Forum of Mathematics, Sigma (2026), **Vol. 14**:e49 1–45
doi:10.1017/fms.2026.10194

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Feasibility of primality in bounded arithmetic

Raheleh Jalali[1] and Ondřej Ježil[2]

[1]Department of Computer Science, University of Bath, Bath, United Kingdom;
E-mail: rjk53@bath.ac.uk (Corresponding author).
[2]Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic; E-mail: ondrej.jezil@email.cz.

Received: 23 April 2025; **Revised:** 23 January 2026; **Accepted:** 23 January 2026

2020 Mathematics Subject Classification: *Primary* – 03F30, 03D15; *Secondary* – 11C08, 13F20, 11T06, 11A51

Abstract

We prove the correctness of the AKS algorithm [1] within the bounded arithmetic theory T_2^{count} or, equivalently, the first-order consequences of the theory VTC^0 expanded by the smash function, which we denote by VTC^0_2. Our approach initially demonstrates the correctness within the theory $S^1_2 + \mathrm{iWPHP}$ augmented by two algebraic axioms and then shows that they are provable in VTC^0_2. The two axioms are: a generalized version of Fermat's Little Theorem and an axiom adding a new function symbol which injectively maps roots of polynomials over a definable finite field to numbers bounded by the degree of the given polynomial. To obtain our main result, we also give new formalizations of parts of number theory and algebra:

- In PV_1: We formalize Legendre's Formula on the prime factorization of $n!$, key properties of the Combinatorial Number System and the existence of cyclotomic polynomials over the finite fields $\mathbb{Z}/p$.
- In S^1_2: We prove the inequality $\mathrm{lcm}(1,\ldots,2n) \geq 2^n$.
- In VTC^0: We verify the correctness of the Kung–Sieveking algorithm for polynomial division.

Contents

1 Introduction **2**
2 Preliminaries **3**
2.1 Bounded arithmetic and the theories in question . . . 3
2.2 Algebraic primitives in bounded arithmetic . . . 6
3 The AKS algorithm and its correctness **8**
3.1 Proof of the correctness . . . 8
3.2 Overview of our formalization . . . 9
4 Cyclotomic polynomials over finite fields in PV_1 **10**
4.1 Formalization of algebraic structures . . . 10
4.2 Existence of Cyclotomic extensions . . . 12
4.3 The Root Upper Bound axiom . . . 18
5 The correctness in $S^1_2 + \mathrm{iWPHP} + \mathrm{RUB} + \mathrm{GFLT}$ **19**
5.1 $\mathrm{PV}_1 \vdash$ Legendre's formula . . . 19
5.2 Lemma C . . . 22
5.3 Lemma D . . . 24
5.4 Congruence Lemma . . . 25
5.5 Lemma E . . . 27

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

5.6 Lemma F 30
5.7 Lemma G 35
5.8 Lemma H 37
5.9 The correctness 38
6 VTC^0_2 proves S^1_2 + iWPHP + RUB + GFLT **38**
6.1 Σ^B_1-definability of algebraic operations 39
6.2 The binomial theorem and provability of GFLT 39
6.3 Division of high degree polynomials and provability of RUB 42
7 Concluding remarks **44**
References **45**

1. Introduction

In 2002 the first deterministic polynomial-time algorithm for primality testing was found — the AKS algorithm (named after its creators Agrawal, Kayal, and Saxena) [1]. The containment PRIMES $\in$ **P** can be interpreted as saying: "Primality is a *feasible* property". The general question we are treating in this work is:

- How feasible can a proof of the statement PRIMES $\in$ **P** be?

More concretely, since the AKS algorithm is currently the only known primality testing algorithm unconditionally running in deterministic polynomial time, the particular way we interpret this question is to ask:

- How feasible can a proof of the correctness of the AKS algorithm be?

