

Creative Commons Attribution 4.0 International (CC BY 4.0)

<https://creativecommons.org/licenses/by/4.0/>

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

New Proof of the recent Baseline Primality Conjecture

This paper was downloaded from TechRxiv (<https://www.techrxiv.org>).

LICENSE

CC BY 4.0

SUBMISSION DATE / POSTED DATE

07-12-2021 / 10-07-2023

CITATION

Phatak, Dhananjay (2021). New Proof of the recent Baseline Primality Conjecture. TechRxiv. Preprint.
<https://doi.org/10.36227/techrxiv.17139041.v2>

DOI

[10.36227/techrxiv.17139041.v2](https://doi.org/10.36227/techrxiv.17139041.v2)

New Proof of the recent Baseline Primality Conjecture

Dhananjay Phatak (phatak@umbc.edu)

CSEE Dept., UMBC, 1000 Hilltop Circle, Baltimore, MD 21250, U.S.A.

List of Revisions

2nd July 2021, December 2021,

Three major revisions in January 2022 based on the feedback from Professor Carl Pomerance [1, 2, 3] (see the [Acknowledgment](#) for details).

First Version of the new proof: 28th January 2023

Last revision: June 8, 2023.

ABSTRACT

This document presents a theoretical proof of the Baseline Primality Conjecture (BPC) that was recently unveiled in [4, Part I]. The BPC identifies a new small set of conditions that are sufficient to decide the primality of any input integer N under test (see [Section 2](#) for the exact statement of the BPC in the original form using algebraic integers; and [Section 3](#) for an equivalent polynomial domain reformulation).

The practical significance of the BPC is that it directly leads to ultra low complexity primality testing algorithms, wherein the number of bit-operations required is essentially a **quadratic** function of the bit-length of the input N [4]. More specifically, the Baseline Primality Result (BPR) demonstrates that after an/any integer in the closed interval $[2, N - 2]$ which is a Quadratic Non Residue (QNR) modulo- N is found; exactly 2 (Two, which is a small $O(1)$ constant, independent of the bit-length of the input N) specific modular exponentiations are sufficient to determine whether N is a composite or a prime.

The BPC was (and to this day continues to be) extensively tested numerically.¹

Additionally, theoretical proofs of the BPC for several specific forms of the input N were also presented in [4]. However, at the time of the original publication [4], we were not able to complete a general theoretical proof of the BPC that covered all possible cases (i.e., forms) of the input N .

A preliminary version of a general proof of the BPC was posted in the IEEE TechRxiv [5]. However, after the release of that document, the author solicited feedback from the renowned number theory expert Prof. Carl Pomerance in Jan. 2022. He pointed out a mistake [2] in that version of the proof (which appears in [5]). Since then, after more than an year of effort, a completely new proof has been developed in the period approximately from the 28th of January 2023 to the end of April 2023. To the best of our knowledge, this proof [6] is error free (and therefore will replace [5] in the near future.)

A concise presentation of that new theoretical proof is the main focus as well as the main new contribution of this article. An auxiliary contribution is a clear and precise explanation of the intuition behind our approach and the illustration of how it leads to the new theoretical results developed in [4].

¹ To date, no counter-example has been found.

§ Section 1 : Brief overview of our recent low complexity Primality Detection Algorithms

In a comprehensive set of 3 companion articles [4] that were recently published in the arXiv (rapid dissemination) archive; we unveiled new low complexity deterministic primality testing algorithms. As mentioned before, that document set includes three companion manuscripts/articles:

Part I covers the theory behind the methods, followed by specifications of the primality detection algorithms.

Part II (the second companion manuscript) presents extensive experimental (numerical) data to corroborate each of the algorithms and

Part III illustrates proofs of some of the theoretical results underlying the algorithms for some specific forms of the integer N , under test.

However, a complete theoretical proof covering all possible values of the input N eluded us at the time of the original publication. *Consequently, the main results in [4] had to be unveiled as “conjectures”.*

The “Baseline Primality Conjecture” is the first major conjecture introduced in [4, Part/Paper I, Section 2]. The BPC states that after a **Quadratic Non Residue (QNR) [7] value** $(q \bmod N)$ is found; only two (i.e., a small constant number of) modular exponentiation computations need be performed to decide the primality of N .

Further, it turns out that any value of q in the closed interval $[2, N - 2]$ works; there is no need to find “the smallest QNR modulo N ” (see [4], and the ensuing Sections in this article for details).

Consequently, after a QNR q is generated, the number of operations required is upper bounded by $O((\log N)^2 (\text{polylog}(\log N)))$, which is substantially lower than the complexity of other known methods (see “Section 5 in Part I” in [4] for details).

The only caveat is the requirement to generate a QNR value.

To that end, in [4, Part I, Section 5.4], it is demonstrated that it is trivial to generate a QNR modulo N in all cases except when $N \bmod 240 = 1$.

In other words,

an overwhelming majority = $\frac{119}{120} = 99.16\%$ of all odd integers N do not need an explicit search for a QNR.

Further, even when a search is needed, fast (low complexity) probabilistic algorithms exist to quickly generate a QNR value [4].

However, as of today, there is no known deterministic polynomial-complexity algorithm to generate a QNR value in every case [4].

Fortunately, we were able to circumvent that difficulty by developing methods that do not need the explicit numerical value of a quadratic (or higher order) non-residue modulo N (see Section 8 and onward in part I in [4]).

It turns out that any polynomial whose roots do not exist as modulo- N integers is sufficient ; there is no need to “solve that polynomial equation modulo- N ” and obtain the explicit value of the non-residue. In other words, there is no need to evaluate the exact numerical value of any of the roots of that polynomial. Thus, finding any polynomial equation that “implicitly” specifies non-residues as its roots is sufficient.

This fact ultimately led to the development of the Generalized Primality Conjectures (GPCs), that in turn led to fully deterministic primality testing algorithms that have the complexity of $O\left((\log N)^3 (\text{polylog}(\log N))\right)$ bit operations [4].

In this article, however, we do not consider those Generalized Primality Conjectures.

Likewise, we do not address any algorithmic or complexity attributes or explore close connections to other existing primality detection methods (for example, Sections 6 and 7 in Part I in [4] demonstrate close connections between primality tests based on the Baseline Primality Conjecture and the well known Miller-Rabin primality test. Fused algorithms that combine best attributes of both methods were also unveiled in [4]).

Rather, in this article, we narrowly focus only on the Baseline Primality Conjecture (which is the first out of several conjectures developed in [4]) and provide a theoretical proof of that result.

To that end, the next Section reproduces the Baseline Primality Conjecture in the original form [4] using the algebraic-integer \sqrt{q} .

Then, [Section 3](#) presents an equivalent formulation of the same result in the polynomial domain².

The following section (i.e., [Section 4](#)) presents a few well-known results that are used to prove the main result (i.e., the Baseline Primality Theorem).

Next, [Section 5](#) demonstrates the proof of the Baseline Primality Theorem.

The following section (i.e. [Section 6](#)) discusses the relation of our results to the state-of-the-art in Primality Testing and explains the intuition underlying all the new results; including all the results unveiled in [4]. We conclude with brief remarks in [Section 7](#).

As mentioned in the abstract, a preliminary version of the proof was posted in the IEEE TechRxiv [5]. However, after the release of that document, the author solicited feedback from Prof. Carl Pomerance (who is a renowned, leading researcher in computational number theory and allied areas). He pointed out a mistake [2] in that version of the proof (circa December 2021). That erroneous version [5]; as well as the original email message from Prof. Pomerance [2] that kindly and gently identifies the mistake in that document (i.e. ref. [5]), have both been made available publicly; please see references [2] and [5] for further details.

Since then, after more than an year of effort, a completely new proof has been developed in the time period approximately starting from the 28th of January 2023, until today.

To the best of our knowledge ; this new proof is error free.

A concise presentation of that new proof is the main focus of this document.

² This alternate polynomial domain reformulation also appears in the original document [4] in Part I, Section 3, Remark 3.2 on page number 20.

In summary, the new contributions of this article are:

- 1 The proof of the BPC which is the main focus
and
- 2 An auxiliary contribution : In [Section 6](#) ; we present a clear and precise explanation of the intuition underlying our approach and show how it leads to the new theoretical results in [\[4\]](#).

