basis 2. Every composite number can be uniquely expressed as the product of more than one prime number [6,7].

Conjecture. (p, q) being the prime pair; if the difference between p and q is a multiple of 6, the product of p and q must be in the form $6n + 1$. If the difference between p and q is not a multiple of 6, the product of p and q must be in the form $6n + 5$, where p and q is not equal 2 or 3.

Lemma 1. A number is either multiply of 6 or not multiply of 6.

Proof.

$$P(n) : \text{“The number is multiply of 6.”}$$

$$\neg P(n) : \text{The number is not multiply of 6.”}$$

In logic, every proposition is either true or false (***the principle of non-contradiction in classical logic***). Therefore, the propositions $P(n)$ and $\neg P(n)$ cannot be true at the same time. We have the expression:

$$P(n) \vee \neg P(n) : \text{“The number is either multiply of 6 or not multiply of 6.”}$$

$P(n)$	$\neg P(n)$	$P(n) \vee \neg P(n)$
1	0	1
0	1	1

This statement is a ***tautology*** in logic, that is, a proposition that is always true.

□

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 December 2024 doi:10.20944/preprints202412.2542.v1

Lemma 2. A set of numbers can be separated into a proposition and its negation, with all the elements of the set being partitioned.

Proof. Let A be a set of numbers. Let $P(x)$ be a proposition.

$$A_P = \{x \in A : P(x) \text{ is true}\}$$
$$A_{\neg P} = \{x \in A : P(x) \text{ is false}\}$$

Based on the ***principle of non-contradiction*** in basic logic:

$$A_P \cup A_{\neg P} = A \text{ and } A_P \cap A_{\neg P} = \emptyset.$$

According to the first statement, all elements are partitioned into disjoint subsets. Based on the second statement, it follows that each element satisfies exactly one proposition. Thus, the proof is concluded.

□

Corollary 1. Let A be the set of prime products and let P be the proposition: "the difference between primes is multiple of 6". In this case, all prime products can be separated by the difference between the prime numbers by which they are multiplied. To such an extend, with this separation, all elements will be separated and no element will satisfy both conditions.

Lemma 3. $np + p$ gives all composite numbers where n is a positive natural numbers and p is a prime number [8].

Proof. $np + p = p(n+1)$. Then, according to fundamental theorem of arithmetic and ***Basis 1***:

$$(n+1 \in \mathbb{C}) \oplus (n+1 \in \mathbb{P})$$

Let $n+1 \in \mathbb{C}$:

$$n+1 = p_m \times \cdots \times p_{m+k}$$

Then,

$$p(n+1) = p \times (p_m \times \cdots \times p_{m+k})$$

Let $n+1 \in \mathbb{P}$:

$$n+1 = p_m$$

Then,

$$p(n+1) = p \times p_m$$

$$\therefore p(n+1) = p \times (p_m \times \cdots \times p_{m+k}) \oplus p(n+1) = p \times p_m$$

Thus, this expression gives all composite numbers by ***Basis 2***.

□

Lemma 4. $2np + p$ gives all odd composite numbers where n is a positive natural numbers and p is an odd prime numbers.

Proof. $np + p$ gives all composite numbers where p is an prime number and n is a positive natural number by ***Lemma 3***. Only the possibility for an odd composite just specified: $np + p$ gives all odd composite numbers where p is an odd number and n is a even number. This equals to: $2np + p$ gives all odd composite numbers where n is a positive natural number and p is an odd prime number.

