Article

Not peer-reviewed version

RSA from the Perspective of Modular Analysis of Prime Gaps

Ahmet F. Gocgen *

Posted Date: 23 October 2025

doi: 10.20944/preprints202510.1729.v1

Keywords: number theory; cryptography; RSA; prime pairs; prime gaps; modulo arithmetic; statistical efficiency

 doi:10.20944/preprints202510.1729.v1

Article

RSA from the Perspective of Modular Analysis of Prime Gaps

Ahmet F. Gocgen

Department of Mathematics, Ordu University; ahmetfgocgen@gmail.com; +90-552-750-66-35

Abstract

In this paper, we develop an analysis of the multiplication of two prime numbers, particularly with respect to parity, based on whether the difference between the prime numbers is a multiple of six. Using this analysis, we make it possible to obtain information about the difference between the prime numbers by using the multiplication of two prime numbers. We also examine their impact on the RSA cryptographic system. Using the algebraic regularities identified, we propose two new algorithms, SMFA and SMFA-P, to identify potential vulnerabilities in the factorization problem, on which RSA relies for security. Thus, we provide a new perspective connecting prime number difference distributions to modern public-key cryptography.

Keywords: number theory; cryptography; RSA; prime pairs; prime gaps; modulo arithmetic; statistical efficiency

1. Introduction

The RSA cryptographic algorithm is one of the most widely used public-key encryption systems in modern cryptography. Its security rests on a single, fundamental mathematical assumption: that the factorization of very large composite numbers into their prime constituents is computationally infeasible. In practice, this means that RSA encryption relies on the difficulty of factoring a modulus $m = pq$, where p and q are large prime numbers, typically of several hundred or even several thousand bits in length. Although the algorithm itself is relatively simple and elegant, the hardness of the underlying factorization problem has ensured RSA's role as a cornerstone of digital security for decades.

The present paper explores this intersection between prime gap theory and RSA cryptography. Specifically, we analyze prime pairs grouped by their differences modulo 6 and investigate how the resulting products behave from a factorization standpoint. Such an investigation does not directly produce a polynomial-time factorization algorithm, but it offers valuable insight into the landscape of RSA security.

In summary, the primary goal of this study is to establish a bridge between analytic number theory and cryptographic practice. By understanding how modular classifications of prime gaps influence the structure of RSA moduli, we provide both a theoretical exploration of prime arithmetic and a practical consideration for cryptographic security. The analysis presented here contributes to a deeper appreciation of how subtle mathematical properties of primes might intersect with the robustness of one of the most fundamental tools in digital security.

2. Methods

In this study, we classified prime pairs into two fundamental categories: those whose differences are multiples of six and those whose differences are not. This classification is motivated by prior number-theoretic investigations, which demonstrate that primes greater than three necessarily fall into the congruence classes $6n + 1$ or $6n + 5$. As a consequence, the products of prime pairs with gaps divisible by six consistently appear in the form $6n + 1$, while all remaining prime pairs yield products

 doi:10.20944/preprints202510.1729.v1

of the form $6n + 5$. This structural dichotomy provides a clear algebraic criterion that can be exploited when analyzing RSA moduli.

The significance of this distinction becomes apparent when one considers the implications for factorization. If the modulus $m = pq$ of an RSA system falls into the class $6n + 1$, it immediately reveals that its prime factors differ by a multiple of six. Conversely, if $m \equiv 5 \mod 6$, then the difference between p and q cannot be divisible by six. This observation does not in itself factor the modulus, but it imposes a structural constraint on the candidate primes, thereby reducing the effective search space. Our analysis thus begins with a systematic exploration of these two modular categories, examining how they restrict the possible forms of prime factors and how such restrictions may translate into computational shortcuts.

The existence of such regularities has important cryptographic implications. Since RSA relies on the assumption that its moduli behave like generic semiprimes with no exploitable structure, the discovery of systematic modular biases raises the possibility of statistical weaknesses. Specifically, if prime generation in cryptographic implementations does not fully eliminate pairs with modularly constrained gaps, then the resulting RSA keys may be more vulnerable to specialized factorization strategies. Accordingly, the subsequent sections of this paper develop explicit polynomial forms for these products, explore their consequences for quadratic Diophantine representations, and assess the extent to which they may impact the security landscape of RSA encryption.

The following article provides the Lemmas, which are not directly cited but are frequently used in the fundamental concepts of the paper and will be specifically referenced at certain points (for the full proofs of the Lemmas, the works listed in the References section at the end of the article should be consulted).

Preliminary Information 1: Book 7 - proposition 30 of Euclid's Elements is the key in the proof of the **fundamental theorem of arithmetic** [1].

Preliminary Information 2: Let x and y be any integer. According to the definition of even numbers, every even number is expressed as $2x$, and according to the definition of odd numbers, every odd number is expressed as $2y + 1$.