§ Section 2 : The original form of the conjecture using Algebraic Integers [\[4\]](#)

The Baseline Primality Conjecture (BPC) [\[4, Section 2, page no. 16 in Part/Article I\]](#) :

Given any positive integer N (to be tested for primality), suppose that we find some integer q , that together with N , satisfies the following conditions

C-1 : $N > 1$ is an odd integer and is not a perfect square of any other integer.

C-2 : The **Jacobi-Symbol** [\[8\]](#) of q w.r.t. $N \stackrel{\Delta}{=}^3 \mathbf{Jacobi_Symbol}(q, N) = -1$
 $\Rightarrow q$ is a **QNR** (Quadratic Non Residue [\[7\]](#)) modulo- N

Note that q can be any **QNR** value, except one restriction/exclusion:

C-3 : $q \neq -1 \pmod{N}$.

In other words, only the largest value in $Z_N^* = (N-1)$ is not acceptable as a **QNR** .

Any other integer in the closed interval $[2, N-2]$ that is a **QNR** modulo N works.

C-4 : q satisfies the **Euler Criterion** [\[9\]](#) modulo- N

$$q^{\left(\frac{N-1}{2}\right)} \pmod{N} = \mathbf{Jacobi_Symbol}(q, N) = -1 \pmod{N} . \quad (1)$$

C-5 : \sqrt{q} also satisfies the Modular Binomial Expansion Congruence (**MBEC**) :

$$(1 + \sqrt{q})^N \pmod{N} = 1 + \left[(\sqrt{q})^N \pmod{N} \right] . \quad (2)$$

The claim is that if all of the above conditions are satisfied, then N must be prime.

³ The symbol $\stackrel{\Delta}{=}$ denotes a definition.

§ Section 3 : Re-stating the result in the polynomial domain [4, Part I, Sec. 3, Remark 3.2, page 20]

Baseline Primality Theorem (BPT) : Given any positive integer N (to be tested for primality), suppose that we find some integer q , that together with N , satisfies the following conditions:

C-1-p : $N > 1$ is an odd integer and is not a square of any other integer.

C-2-p : The **Jacobi-Symbol** of q w.r.t. $N \triangleq \mathbf{Jacobi_Symbol}(q, N) = -1$
 $\Rightarrow q$ is a Quadratic Non Residue (**QNR**) modulo- N .

Note that q can be any **QNR** value, except one restriction/exclusion:

C-3-p : $q \neq -1 \pmod{N}$.

In other words, only the largest value $(N-1)$ in Z_N^* is not acceptable as a **QNR**;

Any other integer in the closed interval $[2, (N-2)]$ that is a **QNR** modulo- N works.

C-4-p : q satisfies the **Euler Criterion** modulo- N , i.e.,

$$x^{(N-1)} \pmod{\langle (x^2 - q), N \rangle} = \mathbf{Jacobi_Symbol}(q, N) = -1 \quad (3)$$

C-5-p : N also satisfies the Modular Binomial Expansion Congruence (**MBEC**)

$$(1+x)^N \pmod{\langle (x^2 - q), N \rangle} = 1 + \left[(x)^N \pmod{\langle (x^2 - q), N \rangle} \right] \quad (4)$$

The claim is that if all of the above conditions are satisfied, then N must prime.

Next, we briefly state our assumptions, explain our notation, and then mention well-known fact(s) that follow from the assumptions.

A_1. In this document ; unless explicitly stated otherwise ; all polynomials $\mathcal{P}(x)$ of interest are assumed to be uni-variate ; i.e., they include a single variable/indeterminate argument “ x ” ; and all coefficients of all polynomials are Integers.

A_2. Since x is a variable, arriving at an equation of the form $x = m \pmod{N}$; where ; m is a specific numerical value (or in other words, m is an arbitrary constant) is tantamount to a contradiction because it assigns a specific value to x thereby contradicting the assumption/hypothesis that x is an indeterminate.

A_3. From the preceding assumption, it follows that $x \neq m \pmod{N}$ is a valid assertion.

A_4. A special case of the preceding statement is the practically useful assertion that $x \neq 0 \pmod{N}$.
 (This assertion is used a few times in the proof).

Notation_1: The notation “ $\mathcal{P}(x) \bmod \langle (x^2 - q), N \rangle$ ” denotes the result obtained by
 (i) reducing (i.e., taking the remainder of) polynomial $\mathcal{P}(x)$ with respect to
 the divisor polynomial $(x^2 - q)$; wherein; x is the indeterminate/variable argument of the polynomials;
 and
 (ii) then reducing all the coefficients in the polynomial remainder modulo- N .

Fact_0: It turns out that the order of the remaindering operations (w.r.t. $(x^2 - q)$ and w.r.t. N) does not affect the final result of the modular reduction.

§ Section 4 : Well known results used in the Proof

In this section, we state a few facts/results that are well known. To that end, we start with some definitions.

Let

$$\mathcal{P}(x) = C_0 + C_1x + C_2x^2 + \cdots + C_i x^i + \cdots + C_k x^k \quad (5)$$

be an arbitrary polynomial of degree k . Then, $\mathcal{P}(x)$ can always be written as the sum of its even and odd parts:

$$\mathcal{P}(x) = \mathcal{P}_{\text{even}}(x) + \mathcal{P}_{\text{odd}}(x) \quad (6)$$

where ;

$$\mathcal{P}_{\text{even}}(x) \triangleq \text{sum of all terms with even powers of } x = [C_0 + C_2x^2 + \cdots + C_{2m}x^{2m} + \cdots] \quad (7)$$

and

$$\mathcal{P}_{\text{odd}}(x) \triangleq \text{sum of all odd degree terms} = [C_1x + C_3x^3 + \cdots + C_{(2m+1)}x^{(2m+1)} + \cdots] \quad (8)$$

Since

$$\mathcal{P}_{\text{even}}(-x) = \mathcal{P}_{\text{even}}(x) \quad (9)$$

and

$$\mathcal{P}_{\text{odd}}(-x) = -\mathcal{P}_{\text{odd}}(x) \quad (10)$$

then it follows that

$$\mathcal{P}_{\text{even}}(x) = \frac{1}{2}(\mathcal{P}(x) + \mathcal{P}(-x)) \quad (11)$$

and

$$\mathcal{P}_{\text{odd}}(x) = \frac{1}{2}(\mathcal{P}(x) - \mathcal{P}(-x)) \quad (12)$$

We are interested only in polynomials whose coefficients C_i are all integers. Therefore, each coefficient C_i can be expressed as

$$C_i = \alpha_i * N + \beta_i \quad (13)$$

wherein

$$\alpha_i = \text{the quotient when } C_i \text{ is divided by } N \quad \text{and} \quad \beta_i = \text{the corresponding remainder} \quad (14)$$

Then, it follows that the following exact algebraic equation holds :

$$\mathcal{P}(x) = \mathcal{P}(x) \bmod N + N \times \Delta_{\mathcal{P}}(x) \quad (15)$$

wherein

$$\mathcal{P}(x) \bmod N = \text{the polynomial with each coefficient in } \mathcal{P}(x) \text{ reduced modulo } N. \quad (16)$$

$$= \sum_{i=0}^k (C_i \bmod N) x^i = \sum_{i=0}^k \beta_i x^i \quad (17)$$

$$\text{and } \Delta_{\mathcal{P}}(x) = \sum_{i=0}^k \alpha_i x^i \quad (18)$$

where, the coefficients α_i of polynomial $\Delta_{\mathcal{P}}(x)$ are unrestricted integers (unlike β_i that are modulo- N integers restricted to the range $0 \leq \beta_i < N$).

It should be re-emphasized that relation (15) is an exact algebraic equality ; it is not a modular congruence (which refers to an equation wherein one or both sides of the equality are remainders of some (arbitrary) source polynomials or expressions; w.r.t. a common modulus).