□

Theorem 1. All odd prime numbers except 3 must be of the form $6n+5$ or $6n+7$, as a result of formula $2np + p$ [9].

$$\forall p \in \mathbb{P} - \{3\} \cap \mathbb{O} \implies \exists n \in \mathbb{N}, (p = 6n+5 \text{ or } p = 6n+7)$$

Proof.

$$2np + p, p = 3 \implies 6n+3$$
$$\forall n \in \mathbb{N}^+, \quad 3(2n+1) = 6n+3.$$
$$6n+3 < x < 6(n+1)+3 \quad \implies \quad x \in \{6n+4, 6n+5, 6n+6, 6n+7, 6n+8\}(n \in \mathbb{N}^+ \implies n \in \mathbb{N})$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 December 2024 doi:10.20944/preprints202412.2542.v1

$$
\begin{gathered}
6n+4 \equiv 0 \pmod 2 \\
6n+5 \equiv 1 \pmod 2 \\
6n+6 \equiv 0 \pmod 2 \\
6n+7 \equiv 1 \pmod 2 \\
6n+8 \equiv 0 \pmod 2 \\
x \in \{6n+4, 6n+6, 6n+8\} \implies 2 \mid x \iff x \notin \mathbb{P} - \{3\} \cap \mathbb{O} \\
x \in \{6n+5, 6n+7\} \implies x \mod 2 = 1 \quad \wedge x \notin 3k \\
\therefore \forall p \in \mathbb{P} - \{3\} \cap \mathbb{O} \implies \exists n \in \mathbb{N}, (p = 6n+5 \text{ or } p = 6n+7)
\end{gathered}
$$

□

Corollary 4. It is possible to examine the prime multiplications, excluding those involving 2 and 3, forms of $6n+5$ and $6n+7$ by ***Theorem 1***.

Lemma 5. The result of subtracting two odd numbers is always even.

Proof.

$$
\begin{gathered}
\forall p = 2n+1 \text{ where } n \in \mathbb{N} \text{ and } p \in \mathbb{P} - \{3\} \cap \mathbb{O} \\
\therefore p_i - p_j = (2n_i+1) - (2n_j+1) = 2n_i + 1 - 2j_i - 1 = 2(n_i - n_j)
\end{gathered}
$$

where $p_i = 2n_i + 1$, $p_j = 2n_j + 1$ and $i > j$ when $i, j \in \mathbb{N}$

□

Theorem 2. The structure mentioned in ***Corollary 1*** is mathematically separated by $6k$ and $6k+2$, $6k+4$.

$$\forall x \in \mathbb{N} \cap \mathbb{E}, x = 6k \oplus (6k+2 \oplus 6k+4),\ k \in \mathbb{N}$$

Proof. According to the principle of non-contradiction and as shown in ***Lemma 1***:

$$
\begin{gathered}
\text{Let } \forall n \in \mathbb{N} \text{ be such that } n = 6k \oplus n \neq 6k \\
n = 6k \iff 6 \mid n \\
n \neq 6k \iff 6k < x < 6(k+1)
\end{gathered}
$$

Therefore:

$$
\begin{gathered}
6k+1 \equiv 1 \pmod 2 \\
6k+2 \equiv 0 \pmod 2 \\
6k+3 \equiv 1 \pmod 2 \\
6k+4 \equiv 0 \pmod 2 \\
6k+5 \equiv 1 \pmod 2
\end{gathered}
$$

According to Lemma 5:

$$
\begin{gathered}
\text{If } n \equiv 2 \pmod 6, n = 6k+2. \\
\text{If } n \equiv 4 \pmod 6, n = 6k+4. \\
\therefore \forall x \in \mathbb{N} \cap \mathbb{E}, x = 6k \oplus (6k+2 \oplus 6k+4),\ k \in \mathbb{N}
\end{gathered}
$$

□

Corollary 5. The structures to be examined are as follows:

Let $\forall p, q \in \mathbb{P} - \{3\} \cap \mathbb{O}$ be such that $|p-q| = 6k$:

$$(p,q) = (6n+5, 6n+5+6k) \oplus (6n+7, 6n+7+6k)$$

Let $|p-q| = 6k+2 \oplus 6k+4$:

$$
\begin{gathered}
(p,q) = (6n+5, 6n+5+6k+2) \oplus (6n+7, 6n+7+6k+2) \\
\oplus (6n+5, 6n+5+6k+4) \oplus (6n+7, 6n+7+6k+4)
\end{gathered}
$$