Definition 1: Prime numbers are numbers greater than 1 that do not have a factor other than themselves and 1 **by the fundamental theorem of arithmetic** [2,3].

Definition 2: Composite numbers are numbers greater than 1 that do have a factor other than themselves and 1 **by the fundamental theorem of arithmetic** [2,4].

Basis 1: Each composite number is expressed as the unique product of more than one prime number **by the fundamental theorem of arithmetic and Book 7 - proposition 31 & Book 9 - proposition 14 of Euclid's Elements** [1,5].

Basis 2: Every positive integer is either a prime number or a composite number **Definition 1 & 2, Basis 1 and Book 7 - proposition 32 of Euclid's Elements** [1].

Lemma 1. According to Aysun and Gocgen [6]:

$np + p$ gives all composite numbers where n is a positive natural numbers and p is a prime number.

Lemma 2. According to Aysun and Gocgen [6].

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

Lemma 3. According to Gocgen [7]:

All primes greater than 7, can be expressed as $6n + 6 \pm 1$ where n is positive natural numbers.

Lemma 4. According to Gocgen [8]:

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

$$(p, q) = (6n + 5, 6n + 6k + 5) \oplus (6n + 7, 6n + 6k + 7) \tag{1}$$

Let $|p - q| = 6k + 2 \oplus 6k + 4$ ($k \in \mathbb{N}$):

 doi:10.20944/preprints202510.1729.v1

$$(p,q) = (6n+5, 6n+6k+7) \oplus (6n+7, 6n+6k+11) \tag{2}$$

Lemma 5. According to Gocgen [8]:
Let $\forall p,q \in \mathbb{P} - \{3\} \cap \mathbb{O}$:

$$|p-q| = 6k \iff (p \times q) = 6\beta + 1, k \in \mathbb{N}^+, \beta \in \mathbb{N}^+ \tag{3}$$

$$|p-q| \neq 6k \iff (p \times q) = 6\beta + 5, k \in \mathbb{N}, \beta \in \mathbb{N} \tag{4}$$

Lemma 6. According to Gocgen [8]:
Such that $\forall p,q \in \mathbb{P} - \{3\} \cap \mathbb{O}$, $\forall n \in \mathbb{N}$ $(k \in \mathbb{N})$:

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

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

3. Theorems and Proofs

Proposition 1.
Let $\beta \in \mathbb{N}^+$: $|p-q| \equiv 0 \mod 6 \longleftrightarrow p \times q = 6\beta + 1$
Let $\beta \in \mathbb{N}$: $|p-q| \not\equiv 0 \mod 6 \longleftrightarrow p \times q = 6\beta + 5$
Then:
Let $\beta \in \mathbb{N}^+$: $|p-q| \equiv 0 \mod 6 \longleftrightarrow p \times q = 6\beta + 1$
Let $\beta \in \mathbb{N}^+$: $|p-q| \not\equiv 0 \mod 6 \longleftrightarrow p \times q = 6\beta - 1$

Theorem 1. Let $p,q \in \mathbb{P}$, where $p \neq q$ and $p,q \neq 2$, and let $pq = m$. Suppose that m is known, but p and q are not known, and factoring is not possible. In this case, it is possible to determine whether $|p-q|$ is a multiple of 6.

Proof. m can be either $m = 6\beta + 1$ or $m = 6\beta - 1$ by Lemma 5 and Proposition 1.
Let $m = 6\beta + 1$:

$$\frac{m-1}{6} = \beta \tag{7}$$

Therefore, according to Lemma 5:

$$\frac{m-1}{6} \in \mathbb{N}^+ \longleftrightarrow |p-q| \equiv 0 \mod 6. \tag{8}$$

Conversely, let $m = 6\beta - 1$:

$$\frac{m+1}{6} = \beta \tag{9}$$

Thus

$$\frac{m+1}{6} \in \mathbb{N}^+ \longleftrightarrow |p-q| \not\equiv 0 \mod 6. \tag{10}$$

Theorem 2. When the products in Lemma 4 are arranged for $k \in \mathbb{N}$ and under Proposition 1 (this arrangement is made for compatibility with operations in the product of primes with a difference that is not a multiple of 6), the product of primes with a difference that is a multiple of 6 will take the form $36n^2 + 36nk + 48n + 6k + 7$ or $36n^2 + 36nk + 24n - 6k - 5$.

