SCIENCE SET
OPEN ACCESS PUBLISHERS

ISSN: 3067-8307
Research Article

World Journal of Applied Mathematics and Statistics

Homotopy Type Theory Finitist Foundation for Quantum Computing

Ed Gerck

781 Washington St. #3423, Sonora, CA 95370

[*]**Corresponding author:** Ed Gerck, 781 Washington St. #3423, Sonora, CA 95370.

Submitted: 16 December 2025 **Accepted:** 22 December 2025 **Published:** 29 December 2025

https://doi.org/10.63620/MKWJAMS.2025.1029

Citation: *Gerck, E.(2025). Homotopy Type Theory Finitist Foundation for Quantum Computing. Wor Jour of Appl Math and Sta, 1(4), 01-08.*

Abstract

The core intellectual problem in this work is the perceived disconnect between measured discrete physical reality and theoretical, continuous mathematical models of computation. This goes beyond a quantum ontology, addressing the computability of the diagonal of a unity square (√2) and the area of the unit circle (π). The proposed solution is — jointly, a finitist, integer-based constructive framework via Homotopy Type Theory (HoTT), as HoTT is inherently about structure and identity. The main experimental conjectures are two new paradigms: the Logically Decidable (LD), focusing on exact logic, and the Fast Calculation (FC), concerning the exact representation of irrationals; offering a potential to model quantum phenomena based in algebra, material-free. We estimate, in our finitist model, to reduce uncertainty from 2048 binary bits to about 112 binary bits in RSA-2048.

Keywords: Quantum Computing, Irrational Numbers, ZKP.

Introduction

Computation has carried, for centuries, a deep, albeit becoming more and more well-known, contradiction with the physical world — which is its inescapable ontology. The physical world is, undoubtedly now in the 21st century, discrete and quantized, in every known creation or measurement.

Quantum physics shows this conflict, at every scale. Even macroscopically (e.g., the 2025 Nobel prize in physics, as well-known, where John Clarke, Michel H. Devoret, and John M. Martinis, were recognized for their work on macroscopic quantum mechanical tunneling and energy quantization in an electric circuit).

Yet the prevailing computing and mathematical framework, and AI training, are still constructed from infinities in computation, real numbers that cannot be written entirely, completed processes that cannot be executed, infinitesimals that "disappear" in endless subdivisions below any possible particle scale, and are based on the well-known Weierstrass limit -- that presupposes continuity -- but cannot be achieved in any observations and any physical or computational reality.

We suggest that several objects exist only inside current mathematics itself — based on unverified, even though peer-defined by choice, but not by measurement, not by computation, and create well-known, long-standing conflicts.

This work assumes familiarity with foundational logic, type theory, and quantum computation. We argue that the future of computation, to focus on this area, lies not in ignoring, extending or “justifying“ by choice this supposed continuum, but in replacing it entirely by an experimental, measured reality in the 21st century — as ontologically measured and modeled.

The foundation of computation must, in this view, eventually become finite, computable, and algebraic. There is no other option, we suggest in this work and in many publications, favorable and unfavorable, by us and others [1-25].

This work is organized as follows. Section (2.1) proposes definitions to be used hereafter. Section (2.2) proposes the property of propositions that are Logically Decidable (LD). Latent in the proposed solution, LD is an example of hard to find properties albeit straight-forward to verify. After Section (2.2), we use Homotopy Type Theory (HoTT) [1], which was advanced by the well-known Omar Khayyam who declared “there is no difference between algebra and geometry”. Section (2.3) defines the property of Fast Computation (FC) and suggests some examples of fast computation with infinite sums and a reexamination of irrational numbers Sections (2.4-6) propose a material-free model of quantum computation (MFQC), hidden in the algebraic foundation of integers but easy to verify. Section (2.6.6) introduces the new computation system that is grounded on the claims of Ses.(2.1-6), founded on algebra as a constructive, integer finitist framework, defined on finite HoTT. We present this experimental conjecture to be evaluated by the readers, and hopefully it can make Mathematics and Physics work better together.

Methods

HoTT offers a new, alternative foundation for mathematics compared to traditional ZF and ZFC set theories. HoTT goes beyond simple equivalence— and offers new computational pathways that are currently difficult to find. HoTT, also known as Univalent Foundations, is a new foundational system for mathematics developed by Vladimir Voevodsky, with consequences declared by Omar Khayyam, uses type theory with the Univalence Axiom, which states that isomorphic types are equal. Identity between terms corresponds to equality (as known before HoTT) and also to paths between points, with univalence equating said identity in terms of equivalent spaces. This makes the formal system invariant under equivalences of mathematical structures in different spaces and allows different, but equivalent, approaches to be considered at the same time. HoTT is used only after Sec. (2.2).

Intrasubjective definitions of numbers and an objective definition of finitist integers follow finite HoTT, allowing mathematics to coherently represent different views.

