On Visual Proofs for Primality

Akash Pardeshi*
University Laboratory High School
University of Illinois at Urbana-Champaign, IL 61801
pardesh2@illinois.edu

Lawrence Zhao†
University Laboratory High School
University of Illinois at Urbana-Champaign, IL 61801
lyzhao2@illinois.edu

Abstract

We construct two different primality proofs: one using trial divisions, the other using Pratt Certificates. Both proofs are visually implemented in JavaScript and Python and show that Pratt Certificates are efficient certifying algorithms while trial division proofs are not. However, this efficiency comes at a cost of additional proof obligations.

Keywords Pratt certificate, certifying algorithm, computational complexity.

1 Introduction

Definition 1. *A natural number $n \in \mathbb{N}_{\geq 2}$ is* composite *if*

$$\exists a, b \in \mathbb{N}_{\geq 2} \text{ s.t. } n = a \cdot b.$$

If such a and b exist, they are called factors *of n.*

Definition 2. *A natural number $n \in \mathbb{N}_{\geq 2}$ is* prime *if it is not composite.*

Definition 3. *A natural number $a \in \mathbb{N}_{\geq 2}$ is a* prime factor *of n if a is a factor of n and a is prime.*

If n is composite, it is possible to create a rectangular arrangement of dots with a rows and b columns. Such a diagram constitutes a *proof without words*[1] for the compositeness of n.

For composite numbers, *factorization diagrams* [Yor12, VW12] go one step further and not only prove that n is composite but also show the prime factorization

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} = \prod_{k=1}^{M} {p_k}^{e_k},$$

$p_i \in \{primes\}$.

Without loss of generality, let $p_1 \leq p_2 \leq \cdots \leq p_k$, where p_1 through p_k make up the prime factorization of n.

As seen in Figure 1, for composite numbers, each prime factor p is represented as the verticies of a regular p-gon. The diagrams are constructed by first drawing a p_1-gon, where each vertex is a dot. Then, we recursively draw a regular p_k-gon where each vertex is a p_{k-1}-gon for all of the remaining $k-1$ factors of n, serving as proofs of compositeness. In order to reduce the size of the composite proof, we have combined $2 \cdot 2$ to form a square with 4 dots.

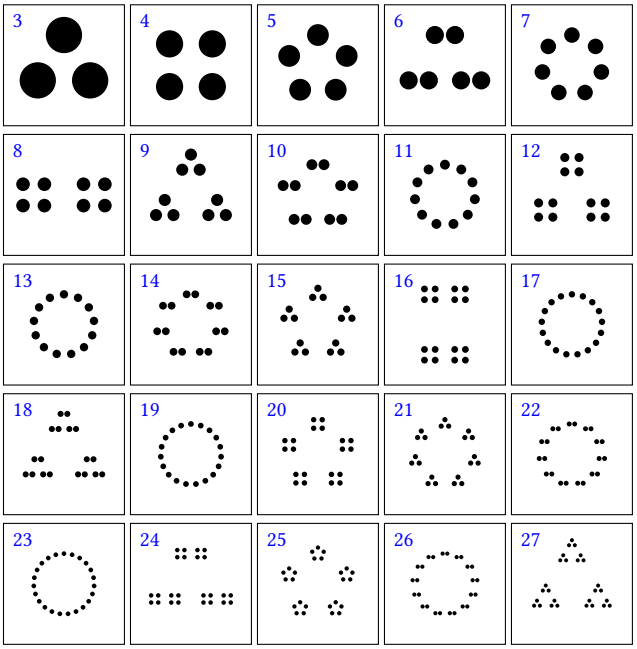

Figure 1. Factorization diagrams for $n \in \{3, \ldots, 27\}$: for composite n, prime factors are represented by visual arrangement, proving n is composite. If n is prime, no such arrangement exists and a regular n-gon (approximating a circle) is drawn instead and the diagram does *not* prove n is prime.

However, for n which are prime, the above factorization diagrams fail to constitute proofs of primality. The prime figures are drawn as a ring of n dots. But any composite c could also be drawn as a ring. So, a diagram that is a ring of dots is ambiguous and does not qualify as a proof.