Because Equation (15) is an exact algebraic equality that includes algebraic expressions (such as polynomials) of the argument x ; it is valid for all scalar values of the argument x ; which includes

- (i) all Real and Complex numbers ; as well as**
- (ii) any arbitrary scalar expression of arbitrary scalar arguments: for instance, substitutions such as $x = (y^3 + z)$ or $x = (w + \frac{1}{s})$ (wherein, s, w, y and z are arbitrary indeterminate variables) ; are valid operations that result in other exact algebraic equalities.**

It turns out that one specific substitution; viz; $x = (-x)$ is a particularly useful and powerful mechanism/tool that is used several times in the proof (in the next section).

Equation (15) can be used to derive the following extremely important and useful result:

Fact_1 : If two arbitrary polynomials $\mathcal{P}(x)$ and $\mathcal{L}(x)$ satisfy the modular congruence

$$\mathcal{P}(x) \bmod N = \mathcal{L}(x) \bmod N \quad (19)$$

Then, there exists a polynomial $\Delta_{(\mathcal{P}\mathcal{L})}(x)$ such that the following exact algebraic equality holds:⁴

$$\mathcal{P}(x) = \mathcal{L}(x) + N \times [\Delta_{(\mathcal{P}\mathcal{L})}(x)] \quad (22)$$

Proof of Fact_1 : From the definition in Equation (16), analogous to Equation (15) we obtain :

$$\mathcal{L}(x) = \mathcal{L}(x) \bmod N + N \times \Delta_{\mathcal{L}}(x) \quad (23)$$

Subtract the preceding equation (i.e., equation (23)) from Equation (15) to obtain

$$\mathcal{P}(x) - \mathcal{L}(x) = [\mathcal{P}(x) \bmod N - \mathcal{L}(x) \bmod N] + N \times (\Delta_{\mathcal{P}}(x) - \Delta_{\mathcal{L}}(x)) \quad (24)$$

Since $\mathcal{P}(x)$ and $\mathcal{L}(x)$ satisfy the modular congruence in Equation (19), then the first term on the right hand side of the preceding equation (i.e., the expression inside the square brackets on the right hand side of the preceding equation) is zero. Dropping that term, we obtain

$$\mathcal{P}(x) - \mathcal{L}(x) = N \times (\Delta_{\mathcal{P}}(x) - \Delta_{\mathcal{L}}(x)) \quad (25)$$

Then,

$$\text{Let } \Delta_{(\mathcal{P}\mathcal{L})}(x) \triangleq \Delta_{\mathcal{P}}(x) - \Delta_{\mathcal{L}}(x) \quad (26)$$

and re-arrange terms to obtain Equation (22) ; which completes the proof. \square

The significance of Fact_1 is that the polynomial $\Delta_{(\mathcal{P}\mathcal{L})}(x)$ can be thought to transform or “Lift” a modular congruence such as Relation (19) ; into the corresponding exact algebraic equality such as Equation (22). Accordingly, we refer to any such polynomial like $\Delta_{\mathcal{P}}(x)$, $\Delta_{\mathcal{L}}(x)$, $\Delta_{(\mathcal{P}\mathcal{L})}(x)$, \dots etc., that transforms a modular congruence relation into the corresponding exact algebraic equality; as the “lifter” polynomial.

The exact algebraic equality can then be reduced modulo any arbitrary modulus which can be distinct from, and/or co-prime w.r.t. the default modulus $\langle (x^2 - q), N \rangle$; or it could include the product of one or more factors of the default modulus.

Moreover, any integer value can be substituted for the argument x in the exact algebraic equality, and the resulting (exact) integer equality can be further reduced w.r.t. arbitrary integer moduli.

⁴ Note that **Fact_1** also implies the “duel” of Equation (22) :

$$\mathcal{L}(x) = \mathcal{P}(x) + N \times [\Delta_{(\mathcal{L}\mathcal{P})}(x)] \quad (20)$$

where,

$$\Delta_{(\mathcal{L}\mathcal{P})}(x) \triangleq (\Delta_{\mathcal{L}}(x) - \Delta_{\mathcal{P}}(x)) = -(\Delta_{(\mathcal{P}\mathcal{L})}(x)) \quad (21)$$

We provide a numerical example for small/toy value of N to illustrate **Fact_1**.

Let $N = 15$ and

$$\mathcal{P}(x) = 285x^{33} + 120x^{24} + 135x^{19} + 17x^{13} + 7x^{10} + 49x^8 + 39x^5 + 27x^4 + 31x^2 + 28x + 81 \quad (27)$$

and

$$\mathcal{L}(x) = 15x^{24} + 165x^{15} + 152x^{13} + 7x^{10} + 64x^8 + 54x^5 + 42x^4 + 31x^2 + 28x + 351 \quad (28)$$

be two arbitrary polynomials that satisfy the modular congruence

$$(\mathcal{P}(x) \bmod N) = (\mathcal{L}(x) \bmod N) = \mathcal{S}(x)$$

where,

$$\mathcal{S}(x) = 2x^{13} + 7x^{10} + 4x^8 + 9x^5 + 12x^4 + x^2 + 13x + 6 \quad (29)$$

Then, it can be verified that

$$\mathcal{P}(x) = (\mathcal{P}(x) \bmod N) + N \times \Delta_{\mathcal{P}}(x) \quad (30)$$

where

$$\begin{aligned} \Delta_{\mathcal{P}}(x) &= \text{the polynomial that "lifts" } (\mathcal{P}(x) \bmod N) \text{ to } \mathcal{P}(x) \\ &= 19x^{33} + 8x^{24} + 9x^{19} + x^{13} + 3x^8 + 2x^5 + x^4 + 2x^2 + x + 5 \end{aligned} \quad (31)$$

and

$$\mathcal{L}(x) = (\mathcal{L}(x) \bmod N) + N \times \Delta_{\mathcal{L}}(x) \quad (32)$$

where

$$\begin{aligned} \Delta_{\mathcal{L}}(x) &= \text{the polynomial that "lifts" } (\mathcal{L}(x) \bmod N) \text{ to } \mathcal{L}(x) \\ &= x^{24} + 11x^{15} + 10x^{13} + 4x^8 + 3x^5 + 2x^4 + 2x^2 + x + 23 \end{aligned} \quad (33)$$

Then, as per **Fact_1** it can be verified that the polynomial

$$\begin{aligned} \Delta_{(\mathcal{P}\mathcal{L})}(x) &= \text{The polynomial which "Lifts" } \mathcal{L}(x) \text{ to the polynomial } \mathcal{P}(x) \\ &= [\Delta_{\mathcal{P}}(x) - \Delta_{\mathcal{L}}(x)] \end{aligned} \quad (34)$$

$$= 19x^{33} + 7x^{24} + 9x^{19} - 11x^{15} - 9x^{13} - x^8 - x^5 - x^4 - 18 \quad (35)$$

Note that the coefficients in the preceding (exact algebraic) equation are not modulo- N numbers; rather, their values are (unrestricted) integers.

It turns out that the mere existence of a lifter polynomial (for every modular congruence of interest in this document) is sufficient for the new proof.

Specification of the exact values of all the coefficients in the lifter polynomial is not necessary.

Next, we summarize a few facts related to the “Binomial expansion theorem”.

$$\begin{aligned} B(x) &\triangleq \text{the (Binomial) expansion of } (1+x)^N \\ &= 1 + \binom{N}{1} \cdot x + \binom{N}{2} \cdot x^2 + \cdots + \binom{N}{k} \cdot x^k + \cdots + \binom{N}{N-1} \cdot x^{N-1} + x^N \end{aligned} \quad (36)$$

where

$$\binom{N}{k} = \text{the binomial coefficient } N_choose_k \quad (37)$$

Note that Equation (36) is an exact algebraic equality ; it is not a modular congruence. It is therefore valid for all Real as well as Complex scalar values of the argument x .

Let

$$R(x) \triangleq (1+x)^N - 1 - x^N = B(x) - 1 - x^N \quad (38)$$

$$= \binom{N}{1} \cdot x + \binom{N}{2} \cdot x^2 + \cdots + \binom{N}{k} \cdot x^k + \cdots + \binom{N}{N-1} \cdot x^{N-1} \quad (39)$$

The preceding two relations are also exact algebraic equalities.