Definitions

A number is an abstract mathematical object, and is intrasubjective. But numbers are communicated and computed through concrete, objective symbols.

The HoTT contribution, specifically the Univalence Axiom, allows us to treat computationally equivalent representations of a number as identical, simplifying proof and search of abstract quantities. Semiotics studies this relationship, and may use trust to assign different meanings to the same literal syntax, or vice-versa, allowing meaning and syntax to be independent, which will be important in this work.

HoTT also provides a formal framework for treating different representations (like '1', '1.0', 'one') as equivalent paths to the same symbol, and vice-versa, as different symbols can be linked to the same representation — allowing intrasubjectivity on numbers.

Finitist Integers Definition: finitist integers are represented in a closed set as $\mathbb{Z}_n$ or, in an open set by the ordered pair ($\mathbb{Z}_n$, $\mathbb{Z}_n$ > 0). This is valid for an arbitrarily-long number n of digits in $\mathbb{Z}_n$.

This replaces the undefinable number corresponding to “infinity”. A finitist integer provides for modular arithmetic within $\mathbb{Z}_n$, in closed or open sets.

The new system is constructive, with no irrational numbers, mathematical real-numbers, complex numbers, p-adic numbers, or the Axiom of Choice.

Logically Decidable (LD)

Because every statement in this system boils down to checking all elements of a finite type (in a finite number of cases), every well-formed statement is constructed to be logically decidable.

Those elements that are not decidable are not relevant, so nothing is lost by rejecting infinity as not reachable. LD is not restrictive, but allows the unconcerned use of logic albeit not of infinite sets. One can always write an algorithm that will definitively say true or false in a finite amount of time.

By forgoing infinite sets and unbounded recursion, the finitist framework ensures that any constructivist (well-formed) statement within the system is logically decidable (LD), provably true or false.

The crucial point is our rejection of the infinite set $\mathbb{Z}$, without reducing the application of logic itself — since the infinite set $\mathbb{Z}$, in this view, is what causes undecidability.

We gain decidability by imposing a finite bound. We suggest that the Gödel’s uncertainties demonstrate that the source of formal undecidability in Gödel's theorems is tied to the assumption of infinite sets (like $\mathbb{Z}$) or unbounded recursion; a rigorously finitist system regains decidability and does not limit the use of logic.

In summary: statements are decidable in LD because we admit only decidable statements; the rest are not LD. LD is a constructive set.

Otherwise, the well-known Gödel's theorems apply.

LD has significant implications for the automation and objective verification of formal proofs by any independent party, which was attempted by Voevodsky, and is presented in Sec.(2.3).

Gödel's Theorems: Structural Diagnosis in the Finitist Context

To be clear, the groundbreaking work of Kurt Gödel established two incompleteness theorems.

In the context of the LD paradigm, the conventional interpretation of both Gödel's theorems is fully accepted by LD, but their source is proposed not to be due to logic:

- **Proposed Source is the Unbounded:** Formal systems powerful enough to contain arithmetic (like Peano Arithmetic) necessarily rely on the existence of the infinite set of integers $\mathbb{Z}$ and/or unbounded recursion (the ability to repeat an operation indefinitely).
- **The Fatal Link:** The structural power needed to encode self-referential statements (the basis of the Gödel sentence) is intimately tied to this assumption of unboundedness or infinity. When one formalizes arithmetic over an infinite domain, one inevitably introduces the possibility of statements that refer to the entire set, leading to the necessary existence of formally undecidable propositions.

The Finitist Proposed Solution: Decidability Regained

The LD paradigm proposes that by adopting a strictly finitist framework based on the set of arbitrarily-long integers $\mathbb{Z}_n$, one removes the structural precondition for Gödelian undecidability, without losing anything decidable:

- **Finite Boundaries:** By imposing a finite but arbitrarily-long bound on the scope of all objects and computations, eliminating the use of the infinite set $\mathbb{Z}$.

- **Decidability is Guaranteed:** Because every statement within the LD system is ultimately reduced to checking a finite number of elements of a finite type, the system is trivially decidable. We propose that this is not avoiding or reducing the power of logic; this is demonstrating that a system founded on “constructive, bounded principles” naturally bypasses the conditions that lead to formal incompleteness.

Therefore, the LD paradigm views Gödel's theorems not as “flawed”, or as “a fundamental limitation of all formal reasoning”, but as a specific structural limitation imposed by the use of infinite sets and recursion in traditional set theory foundations.

Fast Calculation (FC)

Here, we suggest some LD reasoning with uncertainties, such as conventional irrational numbers, allowing fast calculation with infinite sums in products, arriving at $\mathbb{Z}_n$ -- an exact value.