2 Proof Method 1: Elementary Approach

Definition 2 yields a basis to construct diagrams which constitute a visual proof of primality (where the factorization diagrams fail in the prime cases):

$$\neg \left(\exists a, b \in \mathbb{N}_{\geq 2} \text{ s.t. } n = a \cdot b\right) \tag{1}$$

$$\forall a, b \in \mathbb{N}_{\geq 2} \text{ s.t. } n \neq a \cdot b \tag{2}$$

*Pratt primality certificates in Haskell and Python.
†Primality visualizations in Javascript.
[1] https://en.wikipedia.org/wiki/Proof_without_words

Pardeshi and Zhao are mentored by Dr. Bertram Ludäscher.

NCSA-SPIN Internship, May 2019, University of Illinois, Urbana-Champaign
2019. ACM ISBN …$15.00
https://doi.org/\relax

Claim 1. *n is composite if $\exists a, b \in \mathbb{N}_{\leq \frac{n}{2}}$ s.t. $n = a \cdot b$*

Proof. We try to create the largest subset of $\mathbb{N}$ that factors a, b must be in. Assume n is composite. By (1), $b = \frac{n}{a}$. To maximize the subset, we let a be as small as possible. The smallest value we include is 2, which means b is $\frac{n}{2}$. Thus, to test for compositeness, we perform trial divisions of $a = \{2, 3, \ldots \lfloor \frac{n}{2} \rfloor\}$. If we find an a that produces a natural number b, n is composite. By (2), we test for primality by performing the same trial divisions. n is prime if no $a \in \{2, 3, \ldots \lfloor \frac{n}{2} \rfloor\}$ produces a natural b. □

Figure 2. Here, $n = 19$. a ranges from 2 to $\lfloor \frac{n}{2} \rfloor = 9$. Since none of the figures are perfect rectangles as each subfigure contains "leftover" red dots, we conclude 19 is prime.

This primality test leads to a basic visual proof, as shown in Figure 2. Each subfigure has a columns, representing a trial division, with a ranging from 2 to $\lfloor \frac{n}{2} \rfloor$.

This bound can be improved to only testing $a \in \{2, 3, \ldots \lfloor \sqrt{n} \rfloor\}$.

Claim 2. *If n is composite, there exists a factor a of n s.t. $a \leq \lfloor \sqrt{n} \rfloor$.*

Proof. Without loss of generality, let $a \leq b$, where a is a factor of n and $a > \sqrt{n}$.

$$a \cdot b = n$$

$$b = \frac{n}{a}$$

$$\frac{n}{a} < \frac{n}{\sqrt{n}} \Rightarrow b < \sqrt{n},$$

a contradiction. So, a must be a factor less than or equal to $\sqrt{n}$.

□

This leads to a condensed visual proof shown in Figure 3.

We observe that for larger and larger numbers n, the elementary diagrams become large very quick. Specifically, the number of diagrams is $O(\sqrt{n})$, and each subfigure has n dots. To verify a figure, all $n \cdot \sqrt{n}$ dots must be counted, making the verification of such a proof $O(n^{1.5})$. We note that the generation time is also $O(n^{1.5})$.

[VW12]
2

[2]Derived from www.datapointed.net/2012/10/animated-factorization-diagrams

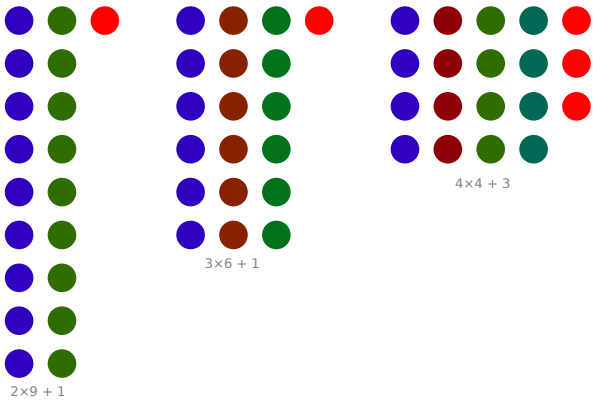

Figure 3. Here, $n = 19$. a ranges from 2 to $\lfloor \sqrt{n} \rfloor = 4$. Since none of the figures are perfect rectangles, we conclude 19 is prime.

3 Proof Method 2: Pratt Certificates

In 1974, Vaughan Pratt showed that every prime number has a succinct certificate [Pra74]. In particular, he showed that prime factorization lies in the complexity class NP. This means his certificates can be confirmed correct in polynomial time. But how much better are Pratt Certificates than the elementary proofs?