Then, it follows that

$$R(x) \bmod N = R_{\text{even}}(x) \bmod N + R_{\text{odd}}(x) \bmod N \quad (40)$$

With the polynomials of interest defined as above, we state the following well known results:

Fact_2 [10, 11, 12, 13, 14] :

$$N \text{ is a prime Iff } \binom{N}{k} \bmod N = 0 \text{ for } 1 \leq k \leq N-1 \quad (41)$$

In other words, N is a prime iff all non-trivial binomial coefficients $\binom{N}{k}$ are divisible by N .

We close out this section with one more fact (which directly follows from Fact_2) :

Fact_3 [10, 11, 12, 13, 14] :

N is a prime Iff

$$\mathcal{R}(x) \bmod N = 0 \text{ and } R_{\text{even}}(x) \bmod N = 0 \text{ and } R_{\text{odd}}(x) \bmod N = 0 \quad (42)$$

otherwise, N is a composite, and in that case

$$\mathcal{R}(x) \bmod N \neq 0 \text{ and } R_{\text{even}}(x) \bmod N \neq 0 \text{ and } R_{\text{odd}}(x) \bmod N \neq 0 \quad (43)$$

For example, for $N = 9$, it can be verified that

$$(1+x)^9 \bmod 9 = x^9 + 3x^6 + 3x^3 + 1 \quad (44)$$

$$\begin{aligned} \Rightarrow R_{\text{even}}(x) \bmod 9 &= 3x^6 \text{ and } R_{\text{odd}}(x) \bmod 9 = 3x^3 \\ \text{and } R(x) \bmod 9 &= 3x^6 + 3x^3 \end{aligned} \quad (45)$$

likewise, for $N = 15$

$$(1+x)^N \bmod N = x^{15} + 5x^{12} + 3x^{10} + 10x^9 + 10x^6 + 3x^5 + 5x^3 + 1 \quad (46)$$

$$\Rightarrow R_{\text{even}}(x) \bmod N = 5x^{12} + 3x^{10} + 10x^6$$

and

$$R_{\text{odd}}(x) \bmod N = 10x^9 + 3x^5 + 5x^3$$

and

$$\begin{aligned} R(x) \bmod N &= (R_{\text{even}}(x) \bmod N) + (R_{\text{odd}}(x) \bmod N) \\ &= 5x^{12} + 3x^{10} + 10x^9 + 10x^6 + 3x^5 + 5x^3 \end{aligned} \quad (47)$$

That completes a brief summary of well known facts that are used in the proof.

In the next section we demonstrate the proof of the Baseline Primality Theorem.

§ Section 5 : Proof of the Baseline Primality Theorem

§ Subsection 5.1 : Explanation of the exclusion of $q = -1 \pmod N$ as the QNR

First, we briefly explain why the QNR value $q = -1$ must be excluded.

The Euler's Criterion Check (condition [C-4-p](#) from [Section 3](#)), when expressed via polynomial remainder operation, takes the form

$$x^{(N-1)} \pmod{\langle (x^2 - q), N \rangle} = -1 \quad . \quad \text{which is Eqn. (3) repeated for convenience}$$

The preceding equation can be re-arranged as

$$(x^{(N-1)} + 1) \pmod{\langle (x^2 - q), N \rangle} = 0 \quad . \quad (48)$$

Since N is odd, $(N - 1)$ is an even integer. Accordingly,

$$\text{let } \frac{N-1}{2} = \delta \quad . \quad (49)$$

Then, Eqn. (48) can be expressed in terms of δ as follows:

$$((x^2)^\delta + 1) \pmod{\langle (x^2 - q), N \rangle} = 0 \quad . \quad (50)$$

If QNR $q = -1$ is used, then the divisor polynomial is

$$\mathcal{D}(x) = x^2 - q = x^2 - (-1) = x^2 + 1 \quad (51)$$

and Eqn. (50) becomes

$$((x^2)^\delta + 1) \pmod{\langle (x^2 + 1), N \rangle} = 0 \quad . \quad (52)$$

Note that

$$\text{if } \delta \text{ is an odd number, then } ((x^2)^\delta + 1) \text{ is divisible by } (x^2 + 1) \quad . \quad (53)$$

irrespective of any other condition on N .

As a result, a large number of arbitrary values of N (that are not prime numbers or Carmichael numbers) can satisfy the Euler's Criterion, if $q = -1$ is allowed.

To steer clear of this obstacle, we simply disallow $q = -1$, so that

$$(x^2 - q) \pmod N \neq x^2 + 1 \quad . \quad (54)$$

Consequently, the full discriminating power of the Euler Criterion Check is leveraged.

Next, we derive two auxiliary conditions that are needed in the proof.

§ Subsection 5.2 : Derivation of two auxiliary identities needed for the proof

The two equations of interest are the following two integer modular congruences:

$$\textbf{Auxiliary Condition 1 (A-C-1)} : (1-q)^N \bmod N = (1-q) \quad (55)$$

and

$$\textbf{Auxiliary Condition 2 (A-C-2)} : (1+q)^N \bmod N = (1+q) \quad (56)$$

In other words, the two auxiliary identities state that the modulo- N integers $[(1-q) \bmod N]$ and $[(1+q) \bmod N]$ both satisfy Fermat's Little Theorem (FLT) [15].

Derivation of Auxiliary Condition 1 (A-C-1) :

First, note that the Binomial Congruence Check (i.e., condition [\(C-5-p\)](#)) yields

$$(1+x)^N \bmod \langle (x^2-q), N \rangle = 1 + \left[(x)^N \bmod \langle (x^2-q), N \rangle \right] \quad (57)$$

$$\text{Euler Criterion yields } x^{(N-1)} \bmod \langle (x^2-q), N \rangle = \textbf{Jacobi_Symbol}(q, N) = -1 \quad (58)$$

Since $x \neq 0$ as per assertion [A_4](#) ; then multiply both sides of the preceding equation by x to obtain

$$x^N \bmod \langle (x^2-q), N \rangle = -x \quad (59)$$

Next, plug-in the result of the preceding equation into the modular congruence relation [\(57\)](#).

In other words, plug-in $(-x)$ for x^N into [\(57\)](#) to obtain

$$(1+x)^N \bmod \langle (x^2-q), N \rangle = (1-x) \bmod \langle (x^2-q), N \rangle \quad (60)$$

In the preceding relation, replace (x) with $(-x)$ to obtain⁵

$$(1-x)^N \bmod \langle ((-x)^2-q), N \rangle = (1+x) \bmod \langle ((-x)^2-q), N \rangle \quad (62)$$

⁵ Alternatively; the same equation can be derived from scratch as follows:
Consider the Modular Binomial Expansion Congruence for $(1-x)^N$:

$$\begin{aligned} (1-x)^N \bmod \langle (x^2-q), N \rangle &= 1 + \left[(-x)^N \bmod \langle (x^2-q), N \rangle \right] \\ &= (1-x^N) \bmod \langle (x^2-q), N \rangle \end{aligned} \quad (61)$$

Then using Equation [\(59\)](#) ; replace $-x^N$ with $+x$ on the right hand side of the preceding Equation which also yields Equation [\(62\)](#) \square

Multiplying the two modular congruences in Equations (60) and (62) yields

$$\left((1+x)^N \times (1-x)^N \right) \bmod \langle (x^2-q), N \rangle = [(1-x) \times (1+x)] \bmod \langle (x^2-q), N \rangle \quad (63)$$

or, equivalently

$$(1-x^2)^N \bmod \langle (x^2-q), N \rangle = (1-x^2) \bmod \langle (x^2-q), N \rangle \quad (64)$$

In the preceding equation ; since the order of remaindering operations w.r.t. (x^2-q) and N does not matter ; we take the remainder of each occurrence of the term “ (x^2) ” w.r.t. (x^2-q) to obtain

$$\begin{aligned} \left[1 - \left(x^2 \bmod (x^2-q) \right) \right]^N \bmod \langle (x^2-q), N \rangle = \\ \left[1 - \left(x^2 \bmod (x^2-q) \right) \right] \bmod \langle (x^2-q), N \rangle \end{aligned} \quad (65)$$

Since $x^2 = 1 \times (x^2-q) + q$ then

$$\left(x^2 \bmod (x^2-q) \right) = q \quad (66)$$

Plugging the result of the preceding equation into Equation (65) yields

$$[1-q]^N \bmod \langle (x^2-q), N \rangle = [1-q] \bmod \langle (x^2-q), N \rangle \quad (67)$$

Now, note that $(1-q)$ is an integer; or in other words, $(1-q)$ is a polynomial of degree 0.