The relevant arrangements are made in these groups, and the groups are then written as follows:

Let $|p-q| = 6k$:

$$(p,q) = (6n+5, 6n+6k+5) \oplus (6n+7, 6n+6k+7)$$

Let $|p-q| = 6k+2 \oplus 6k+4$:

$$
\begin{gathered}
(p,q) = (6n+5, 6n+6k+7) \oplus (6n+7, 6n+6k+9) \\
\oplus (6n+5, 6n+6k+9) \oplus (6n+7, 6n+6k+11)
\end{gathered}
$$

Theorem 3. Some expressions in the group lack meaning and can be removed from the group.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 December 2024 doi:10.20944/preprints202412.2542.v1

Proof. $6n + 6k + 9$ is absolutely divisible by 3, so it is not possible for this expression to represent a prime number. Therefore, pairs containing this expression are devoid of meaning and can be removed from the group. As a result, if the groups are rewritten with the remaining expressions:
Let $\forall n \in \mathbb{N}$ be such that $|p - q| = 6k$:

$$(p, q) = (6n + 5, 6n + 6k + 5) \oplus (6n + 7, 6n + 6k + 7)$$

Let $|p - q| = 6k + 2 \oplus 6k + 4$:

$$(p, q) = (6n + 5, 6n + 6k + 7) \oplus (6n + 7, 6n + 6k + 11)$$

expressions emerge.
□

Corollary 6. Then, for the prime pair (p, q); p and q are not equal, 2, 3; if the difference between p and q is not equal to multiply of 6 and has the form $p = 6n + 5$, the form of the difference between p and q must be $6n + 2$. If it is in the form $p = 6n + 7$, the form of the difference between p and q must be $6n + 4$. Such that $\forall p, q \in \mathbb{P} - \{3\} \cap \mathbb{O}$:

$$\text{If } p = 6n + 5 \text{ and } |p - q| \neq 6k \implies |p - q| = 6k + 2$$
$$\text{If } p = 6n + 7 \text{ and } |p - q| \neq 6k \implies |p - q| = 6k + 4$$

Corollary 7. When the relevant multiplication operations are performed on these groups, it becomes possible for the groups to be written as follows:
Let $\forall n \in \mathbb{N}$ be such that $|p - q| = 6k$:

$$(p \times q) = (36n^2 + 36nk + 60n + 30k + 25) \oplus (36n^2 + 36nk + 84n + 42k + 49)$$

Let $|p - q| = 6k + 2$:

$$(p \times q) = (36n^2 + 36nk + 72n + 30k + 35)$$

Let $|p - q| = 6k + 4$:

$$(p \times q) = (36n^2 + 36nk + 108n + 42k + 77)$$

Theorem 4. Both of these groups have characteristic features according to mod 6.
Proof.
Let $\forall n \in \mathbb{N}$ be such that $|p - q| = 6k$:

$$36n^2 + 36nk + 60n + 30k + 25 \equiv 1 \pmod 6$$
$$36n^2 + 36nk + 84n + 42k + 49 \equiv 1 \pmod 6$$

Let $|p - q| = 6k + 2$:

$$36n^2 + 36nk + 72n + 30k + 35 \equiv 5 \pmod 6$$

Let $|p - q| = 6k + 4$:

$$36n^2 + 36nk + 108n + 42k + 77 \equiv 5 \pmod 6$$

□

Corollary 8. The remainder of multiplying two primes with a difference of multiple of 6 and dividing by 6 is 1; the remainder of multiplying two primes without a difference of multiple of 6 and dividing by 6 is 5 where two prime is not equal to 2 or 3.
Corollary 9.
Let $\forall n \in \mathbb{N}$ be such that $|p - q| = 6k$:
First option:

$$36n^2 + 36nk + 60n + 30k + 25 = 6(6n^2 + 6nk + 10n + 5k + 4) + 1$$
$$\beta = 6n^2 + 6nk + 10n + 5k + 4$$
$$36n^2 + 36nk + 60n + 30k + 25 = 6\beta + 1$$