The feasibility of a proof here is captured by concepts from proof complexity, namely from the field of bounded arithmetic. The theories of bounded arithmetic, which are treated in depth in ([15], [6]), are comparatively weak subtheories of Peano arithmetic. Each such theory, in some precise technical sense, corresponds to reasoning with concepts from a concrete complexity class — the theory corresponding to polynomial-time (or *feasible*) reasoning being PV_1. There is already a rich body of results formalizing the correctness of various algorithms and parts of complexity theory in PV_1 and its extensions ([20],[17],[13],[5],[8]), the main motivation being:

- *Bounded reverse mathematics*: Formalizing known mathematics in such theories provides insight into the intrinsic power of these theories and into the feasibility of the underlying constructions. For more details, see [18, 4, 19].
- *Propositional translations*: Provability of sharply bounded formulas in a bounded arithmetic theory T gives a specific proof system corresponding to T in which all propositional tautologies expressing the formula for inputs of various lengths can be efficiently proved.
- *Witnessing results*: Provability of a suitable existential formula in a bounded arithmetic theory T can give an algorithm computing the witness in the complexity class C corresponding to the theory T.

Regarding primality testing, Jeřábek has proved the correctness of the Rabin–Miller primality test in S^2_2 + iWPHP(PV) + PHP(PV) [14, 12].

By the correctness of the AKS algorithm, we mean the statement

$$(\forall x)(\mathrm{Prime}(x) \leftrightarrow \mathrm{AKSPRIME}(x)),$$

where $\mathrm{Prime}(x)$ is the usual Π^b_1-formula defining primality and $\mathrm{AKSPRIME}(x)$ is a predicate stating that the AKS algorithm claims that the number x is a prime. Herbrand's theorem readily implies that if

$$\mathrm{PV}_1 \vdash (\forall x)(\mathrm{Prime}(x) \rightarrow \mathrm{AKSPRIME}(x)),$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

then there is a polynomial-time algorithm for factoring integers, which seems highly unlikely. This conditional unprovability result is not the only obstacle in formalizing the proof. While the original proof is relatively elementary, it still involves number-theoretic and algebraic statements, which were so far untreated in the context of bounded arithmetic. We show that the correctness of the AKS algorithm for primality testing can be proved in the bounded arithmetic theory T_2^{count} by first showing that it can be proved in $S_2^1 + \text{iWPHP}$ enriched by two algebraic axioms. The first axiom is *Generalized Fermat's Little Theorem* (Definition 2.2), which asserts that the polynomials $(\mathcal{X} + a)^p$ and $(\mathcal{X}^p + a)$ are congruent modulo any polynomial $\mathcal{X}^r - 1$ modulo p, where r is of logarithmic size. The second axiom is called *Root Upper Bound*, RUB (Section 4.3): it essentially axiomatizes a new function symbol, which provides an injective function from the roots of the polynomial f into the set $\{1, \ldots, \deg f\}$, which we then allow to appear in the formulas of the schemes axiomizing the base theories PV_1, S_2^1 and T_2. As additional background on formalizing complexity-theoretic statements in bounded arithmetic, it is worth noting that [2] formalizes the Schwartz-Zippel Lemma[1] in S_2^1. They also formalize $\text{FTA}_{\leq}$, half of Fundamental Theorem of Algebra, in S_2^1 [2, Lemma 3.2.]. Let us compare $\text{FTA}_{\leq}$ and our axiom RUB. We see that $\text{FTA}_{\leq}$ works for small-degree univariate polynomials in small-size fields and constructively lists all roots. RUB handles arbitrary-degree sparse polynomials and provides an injective indexing of roots. $\text{FTA}_{\leq}$ is stronger constructively within its limited domain, but RUB applies to cases $\text{FTA}_{\leq}$ cannot handle, making it essential for general sparse polynomial reasoning.

Along the way, we prove in PV_1 Legendre's theorem (Theorem 5.10), the existence of *cyclotomic extensions* of finite fields $\mathbb{Z}/p$ (Theorem 4.18) and the correctness of the combinatorial number system (Lemma 5.32), in S_2^1 the bound $\text{lcm}(1, \ldots, 2n) \geq 2^n$ (Corollary 5.17), and in VTC^0 the correctness of the Kung–Sieveking algorithm (Lemma 6.10) for polynomial division, which could be of independent interest.

Another notable point is that the formalized proofs closely follow the original AKS proofs, preserving their core combinatorial and number-theoretic structure. This shows that bounded arithmetic can naturally capture these fundamental results without requiring major changes to the underlying arguments.