Therefore, taking the remainder of $(1-q)$ w.r.t. the divisor polynomial $\mathcal{D}(x) = (x^2-q)$ has no effect, i.e.,

$$(1-q) \bmod (x^2-q) = (1-q) \quad (68)$$

and therefore

$$(1-q) \bmod \langle (x^2-q), N \rangle = (1-q) \bmod N \quad (69)$$

Likewise, since $(1-q)^N$ is also an integer, then taking its remainder w.r.t. (x^2-q) has no effect, so that

$$(1-q)^N \bmod \langle (x^2-q), N \rangle = (1-q)^N \bmod N \quad (70)$$

Finally, Equations (67), (69) and (70) together yield the desired integer modular congruence :

$$(1-q)^N \bmod N = (1-q) \quad \text{which is auxiliary condition 1 (i.e., [\(A-C-1\)](#))} \quad \square \quad (71)$$

Derivation of Auxiliary Condition 2 (A-C-2) : Note that

$$(1 - q)^N = 1 - \binom{N}{1}C_1 \cdot q + \binom{N}{2}C_2 \cdot q^2 - \binom{N}{3}C_3 \cdot q^3 + \cdots + \binom{N}{N-1}C_{N-1} \cdot q^{N-1} - q^N \quad (72)$$

$$\begin{aligned} &= \text{the binomial expansion polynomial of the integer argument } q \\ &\triangleq \mathcal{P}_B(q) \end{aligned} \quad (73)$$

Therefore

$$\begin{aligned} (1 - q)^N \bmod N &= (1 - q) \\ \Rightarrow \mathcal{P}_B(q) \bmod N &= (1 - q) \end{aligned} \quad (74)$$

Then, using **Fact_1** , it follows that

$$\mathcal{P}_B(q) = (1 - q) + N \times \Delta(q) \quad (75)$$

where, $\Delta(q)$ is the “lifter” polynomial of argument “ q ” that transforms the modular congruence in [\(A-C-1\)](#) into the exact integer equation [\(75\)](#).

The preceding equation implies that

$$(1 - q)^N = (1 - q) + N \times \Delta(q) \quad (76)$$

Since the preceding relation is an exact equality; then the argument “ q ” can be substituted (replaced) with any other scalar argument. Therefore, in Equation [\(76\)](#) replace “ q ” with “ $(-q)$ ” to obtain

$$(1 + q)^N = (1 + q) + N \times \Delta(-q) \quad (77)$$

Finally, take the remainder of both sides of the preceding equation w.r.t. N to obtain :

$$(1 + q)^N \bmod N = (1 + q) \bmod N \quad \text{which is } \a href="#">(A-C-2) \quad \square$$

Next, we unveil the main body of the proof in the following separate sub-section.

§ Subsection 5.3 : Main body of the Proof

Condition **(C-5-p)** in the theorem requires us to explicitly check that the following identity holds with x as a variable/indeterminate:

$$R(x) \bmod \langle (x^2 - q), N \rangle \stackrel{\checkmark}{=} 0 \quad (78)$$

Note that a remainder w.r.t. a quadratic divisor polynomial of the form $(x^2 - q)$ is at most a degree 1 polynomial. Accordingly, we evaluate remainders modulo $(x^2 - q)$ and modulo N in each square-and-reduce step in each modular exponentiation and verify that the final remainder is indeed 0 (a polynomial 0 ; which implies that the coefficients of all degrees in the polynomial remainder are equal to $(0 \bmod N)$).

Therefore, the preceding equation implies that one of the following two cases must hold

Case 1: $R(x) \bmod N = 0$ (the entire polynomial $[R(x) \bmod N] = 0$) ;
and as a result ; taking the remainder of 0 w.r.t. the divisor polynomial $\mathcal{D}(x) = (x^2 - q)$ also yields 0 as seen in Eqn. (78) .

In this case, equating coefficients of each degree of x on both sides of Eqn. (39) yields

$$({}^N C_k) \bmod N = 0 \quad \text{for } 1 \leq k \leq (N-1) \quad (79)$$

The preceding relations imply that N must be a prime and the proof is complete. \square

or

Case 2:

$$[R(x) \bmod N] \neq 0 \quad (80)$$

$$\text{but } [(R(x) \bmod N) \bmod (x^2 - q)] = 0 \bmod N \quad (81)$$

Note that the preceding relation (i.e., equation (81)) is merely a re-statement of the Modular Binomial Congruence Condition **(C-5-p)** (i.e. Relation (4)).

We show that this case leads to an absurd result.

In other words, we demonstrate that
the preceding two relations (i.e., (80) and (81)) ;
together with
the Euler-Criterion-Check (i.e., condition **(C-4-p)**) ;
and the other prior conditions
(that N is an odd number which is not a square of any integer;
and $2 \leq q \leq (N-2)$ is a Quadratic Non Residue (QNR) modulo- N)
lead to a contradiction (i.e., an absurd result).

In yet other words, we demonstrate that all of the conditions (that appear in the statement of the Baseline Primality Theorem/Result) AND the assumption that N is a composite number; together lead to an absurd result ; thereby demonstrating that all those statements cannot hold true together.

To that end, first, we re-state the Euler Criterion Check condition for the sake of convenience and clarity:

$$x^{(N-1)} \mod \langle (x^2 - q), N \rangle = \mathbf{Jacobi_Symbol}(q, N) = -1$$

Then, assuming that $x \neq 0$, multiply (both sides) of the preceding equation by x to obtain

$$x^N \mod \langle (x^2 - q), N \rangle = -x \quad (82)$$

We re-write the expression for $R(x)$ for convenience and clarity :

$$R(x) = (1 + x)^N - 1 - x^N$$

so that

$$R(x) \mod \langle (x^2 - q), N \rangle = [(1 + x)^N - 1 - x^N] \mod \langle (x^2 - q), N \rangle \quad (83)$$

Then using relation (82), plug-in “ $-x$ ” for “ x^N ” on the right hand side of the preceding relation to obtain

$$R(x) \mod \langle (x^2 - q), N \rangle = [(1 + x)^N - 1 + x] \mod \langle (x^2 - q), N \rangle \quad (84)$$

Note that in the case under consideration, the assumption is that the Modular Binomial Congruence Check (MBCC, i.e., condition **(C-5-p)**) is satisfied, i.e.,

$$R(x) \mod \langle (x^2 - q), N \rangle = 0 \quad (85)$$

The preceding two relations together yield

$$[(1 + x)^N - 1 + x] \mod \langle (x^2 - q), N \rangle = 0 \quad (86)$$

Note that the preceding modular congruence (i.e., equation (86)) implies that when the non-zero polynomial $[(1 + x)^N - 1 + x] \mod N$ is divided by the divisor polynomial $(x^2 - q)$, the polynomial remainder is $(0 \mod N)$.

In other words ; $(x^2 - q)$ evenly divides the polynomial $[(1 + x)^N - 1 + x] \mod N$.

Therefore we obtain

$$[(1 + x)^N - 1 + x] \mod N = [T(x) \times (x^2 - q)] \mod N \quad (87)$$

wherein,

$$T(x) \mod N = \text{the modulo-}N \text{ polynomial quotient that results when the non-zero polynomial } [(1 + x)^N - 1 + x] \mod N \text{ is divided by } (x^2 - q) \quad (88)$$

Rearrange the terms in relation (87) to obtain the following

$$\textbf{canonical congruence: } (1+x)^N \bmod N = \left[T(x) \times (x^2 - q) + (1-x) \right] \bmod N \quad (89)$$

Next, using [Fact_1](#) ,

*“lift” the preceding **canonical congruence** into the following exact algebraic equation :*

$$\textbf{canonical algebraic equality : } (1+x)^N = \left[T(x) \times (x^2 - q) + (1-x) \right] + N \times \Delta_B(x) \quad (90)$$

where ; $\Delta_B(x)$ is the “lifter” polynomial.

Since the preceding equation is an exact algebraic equality, then it holds even when the argument x is substituted/replaced with any integer.