Second option:

$$36n^2 + 36nk + 84n + 42k + 49 = 6(6n^2 + 6nk + 14n + 7k + 8) + 1$$
$$\beta = 6n^2 + 6nk + 14n + 7k + 8$$
$$36n^2 + 36nk + 84n + 42k + 49 = 6\beta + 1$$

Let $|p - q| = 6k + 2$:

$$36n^2 + 36nk + 72n + 30k + 35 = 6(6n^2 + 6nk + 12n + 5k + 5) + 5$$
$$\beta = 6n^2 + 6nk + 12n + 5k + 5$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 December 2024 doi:10.20944/preprints202412.2542.v1

$$36n^2 + 36nk + 72n + 30k + 35 = 6\beta + 5$$

Let $|p - q| = 6k + 4$:

$$36n^2 + 36nk + 108n + 42k + 77 = 6(6n^2 + 6nk + 18n + 7k + 12) + 5$$
$$\beta = 6n^2 + 6nk + 18n + 7k + 12$$
$$36n^2 + 36nk + 108n + 42k + 77 = 6\beta + 5$$

The result obtained from here is generalized, which can be achieved in ***Corollaries 5, 6, 7*** and ***Theorem 3, 4***, and the following is obtained; let $\forall p, q \in \mathbb{P} - \{3\} \cap \mathbb{O}$:

$$|p - q| = 6k \iff (p \times q) = 6\beta + 1$$
$$|p - q| \neq 6k \iff (p \times q) = 6\beta + 5$$

This result obtained as a result of all theorems and corollaries proves conjecture.

Q.E.D.

4. Results

A detailed examination has been provided in this study of the primes other than 2 and 3 that can be expressed as $6n + 5$ or $6n + 7$, and their relationship to the prime pairs. Certain forms have been obtained for prime pairs with a difference of a multiple of 6, and for prime pairs without a difference that is a multiple of 6, establishing a foundational understanding of their algebraic structure. Using these forms, it has been proved that the products of prime pairs with a difference of a multiple of 6 must be of the form $6n + 1$, and that the products of prime pairs without a difference of a multiple of 6 must be of the form $6n + 5$. These insights contribute to the broader understanding of prime numbers and offer potential applications in areas such as cryptography, where the properties of prime numbers are essential.

5. Discussion

1. Summary of Key Findings

The study has provided significant insights into the dynamics and forms of products of prime pairs. By systematically analyzing these products, several key observations have been made:

Distribution Characteristics: The products of the prime pairs exhibit different distributional properties. Unlike the primes themselves, which are known to become sparser as numbers increase, the products of prime pairs show unique clustering and gap patterns. The statistical analysis revealed non-uniformity in their distribution, hinting at underlying structural rules governing their occurrence.

Modular Behavior: The exploration of products in various modular systems uncovered fascinating patterns in the residue classes. Certain residue classes are occupied more frequently, suggesting that the products of prime pairs have a predisposition toward specific modular outcomes. This behavior is nontrivial and may reflect deeper arithmetic properties inherent to these primes.

2. Comparison with Existing Literature

The findings of this study build upon and extend existing knowledge on prime numbers, particularly in the context of primes and their products.

Distribution of Primes: Previous studies have extensively examined the distribution of primes and prime pairs (e.g., twin primes, cousin primes...). The results of this study add a new dimension by focusing on the products of prime pairs. Although the distribution of individual primes has been shown to follow known theorems and conjectures, the observed clustering and gap patterns in prime products suggest novel behaviors that merit further exploration.

Modular Arithmetic in Prime Studies: The modular behavior of primes has been a topic of interest in number theory, with studies exploring primes in arithmetic progressions and other modular systems. The results obtained in this paper are specifically in agreement with the modular properties obtained for twin, cousin, and sexy primes [2,10]. The discovery of preferred residue classes for prime products aligns with, but also challenges, some of these established results. The unexpected

 doi:10.20944/preprints202412.2542.v1

regularities observed here could lead to new conjectures about the distribution of prime products in modular systems.

