Generalizing the Difference of Squares via Sequence-Based Transformations
(Rough Draft)

Troy Winarski

April 23, 2025

Abstract

We propose a novel generalization of the classical identity $a^2 - b^2 = (a + b)(a - b)$ by introducing a transformation framework that applies structured integer sequences to derive perfect squares. This transformation enables broader applications in integer factorization and reveals a deeper structure in the difference of values transformed into perfect squares. Unlike traditional methods, our approach does not rely solely on consecutive integers or perfect squares but extends to arbitrary sequences that exhibit algebraic or combinatorial regularity.

1 Introduction

The identity $a^2-b^2 = (a+b)(a-b)$ is a fundamental tool in number theory, especially in the context of factorization methods such as Fermat's method. In its classical form, it assumes that both a and b are integers such that their squares differ by a target number N, which can then be factored.

Fermat's method, attributed to Pierre de Fermat in the 17th century, searches for integers a and b such that $a^2 - b^2 = N$, particularly effective when N is the product of two close factors. Since then, more advanced factorization algorithms have been developed, such as the Quadratic Sieve and the General Number Field Sieve. This work is not intended to compete with or surpass these algorithms, but instead contributes to the richness of factorization theory by exploring structure through transformation.

This paper generalizes the identity by altering the domain of a and b. Rather than selecting values whose squares are naturally close, we generate a and b through structured transformations applied to elements of integer sequences. These transformations produces values that, when squared, exhibit differences equal to N or a multiple thereof. This unlocks new potential for detecting hidden structure in composite numbers.

Triangular numbers, Fibonacci numbers, and slightly altered square sequences have been previously studied in the literature as paths toward structured factorizations. This work extends such explorations by formalizing a broader class of sequence-based transformations. In this context, we replace the traditional notion of *congruence of squares* with a more

general concept: the *congruence of sequence*, where elements transformed through the same functional form preserve a congruence-like behavior that enables factorization.

Related Work

This research complements previous studies in sequence-based factorization. Notably, Samojluk [1] explored the hidden structure of triangular numbers and their immediate application to factorization, offering geometric insights and pattern-driven methods that yield divisors with high computational efficiency. Similarly, Wibowo [2] introduced the concept of Fermat-d sequences derived from iterations of the classical Fermat factorization method, showing that these sequences produce interesting residue structures and pseudo-random jumps within arithmetic progressions.

Although our approach does not directly adopt their optimization strategies or matrix interpretations, it aligns philosophically with the idea that certain structured sequences, such as triangular numbers, Fibonacci sequences, and shifted square sequences, can embed hidden factorization properties. These studies can be seen as a slice of a broader emerging framework that includes our proposed notion of *congruence of sequence*, which generalizes the classical congruence of squares to more abstract, transformation-based structures.

This paper does not claim an advantage over well-established factorization methods such as the Quadratic Sieve or the General Number Field Sieve, but aims to enrich the landscape by uncovering latent algebraic relationships within sequences and their transformed outputs.

2 Sequence-Based Transformations

Let $f : \mathbb{Z} \to \mathbb{Z}$ be a transformation function such that for some inputs $x, y \in \mathbb{Z}$, $f(x)^2 - f(y)^2 = N$. We define such a transformation f based on structured sequences, for example:

- **Linear sequences:** $f(n) = kn + m$
- **Polygonal number roots:** Using the inverse of the general formula for polygonal numbers
- **Composite sequence transformations:** $f(n) = \sqrt{CMn + A^2}$, where $C, M, A \in \mathbb{Z}$

The key is that the values $f(x)$ and $f(y)$ are not arbitrary—they belong to the same transformation rule, and therefore preserve a structured relationship that manifests in the difference of their squares.

Importantly, it is often the *index* of the sequence values (i.e., the original values x and y) that propagate structurally across the transformation, in tandem with the multiplying constants in the transformation function. This propagation reflects a deeper, index-driven coherence in the behavior of transformational sequences.

3 Recasting the Identity

Given two sequence-transformed integers $a = f(x)$, $b = f(y)$, the identity becomes:

$$N = a^2 - b^2 = (a + b)(a - b)$$

This retains the algebraic structure of the classical identity but expands the origin of a and b from static values to dynamic outputs of sequence transformations. In practical terms, this means that for a given N, we may discover a and b through indirect but predictable pathways rooted in number-theoretic structure.

4 Applications to Factorization

While this paper does not explore optimization algorithms or search techniques, the transformation framework is a powerful conceptual tool. It allows the reconstruction of candidates a and b from a known N by applying sequence-based filters and checking for square differences. If a and b yield a valid difference, their sum and difference can be used in the classic fashion:

$$\gcd(a + b, N) \text{ or } \gcd(a - b, N)$$

To potentially produce non-trivial factors of N.

5 Conclusion

Transformation of integer sequences into perfect squares generalizes the identity $a^2 - b^2 = (a + b)(a - b)$ and reveals new avenues for theoretical and applied number theory. This framework encourages future work in the selection and generation of sequences that maximize the efficiency of such transformations and their algebraic properties.

References

[1] A. Samojluk, *About Special Properties of the Hidden Structure of Triangular Numbers for Immediate Factorization*, Technical Sciences, vol. 25, pp. 35–57, 2022.

[2] R. W. Wibowo, *Introducing Fermat Sequences*, Journal of Physics: Conference Series, vol. 1245, 012048, 2019. DOI: 10.1088/1742-6596/1245/1/012048.