The standard equality of rationals is seen as an application of univalence, linking the space of the set $\mathbb{Z}_n$ with all the Rationals (set Q) as the pair ($\mathbb{Z}_n$, $\mathbb{Z}_n > 0$), and where every member of the set $\mathbb{Z}_n$ is a Rational with denominator equal to 1.

If two finitist integers are not divisible, they can be identical if their criss-cross product is equal (e.g., ⅘ = 24/30), considering the Univalence Axiom, where the standard equality of Rationals is seen as an application of Univalence. This is an example of how we can define and find latent algebraic dependencies that are logically decidable (LD).

Computationally, the system enables a fast calculation (FC) paradigm. FC is driven by the efficiency of HoTT in finding more paths among different spaces, using modular arithmetic, and what we term "latent algebraic dependencies": hidden integer relations and structural paths that are computationally difficult to discover but straightforward to verify once found — like for irrational numbers — see Section (2.3.1). The principles of FC further empower cryptographic protocols, including efficient Zero-Knowledge Proofs (ZKPs) due to exact algebraic witnesses, that are LD — see Sec.(2.2).

A cornerstone of our approach is its constructive nature, which logically obviates the need for the non-constructive Axiom of Choice.

Quantities such as π, √2, are imagined, abstract modeling tools, symbolic rather than physically instantiated entities, that would need unphysical infinite information. As symbols, on the other hand, they face the insurmountable Problem of Closure [3] — the inability to operate between rationals and irrationals in a computable way.

Use of HoTT to re-examine irrational numbers

Our entire approach is motivated by the philosophical objection that quantities such as √2 and π cannot be used in computation, numerically. Here, they are not treated as abstract modeling tools or requiring unphysical, infinite information, thus facing the insurmountable Problem of Closure [3]. We reject the necessity of these non-constructive entities, considering them scaffolding. Instead, our goal is to establish the ability to operate between rationals and conventional "irrational numbers" in a demonstrably computable and decidable way within our finitist framework. We achieve this by redefining the meaning of an irrational number from an infinite sequence to an “algebraic and structural type” over the set of arbitrarily-large integers $\mathbb{Z}_n$, using HoTT.

We propose that every conventional "irrational number" is best understood not as a number itself, but as the limit of an optimal, structurally defined sequence of rationals. This allows us to leverage the well-known Hurwitz Theorem to define an optimal bound as an open set limiting how well that irrational number can be approximated by rational numbers. Crucially, the ordered pair ($\mathbb{Z}_n$, $\mathbb{Z}_n > 0$) (representing a fraction/rational) defines, under one open set element (e.g., √2), each approximation of that limit.

This methodology forms the core of the Fast Calculation (FC) paradigm: it enables calculation with products involving these types by treating the irrational as HoTT-equivalent to pairs of finitist integers at any desired precision. The Univalence Axiom provides the formal rigor for this equivalence, establishing a path between the infinite symbol and the finitist algebraic structure. This allows us to perform exact number-theoretic calculations, such as √2.√2 = 2, without appeal to limits or non-constructive number systems.

FC Examples

Our goal is to have the ability to operate between rationals and irrationals in a computable way. We limit each conventional “irrational number“ by the well-known optimal bound as an open set limiting how well that irrational number can be approximated by rational numbers, which are given by the well-known sequences from the Hurwitz Theorem. For an arbitrarily-long number of terms, the pair ($\mathbb{Z}_n$, $\mathbb{Z}_n > 0$) (as a fraction), thus, defines under one open set element (i.e., √2) each approximation of it. This enables calculation with product of irrational numbers using the finitist set $\mathbb{Z}_n$ in a
HoTT equivalence, as follows.

This exemplifies also how to form equivalent types, including how recognizing a type isomorphism via univalence simplifies a computation or proof, such as with conventional irrational numbers, which is seen as equivalent to pairs of ($\mathbb{Z}_n$, $\mathbb{Z}_n > 0$) at any desired precision (cf. Hurwitz Theorem).

This allows exact calculations with conventional irrational numbers using arbitrarily-large integers in $\mathbb{Z}_n$ linked to all the Rationals as the pair ($\mathbb{Z}_n$, $\mathbb{Z}_n > 0$).

Consider the arithmetic identity in $\mathbb{Z}_n$:

$$\sqrt{2} * \sqrt{2} = \sqrt{4} = 2 \tag{1}$$

where an integer, finite, precise number is exactly the product of two supposedly infinite irrational numbers, a number that could not be counted.

This identity is exact, number theoretic, and requires no appeal to limits, irrational numbers, or real-number constructions.

In a finitist rational framework, √2 is not an “irrational magnitude” but a formal algebraic symbol representing a ratio constrained by the equation x^2 - 2=0. Its meaning is entirely captured by algebraic relations among arbitrary-length integers, not by a fuzzy expression, an infinite decimal, or an expansion without end.