3. Theoretical Implications

The results obtained in this study have several theoretical implications for number theory and related fields:

Prime Product Conjectures: The non-random distribution patterns and modular regularities observed in prime products could inform new conjectures in number theory. For instance, the tendency of these products to occupy specific residue classes suggests that there may be deeper, yet undiscovered, rules governing prime product behavior.

Structure of Prime Networks: The graph theoretical insights suggest that primes and their products form structured networks rather than random graphs. This could have implications for understanding the connectivity of primes, potentially leading to new insights into prime gaps, distribution, and the underlying algebraic structures.

Potential Links to Cryptography: The modular properties of prime products might have applications in cryptography, where prime number-based algorithms are foundational. The discovery of non-trivial residue class occupation could lead to the development of new cryptographic methods or the strengthening of existing ones.

4. Future Research Directions

The findings of this study open up several avenues for future research:

Distribution of Primes: The methodologies used in this study for the detection of numbers that are simply the product of two primes can be developed to include all odd composite numbers or all composite numbers. This development could open the door to a deeper understanding of composite numbers and more information about the order of prime numbers.

Twin Prime Conjecture: With the results obtained in this study, a certain form that twin primes must comply with can be determined, and thanks to this form, twin prime conjecture can be expressed with a new definition. This new definition may lead us to gain other insights by using the modular properties obtained.

Extended Modular Analysis: Future studies could extend the modular analysis to include a wider range of moduli, particularly those that have been less explored in number theory. This could involve exploring the behavior of prime products in non-integer moduli or in more complex modular systems.

Cryptographic Applications: Given the modular regularities observed, further research could explore the potential cryptographic applications (especially RSA [11]) of prime products. This could involve developing new algorithms based on the properties of these products or enhancing existing prime-based cryptographic systems [12].

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: We would like to express our sincere gratitude to Bill McEachen and Mehmet Aslan for their invaluable support in reviewing the general structure of this paper, including its mathematical formulation and grammatical aspects. Their insightful feedback and guidance were instrumental in enhancing the clarity and quality of this work.

References

1. Goldstein, L.J. A history of the prime number theorem. *The American Mathematical Monthly* **2019**, *80*, 599–615.
2. Gocgen, A.F.; Buyukyayla, E.M. Dynamics and Forms of Products of Twin, Cousin and Sexy Primes. *Preprints* **2024**.

3. Ingham, A.E. *The distribution of prime numbers*; Number 30, Cambridge University Press, 1990.
4. Selberg, A. An elementary proof of the prime-number theorem. *Annals of Mathematics* **1949**, pp. 305–313.
5. Novikas, A. Composite numbers in the sequences of integers **2012**.
6. Euclid.; Heath, T.L. *The Thirteen Books of the Elements, Vol. 2: Books 3-9*; Dover Publications, 1956.
7. Ağargün, A.G.; Özkan, E.M. A historical survey of the fundamental theorem of arithmetic. *Historia Mathematica* **2001**, *28*, 207–214.
8. Aysun, E.; Gocgen, A.F. A Fundamental Study of Composite Numbers as a Different Perspective on Problems Related to Prime Numbers. *International Journal of Pure and Applied Mathematics Research* **2023**, *3*, 70–76.
9. Gocgen, A.F. Gocgen Approach for Bounded Gaps Between Odd Composite Numbers. *Preprints* **2024**.
10. Nelsen, R. Proof Without Words: Cousin Prime Products Modulo 72. *The College Mathematics Journal* **2024**, *55*, 245–245.
11. Childs, L.N. RSA cryptography and prime numbers. *Cryptology and Error Correction: An Algebraic Introduction and Real-World Applications* **2019**, pp. 135–151.
12. Riesel, H. Prime Numbers and Cryptography. *Prime Numbers and Computer Methods for Factorization* **1994**, pp. 226–238.