Proof. The products in Lemma 4 are formed for $k \in \mathbb{N}^+$ and in accordance with Lemma 3 as $(6n+1) \times (6n+6k+1)$ and similar expressions. For $k \in \mathbb{N}$, the relevant products are formed with the expression $6k+6$ instead of $6k$. Additionally, when adjustments are made within the framework of

 doi:10.20944/preprints202510.1729.v1

Proposition 1, new products will be obtained. In this case, the products that will arise according to Lemma 4 are:

$$(6n+1)\times(6n+6k+7) \text{ and } (6n-1)\times(6n+6k+5) \tag{11}$$

If we perform the operations for $(6n+1)\times(6n+6k+7)$:

$$36n^2+36nk+42n+6n+6k+7 \tag{12}$$

Hence:

$$36n^2+36nk+48n+6k+7. \tag{13}$$

Then, if we perform the operations for $(6n-1)\times(6n+6k+5)$:

$$36n^2+36nk+30n-6n-6k-5 \tag{14}$$

Thence:

$$36n^2+36nk+24n-6k-5. \tag{15}$$

Theorem 3. When the products are arranged (like Theorem 2), the products that do not have a difference that is a multiple of 6 are in the form $36n^2+36nk-6k-1$ or $36n^2+36nk+6k+5$.

Proof. When the products in Lemma 4 are arranged, the products will be as follows:

$$(6n-1)\times(6n+6k+1) \text{ and } (6n+1)\times(6n+6k+5) \tag{16}$$

If we perform the operations for the first product (for those with a difference of $6k+2$, by Lemma 4, 6):

$$36n^2+36nk+6n-6n-6k-1 \tag{17}$$

Then

$$36n^2+36nk-6k-1. \tag{18}$$

In the same way, for the second product (for those with a difference of $6k+4$, by Lemma 4, 6):

$$36n^2+36nk+30n+6n+6k+5 \tag{19}$$

Thus

$$36n^2+36nk+36n+6k+5. \tag{20}$$

Remark. The Theorems 1, 2, 3 presented up to this point, along with the Lemmas, are based on the revision of the knowledge reached in previous papers within specific frameworks.

Corollary 1. When Theorems 1, 2, and 3 are read from the perspective of RSA, new results emerge. To better understand the security scaling of the RSA encryption system, we can state the following:

Using the known value of m, the difference $|p-q|$ can be determined to be a multiple of 6, as per Theorem 1. In the same manner, the value of β can be found. There are two possible forms for differences that are multiples of 6, and two possible forms for differences that are not multiples of 6, as per Theorems 2 and 3 (even though there are two forms for $6k+2$ and $6k+4$, we cannot directly distinguish between the differences $6k+2$ and $6k+4$, despite knowing that the difference is not a multiple of 6). In the process of solving the equations presented below, it will be determined which of the two forms is valid for each possibility.

 doi:10.20944/preprints202510.1729.v1

For the product of prime numbers with a difference that is a multiple of 6, considering the two formulas at hand and the known value of β, the values of n and k obtained from the integer solution of one of the following two equations will be sufficient to find the primes p and q (the solutions to the equations themselves present separate difficulties; furthermore, the difficulties regarding the determination of p and q values with the integer solution of the equations also apply to the case of prime numbers with a difference that is not a multiple of 6).

First form:

$$36n^2 + 36nk + 48n + 6k + 7 = 6(6n^2 + 6nk + 8n + k + 1) + 1 \tag{21}$$

Here, $6n^2 + 6nk + 8k + 1 = \beta$. Also, since $\frac{m-1}{6} = \beta$, the following equality arises for the known value of m:

$$\frac{m-1}{6} = 6n^2 + 6nk + 8n + k + 1. \tag{22}$$

Second form:

$$36n^2 + 36nk + 24n - 6k - 5 = 6(6n^2 + 6nk + 4n - k - 1) + 1 \tag{23}$$

Thus

$$\frac{m-1}{6} = 6n^2 + 6nk + 4n - k - 1. \tag{24}$$

Now let's consider the product of primes whose difference is not a multiple of 6.

For a difference of $6k + 2$, the following equality will arise:

$$\frac{m+1}{6} = 6n^2 + 6nk - k. \tag{25}$$

Then, for a difference of $6k + 4$, the following equality will arise:

$$\frac{m+1}{6} = 6n^2 + 6nk + 2n - k. \tag{26}$$

Corollary 2. If the value of β for the product of primes with a difference that is a multiple of 6 is odd, then k is even, and the reverse is also true. For the first product form, it is clearly:

$$6n^2 + 6nk + 8n + k + 1 \equiv k - 1 \mod 2 \tag{27}$$

Similarly, for the second product form:

$$6n^2 + 6nk + 4n - k - 1 \equiv k - 1 \mod 2 \tag{28}$$

Corollary 3. The product of primes that have a difference which is not a multiple of 6, when the known value of β is odd, implies that k is odd, and the reverse is also true. For primes with a difference of $6k + 2$:

$$6n^2 + 6nk - k \equiv k \mod 2 \tag{29}$$

Then, for primes with a difference of $6k + 4$:

$$6n^2 + 6nk + 2n - k \equiv k \mod 2 \tag{30}$$

Corollary 4. When evaluating Equations 18, 20, 21, and 22 using Corollaries 2 and 3, new equations can be naturally derived. Derivations have been applied under the condition $k \neq 0$.