Accordingly, we plug-in $x = q$ in the **canonical algebraic equality (90)** to obtain the following exact integer equality:

$$(1+q)^N = \left[T(q) \times (q^2 - q) + (1-q) \right] + N \times \Delta_B(q) \quad (91)$$

where ,

$$T(q) \triangleq \left| T(x) \right|_{x=q} = \text{the polynomial } T(x) \text{ evaluated at the argument } x = q \quad (92)$$

and

$$\Delta_B(q) \triangleq \left| \Delta_B(x) \right|_{x=q} = \text{the polynomial } \Delta_B(x) \text{ evaluated at the argument } x = q$$

Taking the remainder of Equation (91) w.r.t. N yields

$$(1+q)^N \bmod N = T(q) \times (q^2 - q) + (1-q) \quad (93)$$

In an exactly analogous manner, plug-in $x = -q$ in (90) to obtain the exact integer equality:

$$(1-q)^N = \left[T(-q) \times ((-q)^2 - q) + (1+q) \right] + N \times \Delta_B(-q) \quad (94)$$

where ,

$$T(-q) = \left| T(x) \right|_{x=-q} \quad \text{and} \quad \Delta_B(-q) = \left| \Delta_B(x) \right|_{x=-q} \quad (95)$$

Taking the remainder of Equation (94) w.r.t. N yields

$$(1-q)^N \bmod N = T(-q) \times (q^2 - q) + (1+q) \quad (96)$$

Note that the preceding equation (96) together with (A-C-1) yields:

$$(1 - q)^N \mod N = (1 - q) = T(-q) \times (q^2 - q) + (1 + q) \quad (97)$$

Likewise, Equation (93) together with (A-C-2) yields:

$$(1 + q)^N \mod N = (1 + q) = T(q) \times (q^2 - q) + (1 - q) \quad (98)$$

Next, subtract Equation (97) from Equation (98) to obtain

$$2q = [(T(q) - T(-q)) \times (q^2 - q) - 2q] \mod N \quad (99)$$

or equivalently

$$4q \mod N = [q(q - 1)(T(q) - T(-q))] \mod N \quad (100)$$

Since, **Jacobi_Symbol**(q, N) = -1, then $\gcd(q, N) = 1$.

Therefore $(\frac{1}{q} \mod N)$ exists and is unique ; which in-turn implies that dividing the preceding modular congruence (i.e., Equation (100)) by q is a valid operation ; and yields

$$4 \mod N = [(q - 1)(T(q) - T(-q))] \mod N \quad (101)$$

In the preceding equation, plug-in

$$T(q) - T(-q) = 2 \times T_{\text{odd}}(q) \quad (102)$$

to obtain

$$[(q - 1) \times T_{\text{odd}}(q)] \mod N = 2 \quad (103)$$

Replacing q with $-q$ in the preceding relation⁶ yields :

$$((-q) - 1) \times T_{\text{odd}}(-q) = 2 \mod N \quad (105)$$

or, equivalently

$$(-1)(q + 1) \times T_{\text{odd}}(-q) = 2 \mod N \quad (106)$$

⁶ to see the validity of this substitution, use **Fact_1** to lift the modular congruence in Equation (103) into the corresponding exact algebraic equality :

$$(q - 1) \times T_{\text{odd}}(q) = 2 + N \times \Delta_F(q) \quad (104)$$

where, $\Delta_F(q)$ is the lifter polynomial (of argument q).

Then, replacing q with $-q$ in the preceding exact equality ; i.e. , Equation (104) ; and then taking the remainder of both sides w.r.t. N yields Equation (105)

However, since $T_{\text{odd}}(q)$ includes only odd powers of q , then

$$T_{\text{odd}}(-q) = -T_{\text{odd}}(q) \quad (107)$$

which, when substituted in Equation (106) ; yields

$$(q+1) \times T_{\text{odd}}(q) \bmod N = 2 \quad (108)$$

Next, subtract Equation (103) from Equation (108) to obtain

$$T_{\text{odd}}(q) \times (q+1 - q+1) = 0 \bmod N$$

or equivalently,

$$T_{\text{odd}}(q) \times 2 = 0 \bmod N \quad (109)$$

The preceding equation implies that

$$T_{\text{odd}}(q) = 0 \bmod N \quad (110)$$

Finally, substitute the preceding result, i.e., the result of Equation (110) into Equation (108) or Equation (103) and note that either of those substitutions yields the following relation:

$$0 = 2 \bmod N \quad (111)$$

The preceding relation is absurd and completes the proof by contradiction. \square

§ Section 6 : Discussion: our results advance the state-of-the-art of Primality Testing

In this section, we first present a brief summary of the current state-of-the-art of deterministic primality testing. We then explain the intuition behind our methods⁷ and demonstrate how it leads to new results; including all of the results unveiled in [4].

§ Subsection 6.1 : Brief summary of current state-of-the-art of Deterministic Primality Testing

It is well known [10] that, any integer N is a prime number **iff** the following Modular Binomial Expansion Congruence (**MBEC**) holds

$$\mathbf{MBEC} \quad : \quad (x + y)^N \bmod N = (x^N + y^N) \bmod N, \quad (112)$$

where, x and y are arbitrary scalar integers or scalar indeterminates/variables.

The proof is based on another well known fact [10, 11, 12, 14]: For every integer $N > 1$,

$$({}^N C_k) \bmod N = 0 \quad \text{for } k = 1, \dots, (N-1) \quad \mathbf{iff} \quad N \text{ is a prime, where} \quad (113)$$

$$({}^N C_k) = \frac{N \cdot (N-1) \cdots (N-k+1)}{1 \cdot 2 \cdots k} = \text{the binomial coefficient } N\text{-choose-}k. \quad (114)$$

For a partial and intuitive explanation of why Eqn. (113) holds: note that if N is a prime number, then none of the factors in the denominator of the binomial coefficient divides N ; and this is true for all non-trivial binomial coefficients, i.e., for k values satisfying $1 \leq k \leq N-1$. As a result, if N is a prime, then N divides all non-trivial binomial coefficients; which in turn implies that the remainder of any non-trivial binomial coefficient modulo N is zero.

Purely symbolic direct verification of the **MBEC** (i.e., Eqn. (112)) leaving x and y as true indeterminate symbols is not possible for all but small toy values of N (because the number of terms in the Binomial Expansion is $N+1$).

The renowned AKS method [10] uses a slightly restricted form of Eqn. (112) wherein they leave a single variable argument x and select some specific integer value “ a ” to be substituted in place of the second variable y , resulting in the congruence

$$(x + a)^N \bmod N = (x^N \bmod N) + (a^N \bmod N). \quad (115)$$

⁷ in prior versions of this document, a sizable fraction of the material presented in this section was placed right after the Introduction. However, some readers commented that with that arrangement, the statement of the Baseline Primality Result got deferred all the way to page number 8; and the main body of the proof did not start until page 14, thereby locating the proof in the last third of that document; which seemed to deviate from the intention and claim to narrowly focus the document on the theoretical proof of the BPR. Therefore in this version, we have kept the introduction to the bare minimum (approximately 2 pages long) and delved into the statement of the Baseline Primality Result and its proof at the earliest possible juncture. We hope that this re-organization keeps the main focus of this document on the BPR and its proof as intended.

By Fermat's Little Theorem, if N is any prime number, then $a^N \bmod N = a$, for every integer $a \in [1, N-1]$, which further simplifies the preceding equation to

$$(x+a)^N \bmod N = (x^N \bmod N) + a \quad (116)$$

Even with this simplification, a direct verification of the preceding equation leaving the argument x as a true indeterminate symbol is not possible for all but small toy values of N .

To circumvent this difficulty the AKS method and its derivatives or variants [11, 13, 14, 16, 17, 18], in essence, can be thought to invoke the following work-around: suppose that instead of trying to verify Eqn. (116) directly; we take the remainder of the identity in that equation with respect to some divisor polynomial $\mathcal{D}(x)$ to obtain the the following modified equation to be tested:

$$[(a+x)^N \bmod N] \bmod \mathcal{D}(x) = [(a+x^N) \bmod N] \bmod \mathcal{D}(x), \quad (117)$$

or equivalently

$$\left[\left((a+x)^N - a - x^N \right) \bmod N \right] \bmod \mathcal{D}(x) = 0. \quad (118)$$

If the degree $\mathcal{D}(x)$ is sufficiently small, then it is possible to check the congruence in the preceding equation in a computationally efficient manner while letting x remain a true indeterminate/variable.