2. Preliminaries

2.1. Bounded arithmetic and the theories in question

In this section, we recall basic facts about the theories relevant to our formalization. We refer the reader interested in a comprehensive treatment of bounded arithmetic to [15].

The minimal language we consider is Buss' language L_{S_2} [3] used in the original definition of the theory S_2^1 (see below). The language L_{S_2} consists of the nonlogical symbols $\{0, S, +, \cdot, \leq, \#, \lfloor x/2 \rfloor, |x|\}$ and all the usual logical symbols. The symbols $0, S, +, \cdot, \leq$ are the zero constant, the successor function, addition, multiplication, and the less-than-or-equal-to relation. The intended meaning of $\lfloor x/2 \rfloor$ is to divide by two and round down, and $|x|$ is $\lceil \log_2(x+1) \rceil$, which is the length of the binary representation of x. We define $x\#y = 2^{|x| \cdot |y|}$. The behavior of these symbols is axiomatized by the 32 universal axioms of BASIC (see [3, Section 2.2]). As we will only consider logarithms base 2, from now on, by $\log x$, we mean $\log_2(x)$. Denote $S(0)$ by 1. The L_{S_2}*-terms* and L_{S_2}*-formulas* are defined as usual.

A *bounded quantification* of the free variable x in an L_{S_2}-formula $\varphi(x)$ is either of the following

$$(\forall x \leq t)(\varphi(x)) \equiv (\forall x)(x \leq t \rightarrow \varphi(x))$$
$$(\exists x \leq t)(\varphi(x)) \equiv (\exists x)(x \leq t \wedge \varphi(x)),$$

where t is an L_{S_2}-term that does not contain x. We call the quantifiers of the above form *bounded*. We say a quantifier is *sharply bounded* if it is bounded and the term t is of the form $|s|$ for some term s. A *(sharply) bounded formula* in the language L_{S_2} is simply a formula in which every quantifier is

[1] Schwartz-Zippel Lemma states that if a low-degree multivariate polynomial with coefficients in a field is not zero everywhere in the field, then it has few roots on every finite subcube of the field.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

(sharply) bounded. The set of all bounded formulas is denoted Σ^b_∞. An L_{S_2}-formula is $\Sigma^b_0 = \Pi^b_0$ if all its quantifiers are sharply bounded. An L_{S_2}-formula is Σ^b_1 (resp. Π^b_1) if it is constructed from sharply bounded formulas using conjunction, disjunction, sharply bounded quantifiers and existential (resp. universal) bounded quantifiers.

The theory S^1_2 is axiomatized over BASIC by the polynomial induction schema Σ^b_1-PIND for any Σ^b_1-formula φ:

$$\varphi(0) \wedge \forall x(\varphi(\lfloor x/2 \rfloor) \to \varphi(x)) \to \varphi(a),$$

or alternatively by the length minimization schema Σ^b_1-LMIN:

$$\varphi(a) \to (\exists x \leq a)(\forall y \leq a)(\varphi(x) \wedge (|y| < |x| \to \neg\varphi(y))$$

for any Σ^b_1-formula φ, or by the length maximization schema Σ^b_1-LMAX:

$$\varphi(0) \to (\exists x \leq a)(\forall y \leq a)(\varphi(x) \wedge (|x| < |y| \to \neg\varphi(y)))$$

for any Σ^b_1-formula φ. The theory T_2 is axiomatized over BASIC by the induction schema Σ^b_∞-IND:

$$\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(x+1)) \to \forall x\varphi(x).$$

for any Σ^b_∞-formula, or equivalently bounded formula φ.