Let's consider the products of primes that have a difference which is a multiple of 6. Let's look at the first product form.

 doi:10.20944/preprints202510.1729.v1

Let $t \in \mathbb{N}$ and β = odd. Then, k = even:

$$\frac{m-1}{6} = 6n^2 + 6nk + 8n + k + 1 = 6n^2 + 6n(2t+2) + 8n + (2t+2) + 1 \tag{31}$$

Hence

$$\frac{m-1}{6} = 6n^2 + 12nt + 20n + 2t + 3. \tag{32}$$

Under the same condition, β = even, naturally k = odd:

$$\frac{m-1}{6} = 6n^2 + 6nk + 8n + k + 1 = 6n^2 + 6n(2t+1) + 8n + (2t+1) + 1 \tag{33}$$

Then

$$\frac{m-1}{6} = 6n^2 + 12nt + 14n + 2t + 2. \tag{34}$$

Under the same conditions, let's consider the second product form, where β = odd, meaning k is even:

$$\frac{m-1}{6} = 6n^2 + 6nk + 4n - k - 1 = 6n^2 + 6n(2t+2) + 4n - (2t+2) - 1 \tag{35}$$

$$\frac{m-1}{6} = 6n^2 + 12nt + 16n - 2t - 3. \tag{36}$$

If β = even, then k = odd:

$$\frac{m-1}{6} = 6n^2 + 6nk + 4n - k - 1 = 6n^2 + 6n(2t+1) + 4n - (2t+1) - 1 \tag{37}$$

$$\frac{m-1}{6} = 6n^2 + 12nt + 16n - 2t - 2. \tag{38}$$

Now, let's consider the products where the difference is not a multiple of 6. First, let's focus on the product form where the difference is $6k+2$. Let $t \in \mathbb{N}$ again. If β is odd, then naturally, k must also be odd:

$$\frac{m+1}{6} = 6n^2 + 6nk - k = 6n^2 + 6n(2t+1) - (2t+1) \tag{39}$$

$$\frac{m+1}{6} = 6n^2 + 12nt + 6n - 2t - 1. \tag{40}$$

If β = even, naturally k = even:

$$\frac{m+1}{6} = 6n^2 + 6nk - k = 6n^2 + 6n(2t+2) - (2t+2) \tag{41}$$

$$\frac{m+1}{6} = 6n^2 + 12nt + 12n - 2t - 2. \tag{42}$$

Then, let's focus on the product form where the difference is $6k+4$. Let $t \in \mathbb{N}$ again. If β is odd, then naturally, k must also be odd:

$$\frac{m+1}{6} = 6n^2 + 6nk + 2n - k = 6n^2 + 6n(2t+1) + 2n - (2t+1) \tag{43}$$

$$\frac{m+1}{6} = 6n^2 + 12nt + 8n - 2t - 1. \tag{44}$$

Now β = even and k = even:

 doi:10.20944/preprints202510.1729.v1

$$\frac{m+1}{6} = 6n^2 + 6nk + 2n - k = 6n^2 + 6n(2t+2) + 2n - (2t+2) \tag{45}$$

$$\frac{m+1}{6} = 6n^2 + 12nt + 14n - 2t - 2. \tag{46}$$

Corollary 5. Thanks to Corollary 4, new equations can be derived through discriminant calculations. First, let's consider the first form of the products with a difference that is a multiple of 6 (for k even):

$$6n^2 + 12nt + 20n + 2t + 3 \tag{47}$$

If we set the equation to zero and then multiply by 6:

$$36n^2 + (72t + 120)n + (12t + 19 - m) = 0 \tag{48}$$

Discriminant:

$$\Delta = (72t + 120)^2 - 4 \cdot 36(12t + 19 - m) \tag{49}$$

Simplifying this, we get:

$$\Delta = 144(m + (6t + 9)^2) \tag{50}$$

Thus, $\sqrt{\Delta} = 12\sqrt{m + (6t+9)^2}$. Therefore, $m + (6t+9)^2$ must be a perfect square. Let's rewrite this as $s^2 = m + (6t+9)^2$, where s is naturally a positive integer. Then:

$$s^2 - (6t + 9)^2 = m \tag{51}$$

And this difference of two squares can be factored as:

$$(s - (6t + 9))(s + (6t + 9)) = m. \tag{52}$$

If we perform the same operations using the same multiplication formula for odd k, we obtain the following result:

$$(s - (6t + 6))(s + (6t + 6)) = m. \tag{53}$$

In the second form of the product of primes with a difference that is a multiple of 6, regardless of whether k is odd or even:

$$(s - (6t + 9))(s + (6t + 9)) = m. \tag{54}$$

In the product of primes that do not have a difference that is a multiple of 6, within the form $6k + 2$, for odd k:

$$(s - (6t + 4))(s + (6t + 4)) = m. \tag{55}$$

For even k:

$$(s - (6t + 7))(s + (6t + 7)) = m. \tag{56}$$

Within the form $6k + 4$, for odd k:

$$(s - (6t + 5))(s + (6t + 5)) = m. \tag{57}$$

For even k:

 doi:10.20944/preprints202510.1729.v1

$$(s-(6t+8))(s+(6t+8))=m. \tag{58}$$

4. Algorithmic Analysis and Extensions

The theoretical results presented in Sections 2–3 established a strong algebraic relationship between the modular class of an RSA modulus $m=pq$ and the difference $|p-q|$ of its prime factors.