However, the main question then becomes: can the divisor polynomial $\mathcal{D}(x)$ be selected in such a way that whenever the congruence in Eqn. (118) holds, the original congruence in Eqn. (116) that we would like to verify/check also holds true?

How many such divisor polynomials need to be tried ?

At how many distinct “ a ” values does the congruence in Eqn. (116) need to be tested (in order to guarantee that it is true for all integer values of x and a) ?

The AKS family of methods deploy a divisor polynomial of the form

$$\mathcal{D}(x) = x^r - 1 \quad (119)$$

The roots of this form of $\mathcal{D}(x)$ are the r -th roots of unity; which have many special properties that enable computationally efficient verification of Relation (118).

The ingenuity of the AKS deterministic primality test [10] lies in demonstrating that the congruence in Eqn. (116) holds for all integer values of x as long as

(i) the degree r of the divisor polynomial $\mathcal{D}(x)$ satisfies a logarithmic bound, w.r.t. N ;

and

(ii) the modular congruence in Eqn. (117) is checked at all integer values of “ a ” up to some threshold value, which is also logarithmically bounded.

§ Subsection 6.2 : Motivation behind our recent work

We took a slightly different approach, considering a more specific form of the MBEC

$$\textbf{Specific version of MBEC (SvMBEC)} : (1+x)^N \bmod N = (1+x^N) \bmod N , \quad (120)$$

where, x is a scalar indeterminate.

If the preceding **SvMBEC** (i.e., Eqn. (120)) could be verified at some numerical value of x such that none of the powers of that numerical value exist as integers, then that single verification would be sufficient to conclude that N must be prime.

For example, if the **SvMBEC** could be verified at a single transcendental real value of x (such as, $x = \pi^8$; or $x = e$ = the base of natural logarithms ; or any real number that is not an algebraic integer); then that single verification should be sufficient to conclude that N must be a prime number.

However, it is not immediately clear how to compute sufficiently accurate floating-point approximations of the “remainders” that would arise in such a numerical verification, in an efficient manner. It is likely that the precision (and consequently the total amount of computations) required to verify the **SvMBEC** at transcendental real values of x is impractically large for all but small toy values of N .

Consequently, like the AKS method and its variants, we also test the preceding **SvMBEC** congruence modulo some divisor polynomial $(\mathcal{D}(x) \bmod N)$:

$$(1+x)^N \bmod \langle \mathcal{D}(x), N \rangle = 1 + (x^N) \bmod \langle \mathcal{D}(x), N \rangle , \quad (121)$$

The substantial difference between the AKS family of methods and our methods lies in how we select the divisor polynomial(s) $\mathcal{D}(x)$:

Unlike the AKS family of methods that focus on a specific form of the divisor polynomial (viz., $\mathcal{D}(x) = x^r - 1$) ;

we deploy divisor polynomials $\mathcal{D}(x)$ (of the smallest degree with the smallest number of non-zero coefficients ; that we can find with the smallest number of bit-operations) ;

$$\text{such that } \mathcal{D}(x) = 0 \bmod N \text{ has no integer roots} . \quad (122)$$

As a result, verifying the congruence in Eqn. (121) is tantamount to verifying the main congruence of interest in Eqn. (120) at the roots of $\mathcal{D}(x) = 0$, i.e., at values that do not exist as modulo- N integers.

To see this fact, suppose that

$$(1+x)^N \bmod N = (Q_1(x) \cdot \mathcal{D}(x) + R_1(x)) \bmod N \quad (123)$$

and

$$1 + (x^N) \bmod N = (Q_2(x) \cdot \mathcal{D}(x) + R_2(x)) \bmod N , \quad (124)$$

⁸ “Archimedes’ ” constant = 3.1415...

where, $Q_1(x), Q_2(x)$ are the quotients and $R_1(x), R_2(x)$ are the corresponding remainders.

Then, evaluate Eqn. (123) and Eqn. (124) at $x = \text{root_of_}\mathcal{D}(x)$ and note that

$$\left| \mathcal{D}(x) \right|_{x = \text{root_of_}\mathcal{D}(x)} = 0 . \quad (125)$$

The left hand side of the preceding equation has the standard notation for the evaluation of an expression in between the vertical lines, at the argument value, which is indicated in the subscript of the second vertical delimiter.

Then, it follows that

$$\left(\left| R_1(x) \right|_{x = \text{root_of_}\mathcal{D}(x)} \right) \bmod N = \left(\left| (1+x)^N \right|_{x = \text{root_of_}\mathcal{D}(x)} \right) \bmod N \quad (126)$$

and

$$\left(\left| R_2(x) \right|_{x = \text{root_of_}\mathcal{D}(x)} \right) \bmod N = \left(\left| 1 + (x)^N \right|_{x = \text{root_of_}\mathcal{D}(x)} \right) \bmod N . \quad (127)$$

Further, if Congruence (121) is satisfied, then the remainders are equal, i.e.,

$$R_1(x) = R_2(x) \bmod \langle \mathcal{D}(x), N \rangle \quad (128)$$

$$\Rightarrow \left(\left| R_1(x) \right|_{x = \text{root_of_}\mathcal{D}(x)} \right) \bmod N = \left(\left| R_2(x) \right|_{x = \text{root_of_}\mathcal{D}(x)} \right) \bmod N , \quad (129)$$

which together with Eqn. (126) and Eqn. (127), yields

$$\left(\left| (1+x)^N \right|_{x = \text{root_of_}\mathcal{D}(x)} \right) \bmod N = \left(\left| 1 + (x)^N \right|_{x = \text{root_of_}\mathcal{D}(x)} \right) \bmod N . \quad (130)$$

The preceding three equations demonstrate that verifying the congruence in Eqn. (121) is tantamount to verifying the main congruence of interest in Eqn. (120), at the roots of $\mathcal{D}(x) = 0$.

We deliberately select $\mathcal{D}(x)$ such that it has no integer roots modulo- N .

Therefore, the roots of $\mathcal{D}(x)$ are algebraic integers including irrational real numbers that do not exist as modulo- N integers.

As a result, our selection of $\mathcal{D}(x)$ enables an implicit verification of the congruence in Eqn. (120) at irrational real values of the argument x that do not exist as modulo- N integers.

★ **Therefore one single check of this type should suffice to conclude that N is prime.** ★

A sub case of the preceding argument was formalized as the “Baseline Primality Conjecture” and has been extensively investigated in [4]; and theoretically proved in this document.

§ Section 7 : Concluding Remarks

We have demonstrated a theoretical proof of the recent Baseline Primality Conjecture introduced in [4] . The main highlights of the proof are:

- The [main case/branch](#) of the proof is a “proof by contradiction” [19].
- All the other parts of the proof fall under the category of a “direct proof” [19].
- Overall, the entire proof is Elementary⁹ [19].
In other words the proof does not depend on advanced and/or modern results or methodologies.
- It is valid for all QNRs except one : $q = -1$ is disallowed.
As a result, the claim is unusually broad ; so much that some experts thought that the claim was unlikely to be true as stated; and speculated that it may hold for one value (or at most a few specific values) of the QNR q , such as, for example, “the smallest QNR value modulo- N ”.
However, strong numerical evidence suggested that the claims should stand as stated. And now, fortunately, the latest version of the theoretical proof has settled that question (assuming that this proof is error free; we hope that peer reviews by experts will corroborate our claims in the near future).
- An intriguing attribute of the proof is that it requires an analysis of only the odd and even symmetry properties of some polynomials.
In other words, the proof does not depend on the exact form of the polynomials (i.e., the exact values of the degrees of the terms in those polynomials or their coefficients), which in turn suggests that similar arguments might work to prove the Generalized Conjectures unveiled in [4] .