Throughout this paper, we shall use the richer language of Cook's theory PV [7] and of the theory PV_1 [16], which contains function symbols for every polynomial-time algorithm. In particular, this language includes L_{S_2}. With a slight abuse of notation, we also use PV to refer to this richer language. We will simply refer to these function symbols for polynomial-time algorithms as PV-*symbols*. We shall sometimes treat them as predicates, which we call PV-*predicates*. The intended meaning of a PV-predicate is that a corresponding PV-symbol for the characteristic function of the predicate outputs 1. The definitions of Σ^b_1, Π^b_1, and Σ^b_∞ can be extended to this new language by allowing the terms and open formulas to be in PV. These classes of formulas are called $\Sigma^b_1(\mathrm{PV})$, $\Pi^b_1(\mathrm{PV})$, and $\Sigma^b_\infty(\mathrm{PV})$, and the expanded theories $S^1_2(\mathrm{PV})$ and $T_2(\mathrm{PV})$. However, with a slight abuse of the notation, we use Σ^b_1, Π^b_1, and Σ^b_∞, S^1_2, and T_2.

The weakest theory we consider is PV_1, first defined in [16] as a conservative extension of Cook's equational theory[2] PV [7]. The theory PV_1, a universal first-order theory, formalizes polynomial-time reasoning in the language of PV. It is shown in [15] that PV_1 proves Σ^b_0-IND. We say that the formula A is Δ^b_1-*definable* in a theory R if there are formulas $B \in \Sigma^b_1$ and $C \in \Pi^b_1$ such that $A \leftrightarrow B$ and $A \leftrightarrow C$ are provable in the theory R. Every PV-function can be Δ^b_1-defined in S^1_2, hence we can see S^1_2 as an extension of PV_1 (see [3]). Also, using Buss' witnessing theorem [3], we can see that S^1_2 is $\forall\Sigma^b_1$-conservative over PV_1. Therefore, when we want to prove a $\forall\Sigma^b_1$-formula in PV_1, we can prove it in S^1_2. As mentioned earlier, we assume that S^1_2 is in the language PV. To prove the existence of prime factorization of numbers, it seems to be necessary to work in S^1_2 (see [10]).

Let us define an axiom schema, which we will use later. The injective weak pigeonhole principle iWPHP(PV) is the axiom schema

$$a > 0 \to \big((\exists x < 2a)(f(x) \geq a) \vee (\exists x < x' < 2a)(f(x) = f(x'))\big)$$

for each PV-symbol f. We will introduce two additional axiom schemata, the *Generalized Fermat's Little Theorem* (GFLT) and the *Root Upper Bound* (RUB), once we have defined all the required notions. The

[2]Another theory PV1 was introduced simultaneously with PV in [7], this theory uses the universal fragment of first order logic. Compare the notation to PV_1 which is a first order theory.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

axiom GFLT is treated in Definition 2.2, and the axiom RUB and the resulting theory S^1_2+iWPHP+RUB are treated in Section 4.3.

Another essential theory for us is the theory T^{count}_2. It consists of the theory $T_2(\text{PV})$ with its language extended by a recursively defined family of counting functions for each Σ^b_∞-formula A. Then, for each bounded formula, it contains the first level counting functions, and so on. We will not work with this theory directly. Instead, we will consider Σ^b_∞-consequences of the theory VTC^0_2 which are fully conservative over T^{count}_2 [15, essentially Lemma 13.1.2].

Let us now define the theory VTC^0_2. First, the theory V^0_2 is a two-sorted extension of T_2, where the first sort is the "*number sort*" denoted by lowercase variables $x, y, \ldots$ as in T_2, and the new "*set sort*" corresponds to binary strings whose bits are indexed by the number sort and is denoted by uppercase variables $X, Y, \ldots$. The language of V^0_2 is extended by an equality symbol for the set sort, the elementhood relation $x \in X$ between the number sort on the left and the set sort on the right, and the length symbol $|X|$, which takes as an input an element of the set sort and outputs an element of the number sort. The intended meaning of $|X|$ is the least strict upper bound on elements of X. There is one exception to the number sort and set sort notation: The name of an arbitrary bounded field will be denoted F despite bounded fields being objects of the number sort. Note that only in the language of V^0_2 we have two sorts (i.e., the number sort and the set sort), and we use the uppercase and lowercase letters to distinguish between them. However, in the language of PV, there is only one sort, i.e., the number sort. Therefore, when we are working in a theory in the language of PV, such as PV_1 or S^1_2, we freely use uppercase letters also to denote objects of the number sort.