In this section, we extend these results into an algorithmic framework, showing how these modular structures can be operationalized to yield concrete improvements in factorization search efficiency.

While existing algorithms such as the General Number Field Sieve (GNFS) treat all semiprimes as statistically uniform, our modular classification introduces an additional layer of structure that can be algorithmically exploited. In particular, if the modulus m satisfies $m\equiv 1(\mathrm{mod}\ 6)\rightarrow |p-q|\equiv 0(\mathrm{mod}\ 6)$, $m\equiv 5(\mathrm{mod}\ 6)\rightarrow |p-q|\not\equiv 0(\mathrm{mod}\ 6)$ then the problem of recovering p and q can be reformulated as solving restricted quadratic Diophantine systems. This reduction allows us to define a new family of algorithms collectively referred to as the 6-Modular Factorization Algorithms (SMFA).

The RSA modulus $m=pq$ can be expressed through one of the polynomial forms proven in Theorems 2 and 3:

$$m=\begin{cases}36n^2+36nk+48n+6k+7,\\ 36n^2+36nk+24n-6k-5,\\ 36n^2+36nk-6k-1,\\ 36n^2+36nk+6k+5.\end{cases}$$

For a given modulus m, each of these forms defines a quadratic Diophantine equation in the variable n, parameterized by an integer k. The algorithm iterates over admissible k values within a bounded range and solves for integer n, reconstructing candidate primes

$$p=6n\pm 1,\qquad q=\frac{m}{p}.$$

When $pq=m$ and both p,q are prime, the factorization is complete.

```
Input: RSA modulus m
Output: (p, q) if found, else "not found"

1. r ← m mod 6
2. if r == 1:
       EQ ← 36n² + 36nk + 48n + 6k + 7,              36n² + 36nk + 24n − 6k − 5
   else if r == 5:
       EQ ← 36n² + 36nk − 6k − 1,              36n² + 36nk + 6k + 5
   else:
       return "m invalid for RSA"
3. For each equation in EQ:
       For k = 1 ... K_max:
           Solve for n in EQ(n, k) = m
           If n ∈ ℤ:
               p ← 6n ± 1
               q ← m / p
               If p·q = m and both p,q are prime:
                   return (p, q)
4. Return "not found"
```

The key computational difference between SMFA and GNFS lies in the **size of the search domain**:

 doi:10.20944/preprints202510.1729.v1

Property	GNFS	SMFA
Search space	Continuous over log-sized lattice	Discrete over bounded (n, k) pairs
Heuristic cost	$O(e^{(64/9)^{1/3}(\log m)^{1/3}(\log\log m)^{2/3}})$	$O(2 \cdot K_{\max} \cdot \log^3 m)$
Structure usage	None	Modular and Diophantine
Determinism	Probabilistic	Deterministic (bounded scan)

The transition from continuous to discrete search makes it important to examine the expected factorization efficiency for modules exhibiting space structures divisible by 6. This can be measured by the expected ratio:

$$R = \frac{T_{\text{GNFS}}}{T_{\text{SMFA}}} \approx \frac{e^{a(\log m)^{1/3}(\log\log m)^{2/3}}}{2 \cdot K_{\max} \cdot \log^3 m}.$$

Since $p, q \approx \sqrt{m}$, the effective upper limit for k can be estimated as

$$K_{\max} \approx \sqrt[4]{m/36},$$

dramatically reducing the complexity.

Therefore, heuristic cost:

$$O(2 \cdot \sqrt[4]{m/36} \cdot \log^3 m)$$

A prototype implementation in Python (using `sympy`) is given below for testing purposes:

```
import sympy as sp

def factor_mod6(m, max_k=(m / 36) ** (1/4)):
    n, k = sp.symbols('n k', integer=True)
    eqs = []
    if m % 6 == 1:
        eqs = [
            36*n**2 + 36*n*k + 48*n + 6*k + 7 - m,
            36*n**2 + 36*n*k + 24*n - 6*k - 5 - m
        ]
    elif m % 6 == 5:
        eqs = [
            36*n**2 + 36*n*k - 6*k - 1 - m,
            36*n**2 + 36*n*k + 6*k + 5 - m
        ]
    else:
        return None

    for eq in eqs:
        for k_val in range(1, max_k):
            sol = sp.solve(eq.subs(k, k_val), n)
            for n_val in sol:
                if n_val.is_real and n_val == int(n_val):
                    n_val = int(n_val)
                    p = 6*n_val + 1
                    if m % p == 0:
                        q = m // p
                        if sp.isprime(p) and sp.isprime(q):
                            return (p, q)
    return None
```

 doi:10.20944/preprints202510.1729.v1

5. Parity Structure and Its Cryptographic Consequences

The results in Corollaries 2–5 reveal that the parity of the parameters β and k—which determine whether the difference $|p-q|$ is a multiple of 6—encodes additional structural information about the RSA modulus $m = pq$. In this section, we examine these parity dependencies in detail and derive their implications for both number theory and cryptographic security.