Thus, in algebraic radicals, the algebraic structure provides exactness where numerical computation cannot, as it must remain in a neighborhood larger than zero.

This is consistent with the broader finitist view that the reals (and irrationals) are a scaffolding rather than foundational; all meaningful operations can be expressed via algebra over finitist integers, including ratios thereof.

This has the potential to change mathematics and physics, to find exact results that can be calculated in a finitist view within a zero neighborhood.

Eq.(1) shows that the square root function is an exact operation, and can be counted, therefore. The phrase "numbers that cannot be counted" for irrational numbers isn't a precise mathematical definition, but it hints at only one space where they exist. We treat this space, though, not as the only space or as symbols, but as pairs (i.e., fractions) of finitist integers where denominators are non-zero: ($\mathbb{Z}_n$, $\mathbb{Z}_n > 0$), creating an open set bounded by that conventional “irrational number”.

Eq.(2) follows:

$$\sqrt{n} * \sqrt{n} = n \tag{2}$$

for all n > 0, any arbitrarily-large integer in $\mathbb{Z}_n > 0$. One can also write:

$$\sqrt{\pi} * \sqrt{\pi} = \pi \tag{3}$$

where we find a square with the exact area as the unit circle (with unit radius), showing that π is not actually “irrational” geometrically and can be exactly divided in two or more parts. In numerical terms, an irrational number is formally defined as a number that “cannot be expressed as a simple fraction”. Not as a non-equality definition: “not a rational number”.

Conventionally, the numerical value of π is approximately $3.1415926535... and its expansion is non-terminating and non-repeating. Its irrationality has been rigorously proven (first by Johann Heinrich Lambert in 1761).

Under HoTT, however, geometry can be used to define identity by isomorphism— the Univalent Axiom. Then, Eq.(3) defines a path where a conventional “irrational” can be divided exactly in two parts — allowing one (in this view) to numerically calculate in numbers with a conventional “irrational” using a conventional “irrational” operation.

This sidesteps its inability to be represented by a fraction of integers, or its geometric representation (disputed by the ancient Greeks), or its ability to be factored. We refer to Sec.(2.3), considering the Univalence Axiom, where the standard equality of rationals was seen as an application of univalence. This is another example of how we can define and find latent algebraic dependencies that are logically decidable (LD).

Thus, we are suggesting the idea that π, while conventionally called "irrational", is structurally exact and constructively representable in the proposed finitist framework (e.g., as the result of a geometric construction or as a path in a HoTT structure following Voevodsky, much like using geometry to solve an algebra problem, by Omar Khayyam). In this context, Eq.(3) criticizes the philosophical implications of the term "irrationality" as applied to physically relevant constants (e.g., how can a quantity that can be measured in any precision, be non-existent?), suggesting that the "disconnect" noted in the abstract is also present in how one classifies numbers — which presently conflicts Mathematics (as a product of mind, necessarily intersubjective) with Physics (as a model of Nature, necessarily objective).

In summary, because π is seen in nature (Physics), it must be either a quantum or have a representation that can be divided. Physics does not support the former, as seen in Astronomy with orbits, and the latter is not allowed by Mathematics. This an example of the perceived “disconnect” this proposal is attempting to solve using the finitist HoTT framework. The FC paradigm allows for the "exact representation of irrationals", in algebra and numerically, within a finitist integer-based system, supporting their exact multiplication and division in Mathematics.

Material-Free Quantum Computation (MFQC)

We demonstrate next in Section (2.5), that this finitist algebraic foundation is sufficient to model the core operational principles of quantum computation—such as superposition, entanglement, interference, and quantum jumps.

This is done without recourse to physical or logical qubits, materials, or time. This "material-free" model of quantum computing (MFQC) captures quantum computation as a consequence of finitist integer algebra and HoTT isomorphisms.

The MFQC, with no quantum-specific hardware, is detailed in Section (2.5), potentially offering a new, non-Turing, non-sequential, discrete, and purely mathematical foundation for the theory of computation.

MFQC

In 2023, we proved that the differentiation of discontinuous functions exists [3], allowing any continuous and discontinuous function1 be differentiated exactly, and integrated, finding new solutions to the Schrödinger equation — including prime numbers or step functions.

Our earlier work [2-4] demonstrated that, computationally, using the Schrödinger equation2, the distinctions between the sets C, R, and Q disappear in a bounded set to 20 decimal digits, as usually dominated by experimental precision. The results show, within numeric terms, that observable quantities such as eigenvalues, for different potential functions, all resolve exactly to $\mathbb{Z}_n$ (including irrational numbers), with no complex value, and none contradicts any established results up to said 20 decimal digits. We mean that for the specific, discrete computational problem of solving the Schrödinger equation for many potentials, where our results are always rational, in a bounded set, linking the space of $\mathbb{Z}_n$ with the set of all well-known physical solutions in that model, and pointing to new ones — at any finite precision.