We can quantify the difference between the two types of primality proofs with the notion of certifying algorithms. An algorithm A that outputs a solution and proof to a problem is a *certifying algorithm*. A is an *efficient* certifying algorithm if

$$O(A) + O(P) = O(N) \tag{3}$$

where P is a proof checker and N is the fastest non-certifying algorithm for the same problem.

A Python3 implementation of Pratt Certificates has been tested and Figure 4 shows Pratt Certificates qualify as efficient certifying algorithms. Figure 5 shows that the trial-division proof is not an efficient certifying algorithm.

4 Implications of Logical Structure

The trial-division proof is based on a "for all" qualifier, as seen in its definition. No matter how tight the bound we consider, the proof will always be comparatively long. The compactness of the Pratt Certificate can be explained by examining its logical structure:

Let p be the set of prime factors of $n - 1$. n is prime if

$$\exists a \text{ s.t. } a^{n-1} \equiv 1 \mod n \wedge a^{\frac{n-1}{p_i}} \not\equiv 1 \mod n,$$

where $p_i \in p$.

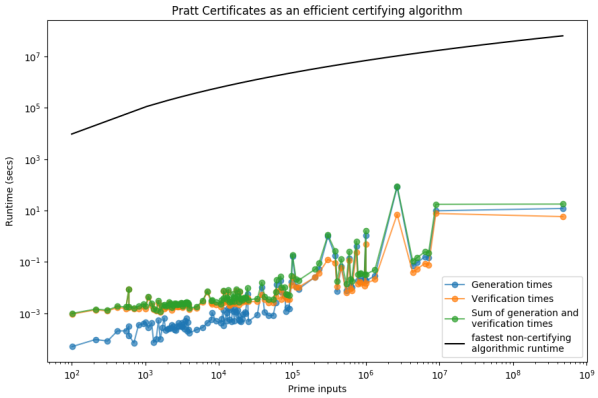

Figure 4. Note how the combined runtimes of the generation and verification of the Pratt Certificates are less than the fastest non-certifying algorithm: $O(\log(x)^6)$ given by the Elliptic Curve Primality Test.

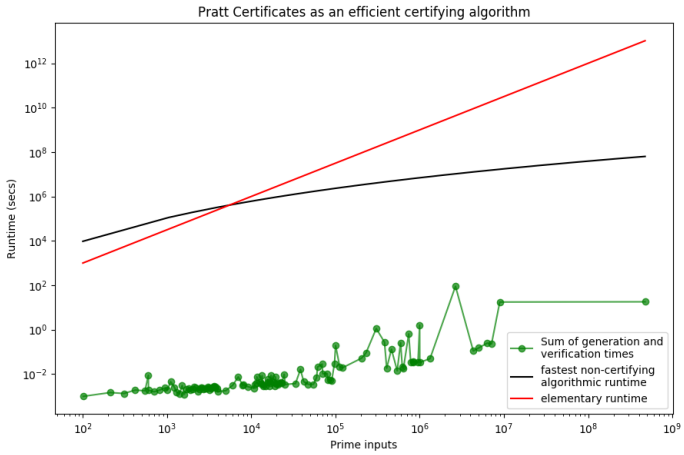

Figure 5. The red curve representing the elementary proof's runtime is $y = 2x^{1.5}$, since the generation and verification times are both $x^{1.5}$. Note the runtimes grow faster than the non-certifying algorithm, meaning the elementary proof is not an efficient certifying algorithm.

The existential qualifier in Pratt's logical statement shortens the resulting proof to at most $4\lceil \log_2(n) \rceil$ lines [Pra74].

However, there is an implicit tradeoff between the two proofs. The compactness of Pratt Certificates are only made possible by the additional mathematical machinery they use, including modular arithmetic, exponentiation, and Fermat's Little Theorem. Therefore, the reader must understand fairly complex mathematical concepts before they can accept a Pratt Certificate as valid.

On the other hand, the elementary proofs are very intuitive. This can be attributed to the fact that they rely on multiplication and addition, making them more obvious.

References

[Pra74] V. Pratt. Every Prime Number Has a Succinct Certificate, July 1974. https://doi.org/10.1137/0204018https://doi.org/10.1137/0204018.

[VW12] S. Von Worley. Dance, Factors, Dance – A Variation On Yorgey's Factorization Diagrams, October 2012. www.datapointed.net/2012/10/animated-factorization-diagrams.

[Yor12] B. Yorgey. Factorization Diagrams, October 2012. mathlesstraveled.com/2012/10/05/factorization-diagrams.