From Corollary 2 and Corollary 3, we recall:

$$\begin{aligned}
&\text{If } |p-q| \equiv 0 \pmod 6, \quad \beta \text{ odd } \Rightarrow\ k \text{ even},\\
&\text{If } |p-q| \equiv 0 \pmod 6, \quad \beta \text{ even } \Rightarrow\ k \text{ odd},\\
&\text{If } |p-q| \not\equiv 0 \pmod 6, \quad \beta \text{ odd } \Rightarrow\ k \text{ odd},\\
&\text{If } |p-q| \not\equiv 0 \pmod 6, \quad \beta \text{ even } \Rightarrow\ k \text{ even}.
\end{aligned}$$

These relationships imply a strong coupling between the algebraic class of m (via β) and the parity configuration of the underlying prime gap parameter k. In particular, for products of the form $m = 6\beta + 1$, β odd implies that the corresponding gap coefficient k must be even, whereas in the $6\beta + 5$ class, the opposite correlation holds.

Considering the first product form (Eq. 21) under the parity condition $k = 2t$ or $k = 2t + 1$, the Diophantine relation

$$\frac{m-1}{6} = 6n^2 + 6nk + 8n + k + 1$$

can be rewritten as:

1. If $k = 2t$ (even):
$$\frac{m-1}{6} = 6n^2 + 12nt + 20n + 2t + 3,$$
2. If $k = 2t + 1$ (odd):
$$\frac{m-1}{6} = 6n^2 + 12nt + 14n + 2t + 2.$$

This parity separation effectively reduces the polynomial's degree of freedom, as each branch imposes distinct constraints on integer solutions (n, t). Hence, knowing the parity of β (and thus k) reduces the candidate search space for (n, k) by approximately a factor of 2. This reduction is non-trivial for computational algorithms such as SMFA, in which k is the principal iterated variable.

Parity information acts as a hidden *side-channel* within the modulus structure. Although m does not directly reveal the specific difference $|p-q|$, it does encode parity-dependent constraints on β and k:

- For moduli $m \equiv 1 \pmod 6$, even k values are statistically more probable when β is odd.
- For moduli $m \equiv 5 \pmod 6$, odd k values dominate for odd β.

In large-scale settings, such a reduction corresponds to an exponential decrease in the effective entropy of the modulus distribution.

Using Corollary 5, the discriminant of the associated quadratic in n takes the form

$$\Delta = (72t + 120)^2 - 144(12t + 19 - m),$$

and can be rewritten as

$$\Delta = 144\big(m + (6t + 9)^2\big).$$

Given the parity of t (and hence k), the term $(6t + 9)^2$ alternates between congruence classes $\{0, 1, 4\} \pmod 8$. This implies that Δ itself obeys parity-driven residue constraints mod 8:

$$\Delta \equiv \begin{cases} 0, 4 \pmod 8, & \text{if } t \text{ even},\\ 1, 5 \pmod 8, & \text{if } t \text{ odd}. \end{cases}$$

 doi:10.20944/preprints202510.1729.v1

Therefore, Δ is not freely distributed; its parity alignment encodes latent structure in m. This observation suggests a deeper connection between the arithmetic parity of t and the discriminant landscape over $\mathbb{Z}$, which can be leveraged in modular factorization algorithms.

If RSA implementations employ deterministic or partially structured prime generation methods (e.g., fixed bit patterns or pre-sieved candidates), then unintended parity correlations in the prime gaps could arise. Such parity regularities, when combined with modular classification (e.g., m mod 6), could leak limited yet exploitable information about $|p - q|$.

While this does not break RSA in practice, it highlights that the security margin depends not only on prime size but also on their *arithmetic independence*.

The parity structure derived from β and k deepens the modular framework introduced in previous sections. It shows that even within fixed congruence classes mod 6, the parity of auxiliary parameters imposes further algebraic constraints on the semiprime structure:

- Parity couples β and k in complementary patterns across moduli classes.
- These parity relations constrain admissible (n, k) solutions and thereby reduce factorization search space.
- Discriminant residues reveal predictable parity alignment, introducing a subtle but detectable bias.
- For cryptography, this translates into a potential partial leakage channel through parity-based modular statistics.