The claim of using irrational numbers, e.g. π or √2, is perceived as a scaffolding. Because the ratio of a circumference to its diameter is measurable, or the diagonal of a unit square, they must reflect a rational number --- at whatever precision (i.e., see Hurwitz Theorem).

The same happens with complex numbers in quantum mechanics. Although complex numbers have been used to model reactive angles in macroscopic electric circuits, superposition, interference, and entanglement in both macroscopic and microscopic examples, they are not needed computationally [2-4], enabling what we call Material-Free Quantum Computing method (MFQC).

Complex numbers have been used conventionally to model the dynamics of quantum systems (e.g., unitary evolution), but the quantum states themselves never assume a complex or real value with infinite information. We provide in [2, 3] concrete examples that solutions to the Schrödinger's equation (in any form3) can be represented exactly, or equivalently to conventional methods when not exactly solvable.

We have seen heretofore that the structural integrity of the finitist integer set $\mathbb{Z}_n$ provides a natural framework for modeling physical reality's discrete nature, moving beyond continuous, non-constructive mathematical models. This framework now suggests an inherent non-Turing model of computation rooted purely in algebra.

We propose that a "quantum jump" can be computationally represented as a non-sequential transition between two prime numbers, C and D, defined by the exact algebraic identity:

$$D = C + 2n, \text{ where the prime number } C>2, n \text{ in } \mathbb{Z}_n \tag{4}$$

This formulation bypasses the need for sequential iteration over intermediate composite numbers. The term 2n represents the structural path between the primes within the $\mathbb{Z}_n$ algebra. This capacity for non-sequential reach has immediate, high-impact implications for conventional cryptography, suggesting that the computational difficulty relied upon by methods like RSA—which assume a sequential search space—is entirely obviated.

Furthermore, the set $\mathbb{Z}_n$ structurally exhibits four properties that are foundational to the quantum realm:

1. **Discrete, Isolated, and Rigorous:** $\mathbb{Z}_n$ is inherently discrete; any two values are structurally separated and non-contacting. This separation guarantees the necessary rigorous (exact) nature of each integer, representing a point of dimension zero.
2. **Indistinguishability:** $\mathbb{Z}_n$ supports the type-theoretic principle of indistinguishability. For instance, the number '11' can be treated as a singular, quantum type, not as a composite aggregation of two separate instances of the numeral '1'. This structural unity reflects the analogous quantum principle of identical particle indistinguishability, in the numeral '1' in '11'.

These four quantum-like properties have been published [3] to explain calculus "without ghosts"4 exactly, using fractions, the differentiation of prime numbers, and non-sequential factorization of large numbers.

We experimentally conjecture that phenomena such as superposition and entanglement are direct structural consequences of this inherent "Discrete, Isolated, Rigorous, and non-local connectivity" and the many available structural paths (multiple possible n values: 2n, 4n, …) between elements in the $\mathbb{Z}_n$ algebra.

The number D is always a prime number, though not always isolated. For the first 100 prime numbers, n in Eq.(2) is equal to 2 or 4.

HoTT and Finitist Model: Four "Toy-examples"
NOTE: The "starting point" is always below √N, where N is the given modulus. It represents the mid-point if both primes are equal, which is never the case. The method presented hereafter resembles the well-known "Fermat attack" on just the starting point, but we are looking for structural identity under HoTT, not only for magnitude identity.

As a first "toy-example", one can reach the prime number 86882443 in a jump by adding 86882414 to the prime number 29, non-sequentially. The neighboring numbers 86882447 and 86882441 are also prime, as expected where n in Eq.(2) is equal to 2 or 4. As the prime number increases, n in Eq.(2) can become quite large, as it is well-known.

Can N Become Predictable? We consider that in Sec.(2.5.1) for a suggested goal using identity under HoTT, not attainable under identity under magnitude.

As a second "toy-example", the largest number factored by a quantum computer using a general method is 261980999226229 (a 48-bit number) = 15538213 * 16860433, as it is well-known. This was achieved by converting the problem to a lattice problem solved with the Quantum Approximate Optimization Algorithm (QAOA) on a superconducting quantum computer with 10 qubits. The starting point in our method was 16185827 or below. We obtained 15538213 * 16860433, just 647616 digits away from the lowest prime number -- in a non-sequential computation first to 16185829. The path was further reduced by other optimizations. We needed fractions of a second, in a commercial cellphone of today. The reader can repeat for independent verification.

As a third "toy-example", we partially factored the MSB 367 decimal digits of RSA-2048 with 617 decimal digits. The starting point was

5019552617082312595172503983807165462898614432824
8462229237779798019330693202048292023548683783342
5207634475741706163699157605252203969037895835866
7936661489786744680588457581239907305052289446427
4593752537007059218713557754906351645416162392926
8486240829374671662765637370473454653729941479883

[1] And distributions.
[2] Traditionally using Hilbert spaces, with complex numbers.
[3] The observation is that there is an isomorphism between the proof systems and the models of computation, known as the Curry-Howard relationship and defining structural logic (computers-as-proof).