The underlying motivation brings out the benefits of pushing the boundaries to see whether fundamental results (such as the binomial expansion theorem) yield additional insights or complexity advantages when applied in domains different from the original ones: for example, letting the variables in the binomial theorem be real numbers or even Matrices (satisfying the added constraint that the product of the two matrices must be commutative). Indeed the matrix experiments in testing primality was how this entire line of investigation originally started in the first place (see [4] for further details).

The practical significance of the results presented in this article is substantial because the theoretical proof of the underlying fundamental theoretical result is the first and most important component of any larger (or more global) proof of correctness of any primality testing algorithms that are based on that theoretical result.

⁹ The most famous example of a proof that is definitely not considered to be “Elementary” is the now renowned proof of Fermat’s Last Theorem that was developed by Professor Andrew Wiles [20].

At the time of this writing, other best known deterministic primality testing algorithms, such as [11, 16, 13, 17, 18, 14], have a complexity that is `quartic` or higher (depending on the details of how the elementary arithmetic operations are defined; and their time-delay, memory and power requirements on a typical processor are characterized). It turns out that for cryptographically secure integer lengths of 1024-bits (or higher); the other known deterministic algorithms are still too slow (despite having a polynomial complexity).

As a result, all real-world implementations (including the GNU as well as Python unlimited precision libraries, Maple, etc) deploy few iterations of the Miller-Rabin test (together with few other tests). In other words, all real life implementations still use only probabilistic primality testing methods. While this has not caused a serious problem as of today, it is desirable to replace the probabilistic methods with deterministic methods. The algorithms based on the BPT that are unveiled in [4] represent a big step in that direction.

Now that the Baseline Primality Result has been theoretically proved; we enthusiastically invite readers, reviewers and peers to take the next logical step, which is to prove¹⁰ (or in the unlikely worst case scenario, disprove) the other conjectures unveiled in [4].

ACKNOWLEDGMENTS

The author would like to thank his colleague Professor Alan T. Sherman for his prompt, detailed and helpful comments on multiple versions of this document.

The author also thanks Professor Erich Bach from the CS Dept. at the University of Wisconsin, Madison for providing proofs of some critical conjectures (other than the BPC) that were unveiled in [4]. See the footnote at the bottom of this page (i.e., page number 26), and reference [21] for further details.

Moreover, Prof. Bach carefully read an early version of this document and pointed out a couple of wrong statements/assertions. Fortunately, those erroneous assertions were not needed for the proof; and therefore have been deleted. Prof. Bach's expert review and feedback was the first one we received, circa Feb 2023, for this latest version of the proof; and therefore it is invaluable and greatly appreciated.

Finally the author would like to profusely thank Professor Carl Pomerance for his timely and invaluable feedback (that ended up showing that the first version of the proof published in December 2021 was actually wrong). The author anticipates sending the latest version of this proof to Prof. Pomerance; in the near future, after it is reviewed/vetted by local domain experts.

¹⁰For instance, on 31st August 2019 ; Prof. Eric Bach, our colleague from CS Dept., Univ of Wisconsin; emailed us the proofs of two other auxiliary conjectures unveiled in the same document [4].

In particular he has provided the proofs of Equations numbered (78) and (79) in [4]. He was extremely generous and told us that we could use the PDF document he provided us or parts thereof anywhere as and when needed. We have therefore made his proofs available via the UMBC CSEE Dept. home page of the author of this article. Please see reference [21] in the bibliography for further details.

Bibliography

- [1] **Pomerance, Carl.**, “Personal Communication: comments on the proof published in the IEEE TechRxiv (ref [5] below in this list) ,” 8th January 2022.
- [2] —, “Personal Communication: second set of comments on the first revision of the proof,” 13th January 2022,
The original email message that pinpoints the mistake in the Dec. 2021 version of the proof (that was published in reference [5] in the IEEE TechRxiv) is available at the following URL :
[Online]. Available: <http://www.csee.umbc.edu/~phatak/newres/dissemin/Prof-Carl-Pomerance-identified-this-mistake.pdf>
- [3] —, “Personal Communication: final comments on the proof published in the IEEE TechRxiv (ref [5] below in this list) ,” 22nd January 2022.
- [4] Dhananjay. S. Phatak, et. al., “PPT : New Low Complexity Deterministic Primality Tests Leveraging Explicit and Implicit Non-Residues.”
August 2019,
The overall document is a set of 3 companion articles available via the following arXiv url.
[Online]. Available: <https://arxiv.org/abs/1908.06964>
- [5] D. S. Phatak , “Analytic Proof of the recent Baseline Primality Conjecture,” December 2021 .
Preliminary version published via the IEEE’s TechRxiv pre-review, pre-print, rapid dissemination and archival service; at the following URL ¹¹
[Online]. Available: <https://doi.org/10.36227/techrxiv.17139041.v1>
- [6] —, “New Proof of the recent Baseline Primality Conjecture,” May 2023 .
This document (= the current document) presents a completely new and correct version of the proof of the Baseline Primality Conjecture.
Therefore, this document will replace the erroneous version [5] in the near future, as soon as the IEEE archive maintainers approve of this update.

¹¹ *** **Prof. Carl Pomerance Identified a mistake in the Dec. 2021 version of the proof.** His original message can be viewed [at the URL \(at the end of\) Reference \[2\] above](#).

This current document (which has the new, correct proof) will replace the older, erroneous version in the TechRxiv in the near future.

However, the original erroneous version of the proof, i.e., reference [5] has also been permanently archived and made available publicly; via the author’s personal web-page at UMBC at the clickable link: [Erroneous early version of the proof](#)

- [7] Wikipedia, “Quadratic residue,” Last modified: Aug. 2018,
https://en.wikipedia.org/wiki/Quadratic_residue.
- [8] —, “Jacobi Symbol,” Last modified: Nov. 2018,
https://en.wikipedia.org/wiki/Jacobi_symbol.
- [9] —, “Euler’s criterion,” Last modified: Nov. 2018,
https://en.wikipedia.org/wiki/Euler’s_criterion.
- [10] M. Agrawal, N. Kayal, and N. Saxena, “PRIMES is in P,” *Annals of mathematics*, pp. 781–793, 2004.
- [11] R. Crandall and C. B. Pomerance, *Prime numbers: a computational perspective*. Springer Science & Business Media, 2006, vol. 182.
- [12] V. Shoup, *A computational introduction to number theory and algebra*. Cambridge university press, 2009.
- [13] H. W. Lenstra Jr. and C. Pomerance, “Primality testing with gaussian periods,” in *FSTTCS*, 2002, p. 1.
- [14] H. W. Lenstra Jr and C. B. Pomerance, “Primality testing with gaussian periods,” *Journal of the European Mathematical Society*, vol. 21, no. 4, pp. 1229–1269, 2019
. [Online]. Available: <https://math.dartmouth.edu/~carlp/aksfinal.pdf>
- [15] Wikipedia, “Fermat’s Little Theorem,” Last modified: Nov. 2022,
https://en.wikipedia.org/wiki/Fermat%27s_little_theorem.
- [16] M. Dietzfelbinger, *Primality testing in polynomial time: from randomized algorithms to "PRIMES is in P"*. Springer, 2004, vol. 3000.
- [17] H. Lenstra Jr. and C. Pomerance, “Primality testing with gaussian periods,” Last modified : 2008,
. [Online]. Available: <https://math.dartmouth.edu/~carlp/aks240817.pdf>
- [18] D. Bernstein, “Proving primality in essentially quartic random time,” *Mathematics of computation*, vol. 76, no. 257, pp. 389–403, 2007.
- [19] Wikipedia, “Mathematical proof,” Last modified: Mar. 2023,
https://en.wikipedia.org/wiki/Mathematical_proof.
- [20] —, “Wiles’s proof of Fermat’s Last Theorem,” Last modified: Feb. 2023,
https://en.wikipedia.org/wiki/Wiles’s_proof_of_Fermat’s_Last_Theorem.
- [21] **Bach, Eric.**, “Personal communication : Proofs of Auxiliary_Conjecture_1 Identities numbered as Equations (78) and (79) in [4],” Computer Science Dept., Univ. of Wisconsin, Madison, PDF document received via Email on the 31st August 2019
. [Online]. Available: <http://www.csee.umbc.edu/~phatak/newres/dissemin/Eric-Bach-proofs-of-eqns-78-79-31aug2019.pdf>