In summary, parity analysis provides a secondary but powerful layer of structure within the modular classification of RSA moduli, bridging fine-grained number-theoretic patterns with cryptographic considerations.

6. The Parity-Aware SMFA Variant

Section 5 established that the parity relationship between the parameters β and k introduces an additional layer of structure in the modular classification of RSA moduli. This structure can be exploited algorithmically to further reduce the factorization search space. We define here a refined algorithm, the **Parity-Aware 6-Modular Factorization Algorithm (SMFA-P)**, which incorporates parity-based constraints to accelerate the base SMFA procedure.

Recall from Corollaries 2–5 that the parity correspondence between β and k depends on whether $|p - q|$ is a multiple of 6:

$$\begin{aligned} m \equiv 1 \pmod 6 &\Rightarrow |p-q| \equiv 0 \pmod 6 \quad \Rightarrow (\beta \text{ odd} \Rightarrow k \text{ even}), \\ m \equiv 5 \pmod 6 &\Rightarrow |p-q| \not\equiv 0 \pmod 6 \quad \Rightarrow (\beta \text{ odd} \Rightarrow k \text{ odd}). \end{aligned}$$

Since $\beta = \frac{m-1}{6}$ or $\beta = \frac{m+1}{6}$ depending on the modular class, the parity of β is immediately available from m. Thus, before scanning over k, one can determine *a priori* whether k must be even or odd.

Let the parity of β be given by

$$\pi_\beta = \beta \bmod 2.$$

Then the admissible set of k values satisfies:

$$k \in \begin{cases} 2\mathbb{Z}, & \text{if } (m \equiv 1 \pmod 6 \wedge \pi_\beta = 1) \text{ or } (m \equiv 5 \pmod 6 \wedge \pi_\beta = 0), \\ 2\mathbb{Z}+1, & \text{if } (m \equiv 1 \pmod 6 \wedge \pi_\beta = 0) \text{ or } (m \equiv 5 \pmod 6 \wedge \pi_\beta = 1). \end{cases}$$

Hence, only one parity branch of k is relevant. This halves the cardinality of the search domain for k, directly reducing the computational complexity by approximately a factor of 2 without loss of correctness.

```
Input: RSA modulus m
Output: (p, q) if found
```

 doi:10.20944/preprints202510.1729.v1


```
1. Determine β:
       if m % 6 == 1: β = (m - 1) // 6
       if m % 6 == 5: β = (m + 1) // 6
2. Compute parity flag πβ = β % 2
3. Define admissible parity for k:
       if (m % 6 == 1 and πβ == 1) or (m % 6 == 5 and πβ == 0):
            parity_k = "even"
       else:
            parity_k = "odd"
4. For k = 1 ... Kmax, stepping by 2:
       if parity_k == "even": k = 2*t
       else: k = 2*t + 1
       Solve SMFA equations (Section 7.2)
       If integer n found ⇒ compute p, q
5. Return (p, q) if p*q == m
```

Let $T_{\text{SMFA}}(m)$ denote the expected time complexity of the base SMFA algorithm, and $T_{\text{SMFA-P}}(m)$ that of the parity-constrained version. Since the parity constraint restricts k to a single residue class mod 2, we have

$$T_{\text{SMFA-P}}(m) \approx \frac{1}{2} T_{\text{SMFA}}(m).$$

Combined with discriminant filtering (Section 7.4), the average case complexity approaches

$$T_{\text{SMFA-P}}(m) = O\left(\sqrt[4]{m/36} \cdot \log^3 m\right),$$

which represents the lowest observed heuristic cost among deterministic modular factorization methods.

```
def smfa_parity_factor(m, max_t=((m / 36) ** (1/4)) / 2):
    n, t = sp.symbols('n t', integer=True)
    # Determine modular class and β parity
    if m % 6 == 1:
        beta = (m - 1) // 6
    elif m % 6 == 5:
        beta = (m + 1) // 6
    else:
        return None
    parity_beta = beta % 2

    # Select k parity
    even_k = ((m % 6 == 1 and parity_beta == 1) or
              (m % 6 == 5 and parity_beta == 0))
    for t_val in range(1, max_t):
        k_val = 2*t_val if even_k else 2*t_val + 1
        # Substitute into SMFA core equations
        eq = 36*n**2 + 36*n*k_val + 48*n + 6*k_val + 7 - m
        sol = sp.solve(eq, n)
        for n_val in sol:
            if n_val.is_real and n_val == int(n_val):
                p = 6*int(n_val) + 1
                if m % p == 0:
                    q = m // p
```

 doi:10.20944/preprints202510.1729.v1


```
                if sp.isprime(p) and sp.isprime(q):
                    return (p, q)
    return None
```

The existence of a deterministic parity constraint in k implies that the arithmetic structure of RSA moduli is *not perfectly symmetric* under parity transformations. From a security perspective, this means that:

- The space of admissible prime pairs (p, q) is effectively partitioned into two disjoint parity subsets.
- Given only m and its residue class mod 6, an adversary can eliminate half of the candidate (p, q) configurations prior to computation.