20622750463093 in fractions a second in a Linux computer using the noncommercial POSIX software bc. As a fourth “toy-example” we used the well-known RSA-576 . Its value is: 188198 8129206079638386972394616504398071635633794173827007 633564229888597152346654853190606065047 4 304531738 801130339671619969232120573403187955065699622130516 8759307650257059. On December 3, 2003, a team of researchers in Germany and several other countries reported a successful factorization of the challenge number RSA-576. According to the announcement by J. Franke: The factors [verified by RSA Laboratories] are: 398075086424064937397125500550386491 199064362342526708406385189575946388957261768583317 and 472772146107435302536223071973048224632914695302 097116459852171130520711256363590397527.

Our starting point was 433818871097844202389623285336968 290605469456301558930293445695571862781832679867424803, directly in a non-sequential jump. We obtain the same number as RSA-576 and the same well-known prime numbers, in days in a Linux computer using the language C with arbitrary-long integers (measured by our team to be 36x times faster than using bc).

The four "toy-examples" validate this approach, under different forms, particularly the last one.

Recall how Shor's algorithm works, also not on magnitude but on structure. It reduces factoring to period finding. So, for a given N = p*q, choose a random number a, co-prime to N, then find the period r in Eq.(5):

$$f(x) = a^x \mod N \tag{5}$$

Eq.(5) requires quantum hardware for speed. If r is even, then (a(r/2) - 1)(a(r/2) + 1) ≡ 0 mod N. Then gcd(a(r/2) -1, N) might give a factor. Shor’s algorithm factors N=p*q by finding the period of f(x), assumed unique for p and q. This is well-known to work for a small modulus, such as 21. However, as of 2025, even the largest quantum computers lack the necessary number of stable, error-corrected qubits to run Shor's algorithm reliably for numbers like 75. While simple numbers like 15 and 21 have been factored in lab demonstrations, these often require specific "tricks" or a high number of attempts due to noise and errors.

Speed is the next factor to verify in Shor’s algorithm. Here, we use HoTT. Examining N = p*q, one sees two spaces that are considered equal to any N, p, q in $\mathbb{Z}_n$. The space of magnitudes with N, and the space of products of prime numbers, with p and q. Thus, when one divides N by a number, even though not recognizing it, it is the same as dividing p or q by that number. Trivially, if $p < \sqrt{N}$ then $q > \sqrt{N}$ or vice-versa. We know by FC that the √ is an exact operation under FC, even though not conventionally calculable.

Drawing on HoTT, we propose a foundational shift in how the RSA modulus N is understood. Rather than treating it as a mere magnitude—a very large integer to be factored—we redefine N as an "algebraic and structural type" over the set of arbitrarily-large integers $\mathbb{Z}_n$. Note that $\mathbb{Z}_n$ denotes the finitist type of integers bounded but with an arbitrarily-extendable length, not only integers modulo n in $\mathbb{Z}$.

Here, N is not defined by its size but as a formal algebraic symbol constrained by Gauss’s fundamental relation N = p*q. Its semantic content is entirely derived from the algebraic relationships it participates among arbitrary-length integers.

This perspective allows us to exploit the structural paths (identifications) available in HoTT. By doing so, we can identify latent algebraic dependencies between N and its prime factors. This identification non-sequentially collapses the search space from a vast set of integers to a specific structural type—or a constrained neighborhood within the type of integers—that corresponds to a complexity far below its nominal bit-length.

For instance, prime numbers of a given length are not merely arbitrarily large integers; they occupy an increasingly sparse and structured subspace as their magnitude grows; in other words, they form a proper, definable subtype characterized by arithmetic constraints that are invariant under length extension. By leveraging this inherent structure within the HoTT framework, the search can be constrained much more effectively than by sequential magnitude-based enumeration.

A further significant reduction is pragmatically attainable by considering the established lower bounds for prime sizes in cryptography. To guard against classical computational threats, primes are practically never chosen below approximately 400 bits. This constraint serves as a reduction of the search type rather than as an attack in itself.

In our finitist algebraic model (not in the classical RAM or oracle model), the residual uncertainty is comparable to 2^{112}.

Consequently, this algebraic and finitist reframing transforms the factorization problem. Within this structural and finitist computational model, the remaining uncertainty is dramatically reduced relative to magnitude-based estimates, reaching levels that may be incompatible with standard security assumptions for RSA-2048.

Formally, this corresponds to restricting the factorization problem to a dependent subtype induced by the path, rather than a more onerous external enumeration over all magnitudes in $\mathbb{Z}$.