A Σ^B_0-formula is a bounded formula in this new language without quantification of the set sort. Following [13], the theory V^0_2 can be axiomatized by T_2, the basic axioms

$$
\begin{aligned}
&|X| \neq 0 \rightarrow (\exists x)(x \in X \wedge |X| = x + 1)\\
&x \in X \rightarrow x < |X|\\
&(\forall x)((x \in X \leftrightarrow x \in Y) \rightarrow X = Y)
\end{aligned}
$$

and the comprehension schema for Σ^B_0-formulas. That is, for every Σ^B_0-formula φ, the following is an axiom schema,

$$(\exists X \leq x)(\forall u < x)(u \in X \leftrightarrow \varphi(u)) \qquad (\varphi\text{–COMP})$$

where a bounded quantification of an element of the set sort $(\exists Y \leq t)(\ldots)$ is interpreted as $(\exists Y)(|Y| \leq t \wedge \ldots)$.

Note that using sets, we can encode sequences of the elements of the number sort, $X^{(i)}$ being the i-th element of such encoding, where X is an element of the set sort and i an element of the number sort. We obtain the theory VTC^0_2 by extending V^0_2 by the axiom (CARD):

$$
\begin{aligned}
(\forall n)(\forall X)(\exists Y)(Y^{(0)} = 0 \wedge\\
(\forall i < n)((i \notin X \rightarrow Y^{(i+1)} = Y^{(i)}) \wedge\\
(i \in X \rightarrow Y^{(i+1)} = Y^{(i)} + 1)))
\end{aligned}
$$

In essence, the theory VTC^0_2 is a simple extension of the two-sorted theory VTC^0 originally defined in [6] by the smash function # for the number sort, and in our setting also by all PV-symbols for the number sort. In this work, we understand the theory VTC^0 as a theory whose axioms are the ones of VTC^0_2 which do not contain the symbol for the smash function #.

We say a formula in the language of VTC^0_2 is Σ^B_1 if it is equivalent over predicate calculus to a formula that contains only bounded number sort quantifications, bounded existential set sort quantification and no negations appear before any of the existential set sort quantifications. A function is Σ^B_1-definable in VTC^0_2 if its graph can be defined in the standard model using a Σ^B_1-formula $\varphi(X, Y)$ such that

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

$\mathrm{VTC}^0_2 \vdash (\forall X)(\exists!Y)\varphi(X,Y)$. It can be shown [6, Theorem IX.3.7.] that VTC^0_2 proves the comprehension axiom which we shall denote Σ^B_0(card)-COMP. This comprehension axiom allows the Σ^B_0-formulas to contain new function symbols each computing a Σ^B_1-definable function in VTC^0_2, similarly it proves the induction axiom Σ^B_0(card)-IND, which allows such formulas in the induction axiom.

2.2. *Algebraic primitives in bounded arithmetic*

Let us start with the formalization of elementary number theory and polynomial arithmetic in PV_1. For numbers x, y we denote x divides y by $x \mid y$. There is a well-behaved PV-symbol $x \bmod m$ which computes the remainder of x modulo m. The primality of a number x is defined by the Π^b_1-formula $\mathrm{Prime}(x)$:

$$x > 1 \wedge (\forall y \leq x)(y \mid x \rightarrow (y = 1 \vee y = x)).$$

Coding of both sets and sequences of elements can be developed in PV_1, here we will describe the main ideas. We use the notation $1^{(r)}$ to denote the number whose binary expansion consists of r-many ones, in other words, the number r is of logarithmic size. Coding of sets is simple, there is a well-behaved PV-symbol $\mathrm{bit}(x,i)$ which outputs the i-th bit of the number x, the elementhood relation $i \in x$ is then defined to be equivalent to $\mathrm{bit}(x,i) = 1$. Regarding sequences, a sequence $(a_1, \ldots, a_k)$, where $1^{(k)}$ exists, can be coded by a pair $\langle a, b\rangle$, with a consisting of a number whose binary expansion is the concatenation of the binary expansions of $a_1, a_2, \ldots, a_k$ and b is the number whose binary expansion contains 1 at the positions which correspond to the beginning of each a_i. We shall denote the pair $\langle a, b\rangle$ by $\langle a_1, \ldots, a_k\rangle$. More details on coding of sequences in PV_1 can be found in [15, Section 5.4]. Sums and products over sequences can also be defined by the obvious iterative algorithm. Such an algorithm obtains a sequence of numbers and outputs the iterated sum/product as a single number.