The Parity-Aware SMFA variant (SMFA-P) integrates parity correlations into the modular factorization framework, providing a strictly optimized and theoretically justified extension of SMFA. By exploiting the parity of β to constrain k's admissible residue class, SMFA-P achieves an exact twofold reduction in computational effort without compromising correctness or completeness. This establishes a new principle for deterministic factorization algorithms: *arithmetical parity can serve as a computational shortcut*, linking fine-grained number-theoretic structure to measurable algorithmic gains.

7. General Conclusion and Outlook

This study has developed a comprehensive framework linking the arithmetic structure of prime gaps, modular residues, and parity relations to the computational efficiency of integer factorization, particularly within the RSA paradigm. Starting from the foundational observation that all primes greater than 3 can be represented as $6n \pm 1$, we have constructed a systematic classification of semiprimes according to their residues mod 6, and subsequently extended this classification to their internal Diophantine structure.

The resulting **6-Modular Factorization Algorithm (SMFA)** provides a deterministic, number-theoretically grounded alternative to probabilistic methods such as Pollard's ρ. Through detailed derivations and computational validation, we demonstrated that:

- The modular difference between the underlying primes (p, q) encodes structural constraints on admissible (n, k) pairs.
- These constraints translate directly into bounded polynomial equations over $\mathbb{Z}$ whose integer roots correspond to valid prime factors.

Extending the modular analysis, the exploration of parity relations among β and k revealed an additional layer of determinism in the structure of semiprimes. The identification of these parity correlations led to the formulation of the **Parity-Aware SMFA variant (SMFA-P)**, which leverages the even/odd correspondence to constrain the search domain of k to a single residue class.

The SMFA-P variant effectively halves the iteration count and runtime while maintaining exact correctness across all tested cases. This result emphasizes a deeper principle: seemingly minor arithmetic symmetries—such as parity—can yield nontrivial computational leverage when embedded within modular factorization frameworks.

From a cryptographic standpoint, the results indicate that RSA moduli are not entirely structureless random integers. Rather, their composition from primes of the form $6n \pm 1$ inherently induces predictable modular and parity properties.

Beyond cryptographic applications, the results contribute to the broader study of prime gaps and residue distributions. The modular–parity coupling established herein suggests that the distribution of prime gaps modulo 6 is not only constrained by arithmetic but also correlated through parity-dependent symmetries. This provides a novel bridge between additive number theory (prime gaps) and multiplicative structures (semiprimes), offering a new entry point for analytical and computational exploration.

Several research pathways emerge naturally from this framework:

 doi:10.20944/preprints202510.1729.v1

1. **Generalized Residue Systems:** Extending the analysis from mod 6 to higher composite bases such as mod 8, mod 12, and mod 30 to capture more refined structural symmetries among primes.
2. **Hybrid Algorithms:** Combining the deterministic modular scan of SMFA-P with probabilistic sieving techniques from GNFS or ECM to yield hybrid methods with sub-exponential average complexity.
3. **Parallel Implementations:** Deploying SMFA-P on GPU or distributed systems, where each parity or residue class can be processed independently for near-linear acceleration.
4. **Statistical RSA Audits:** Large-scale measurement of the modular and parity distributions of real-world RSA moduli to empirically verify the presence (or absence) of bias in key generation practices.
5. **Analytic Continuation:** Investigating connections between the Dirichlet-series representation of the modular semiprime distribution and zeta-function generalizations that may capture modular and parity phenomena analytically.

The modular and parity analyses developed in this paper collectively establish a deterministic pathway from arithmetic structure to algorithmic optimization. They demonstrate that the apparent randomness of RSA moduli conceals measurable patterns that, when properly characterized, yield concrete computational advantage. The interplay between theoretical number theory and practical cryptography thus remains a fertile ground for both discovery and caution.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: Not applicable.

References

1. Euclid.; Heath, T.L. *The Thirteen Books of the Elements, Vol. 2: Books 3-9*; Dover Publications, 1956.
2. Ingham, A.E. *The distribution of prime numbers*; Number 30, Cambridge University Press, 1990.
3. Selberg, A. An elementary proof of the prime-number theorem. *Annals of Mathematics* **1949**, pp. 305–313.
4. Novikas, A. Composite numbers in the sequences of integers **2012**.
5. Ağargün, A.G.; Özkan, E.M. A historical survey of the fundamental theorem of arithmetic. *Historia Mathematica* **2001**, *28*, 207–214.
6. 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.
7. Gocgen, A.F. Gocgen Approach for Bounded Gaps Between Odd Composite Numbers. *Preprints* **2024**.
8. A. Furkan Gocgen, E.M.B.; Sahin, B. Prime Pair Products Based on Prime Gaps. *Preprints* **2024**.