This approach allows us to begin the search from a highly constrained hypothesis for the smaller prime factor, p, fundamentally altering the landscape of the integer factorization problem. The numeric strategy is now clear: for RSA-2048 [19], one can reduce the problem, non-sequentially, to 1024 bits (or less) and start near a hypothesis for p (the smaller prime number). The computation can be fully parallelized across many machines. Well-known estimates from security experts suggest a nation-state might be able to break a 1024-bit RSA key in a few weeks or months using massive, dedicated computing resources (e.g., hundreds of thousands of core-years).

However, this is outside the capabilities of typical users or even academic research teams.

Computational advantage is gained through mathematical in-

[4] *Infinitesimals and Weierstrass continuity.*

sight. This shortens the well-known expectation of trillions of years for any RSA-2048 (and that was the reason to deprecate RSA-1024) to reasonably less than one year or two today, without depending on quantum hardware.

This Model: MFQC

Both classical and quantum computers operate using the binary set B = {0,1} and its extensions in binary as Bn = {0, 1, 01, 10, 11, 001, 010, …}.

Classical computers implement operations through modular arithmetic using the set B, while quantum systems, though often described using complex amplitudes for an imagined (i.e., postulated) state evolution, produce outputs exclusively as discrete binary values in set B.

Despite theoretical models invoking continuous wavefunctions, fluids, real-numbers and complex-valued amplitudes, classical and quantum computers interact with the physical world through discrete inputs and outputs.

Every observable outcome---whether the result of a classical algorithm or a quantum measurement--- is encoded in discrete binary form. This reinforces the view that physical or software computation, at its core, is grounded in finite, discrete processes, see Sec.(1).

The crucial point is that all inputs, outputs, and computational processes are fundamentally discrete, and can be digital using the set B.

Moreover, such computational processes are largely independent of external physical variables such as temperature, further emphasizing their abstraction from phenomena, and from any potential continuity constraint.

We now define a quantum computational model (MFQC) based entirely on finitist integers and their pairs (i.e., fractions) of finitist integers where denominators are non-zero: ($\mathbb{Z}_n$, $\mathbb{Z}_n > 0$), representing respectively closed and open sets — without any materials.

Rational State Space

The MFQC replaces complex Hilbert spaces with finitist or rational spaces.

Measurements and Eigenvalues

Measurements of pure states in quantum mechanics are well-known to be deterministic. Measurement is modeled by deterministic logic based on eigenvalues of operators, in MFQC. Superposition, entanglement, and interference are represented, as well-known. These results suggest that quantum computing can be LD, exact, computationally.

Shor's Algorithm and ISA

Based on the foregoing, we improved the Shor's algorithm with ISA (Improved Shor's Algorithm).

ISA uses only algebra of finitist integers in period finding using the square-root, not complex numbers or a Hilbert space (see Footnote 1).

Numerical Results

To numerically break a RSA modulus, one needs to find the prime numbers, p and q. They surely exist and are unique, cf. Gauss, see Sec.(2.3.2). They are maximum when RSA uses two prime numbers.

When we reach 153 decimal digits or more, we can extend these results, e.g., using the well-known Coppersmith's method (i.e., applying algebraic LLL) where factoring of more than one-quarter of the MSBs of p or q in N=p*q, enables factoring N, verifiable trivially by any independent party, in falsifiable results using only the algebra of integers — for cybersecurity, in a ZKP. Using the same method, we can factor RSA with 2048 or more binary digits, in a well-formed, finitist process using only the algebra of integers, and the MFQC to reduce from 2048 bits to about 112 bits in our finitist model, see Sec.(2.5.1).

Conclusion

The LD and FC paradigms, with HoTT. were crucial in equating division of a magnitude N with the factoring of its primes p*q before the shielding of the multiplication — i.e., giving us direct access to search for p and q in $\mathbb{Z}_n$.

The MFQC was important in allowing a non-sequential quantum jump to approach the upper bound of the lowest prime number, directly skipping 1024 bytes. We estimate, in our finitist model, to reduce uncertainty from 2048 binary bits to about 112 binary bits in RSA-2048.

We are hopeful that future versions of this work will use a ZKP to securely release the prime factors of N.

Funding

This research received external funding from Network Manifold Associates, Inc. (NMA), Safevote, Inc, and Planalto Research. The author declares no conflict of interest. This result is public and online, without material nonpublic information here.

Acknowledgments

The author is indebted to the work of late Mādhava of Sangamagrāma, NMA early investors; Don Sawtelle at Planalto Research in C coding, and five anonymous reviewers.

References

1. Rijke, E. (2025, November). Introduction to homotopy type theory. arXiv. https://arxiv.org/abs/2212.11082
2. Gerck, E. (2023). Algorithms for quantum computation: Derivatives of discontinuous functions. Mathematics, 11, 68. https://doi.org/10.3390/math11010068
3. Gerck, E. (2023). Quantum computing arrives. Mathematical Techniques in Computational Mathematics, 2(8), 356–358.
4. Gerck, E. (2021). On the physical representation of quantum systems. Computational Nanotechnology, 8(3), 13–18. https://doi.org/10.33693/2313-223X-2021-8-3-13-18
5. Vandersypen, L. M., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., & Chuang, I. L. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 414(6866), 883–887. https://doi.org/10.1038/414883a
6. Martin-Lopez, E., Laing, A., Lawson, T., Alvarez, R., Zhou,

X. Q., & O'Brien, J. L. (2012). Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nature Photonics, 6(11), 773–776. https://doi.org/10.1038/nphoton.2012.259

7. Bocharov, A., Roetteler, M., & Svore, K. M. (2017). Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures. Physical Review A, 96, 012306. https://doi.org/10.1103/PhysRevA.96.012306
8. Smolin, J. A., Smith, G., & Vargo, A. (2013). Oversimplifying quantum factoring. Nature, 499, 163–165. https://doi.org/10.1038/499163a
9. Dattani, N. S., & Bryans, N. (2014). Quantum factorization of 56153 with only 4 qubits (arXiv:1411.6758v3). arXiv. https://arxiv.org/abs/1411.6758
10. Yan, S. Y. (2015). Quantum algorithms for integer factorization. In Quantum computational number theory (pp. 59–119). Springer. https://doi.org/10.1007/978-3-319-13039-7_3
11. Peng, X., Liao, Z., Xu, N., Qin, G., Zhou, X., Suter, D., & Du, J. (2008). Quantum adiabatic algorithm for factorization and its experimental implementation. Physical Review Letters, 101(22), 220405. https://doi.org/10.1103/PhysRevLett.101.220405
12. Burges, C. J. C. (2002). Factoring as optimization (MSR-TR-2002-200). Microsoft Research.
13. Wang, B., Yang, X., & Zhang, D. (2022). Research on quantum annealing integer factorization based on different columns. Frontiers in Physics, 10, 914578. https://doi.org/10.3389/fphy.2022.914578
14. Dridi, R., & Alghassi, H. (2017). Prime factorization using quantum annealing and computational geometry. Scientific Reports, 7, 43048. https://doi.org/10.1038/srep43048
15. Xu, N., Zhu, J., Lu, D., Zhou, X., Peng, X., & Du, J. (2012). Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system. Physical Review Letters, 108(13), 130501. https://doi.org/10.1103/PhysRevLett.108.130501
16. Li, Z., Dattani, N. S., Chen, X., Liu, X., Wang, H., Tanburn, R., … Du, J. (2017). High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311. arXiv. https://arxiv.org/abs/1706.08061
17. Xu, K., Xie, T., Li, Z., Xu, X., Wang, M., Ye, X., … Du, J. (2017). Experimental adiabatic quantum factorization under ambient conditions based on a solid-state single spin system. Physical Review Letters, 118(13), 130504. https://doi.org/10.1103/PhysRevLett.118.130504
18. Dhaulakhandi, R., Bikashi, K. B., & Seo, F. J. (2023). Factorization of large tetra and penta prime numbers on IBM quantum processor. arXiv. https://arxiv.org/abs/2304.04999
19. RSA Laboratories. (2006). RSA-2048 challenge. https://web.archive.org/web/20061210141333/http://www.rsasecurity.com/rsalabs/challenges/factoring/RSA-2048.txt
20. Herman, E., & Butler, A. (2023, April 3). Prosperity at risk: The quantum computer threat to the U.S. financial system. Hudson Institute. https://www.hudson.org/technology/prosperity-risk-quantum-computer-threat-us-financial-system
21. Gerck, E. (2021). Tri-state+ communication symmetry using the algebraic approach. Computational Nanotechnology, 8(3), 29–35. https://doi.org/10.33693/2313-223X-2021-8-3-29-35
22. Neppe, V. M., & Close, E. R. (2020). The Neppe–Close triadic dimensional vortical paradigm: An invited summary. International Journal of Physics Research and Applications, 3, 001–014.
23. Phillips, N. (2025). LinkedIn profile. https://www.linkedin.com/in/nigel-phillips-coder/
24. Wolf, C. G. (2025). Values of the fundamental physical constants. ResearchGate. https://www.researchgate.net/publication/368809501
25. Renou, M. O., Acín, A., & Navascués, M. (2025). Quantum physics falls apart without imaginary numbers. Scientific American. https://www.scientificamerican.com/article/quantum-physics-falls-apart-without-imaginary-numbers/
26. Gerck, E. (2025). Can quantum mechanics become computable? Toward a rational, finite, and deterministic framework for physical law. ResearchGate.