Let us note that sometimes we consider sets which are not neccesarily codeable in PV_1 but are definable by a formula: These are just abbreviations in the meta-language where we talk about a definable predicate as if it were the set of all elements which satisfy it. As such, definable sets are not quantifiable. Of special importance are sets of the form $\{x; C(x) = 1\}$ for a Boolean circuit C, as these can appear in the induction formulas. We always make it clear when a set is codeable as oppose to definable.

Polynomials are defined to be sequences of coefficients such that the number of coefficients is one more than the degree of the polynomial, with the addition, multiplication and composition defined as usual, division defined using the long division algorithm, and exponentiation modulo some other polynomial defined using exponentiation by squaring. *Divisibility* of polynomials is defined as usual, the notation $f \mid g$ meaning that the polynomial f divides g. A polynomial is called *irreducible* if it cannot be written as a product of two polynomials, both having positive degrees. We will sometimes call polynomials formalized like this *low degree polynomials*, as their degree is bounded by a number of logarithmic size. Later in this section we will define a second formalization of polynomials in a two sorted theory, and we will call polynomials following this second formalism high degree polynomials.

The basic properties of the *greatest common divisor* (gcd) of numbers are essential for many arguments. The following is well-known (see [12]):

Lemma 2.1 (PV_1, Euclid's algorithm). *There is a* PV*-function symbol* gcd *such that* PV_1 *proves*

$$\begin{aligned}&\gcd(x,y) \mid x\\ &\gcd(x,y) \mid y\\ &(z \mid x \wedge z \mid y) \rightarrow (z \mid \gcd(x,y)),\end{aligned}$$

and also a PV*-function symbol xgcd for which* PV_1 *proves*

$$(xgcd(x,y) = (g,u,v)) \rightarrow (g = \gcd(x,y) \wedge g = ux + vy).$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Throughout this work, we introduce PV-symbols by declaring their name and properties inside the Lemma environment. Therefore, in the subsequent parts of this work, gcd and xgcd in any extension of PV_1 denote specific PV-symbols which satisfy the statement of the Lemma 2.1. We are now ready to define the first algebraic axiom we need for our formalization. Throughout the paper, we will use calligraphic uppercase letters $\mathcal{X}, \mathcal{Y}, \ldots$ for formal variables of polynomials.

Definition 2.2 (Generalized Fermat's Little Theorem). Let GFLT be the natural Σ^b_1-sentence formalizing the following statement, where the exponentiation of polynomials is given by a PV-symbol for exponentiation by repeatedly squaring modulo the polynomial $\mathcal{X}^r - 1$.

> Let p be a prime, and a and $1^{(r)}$ be numbers such that $\gcd(a, p) = 1$ and $r < p$. Then
> $$(\mathcal{X} + a)^p \equiv \mathcal{X}^p + a \pmod{p, \mathcal{X}^r - 1}.$$

The validity of GFLT follows in a sufficiently strong meta-theory by applying binomial theorem to the expresison $(\mathcal{X} + a)^p$ and considering which coefficients are divisible by p, this gives us $(\mathcal{X} + a)^p \equiv \mathcal{X}^p + a \pmod{p}$ which we take modulo $\mathcal{X}^r - 1$. Since there are exponentially many monomials in the expansion of $(\mathcal{X} + a)^p$, it is not clear how to adapt the proof strategy in PV_1 even if we assume the ordinary Fermat's Little Theorem as an axiom.

Let us now discuss the formalization of algebraic concepts in VTC^0_2. As an extension of T_2, all function and relational symbols on the number sort are carried over from PV_1. More interesting is the case of arithmetical operations over the set sort, where we interpret the set X as a number $\sum_{u \in X} 2^u$. Already V^0_2 can prove the totality and basic properties of addition and ordering. However, multiplication is TC^0-complete. Thus, it is known that V^0_2 cannot prove it is total as this would contradict known lower bounds against AC^0. Coding of sequences of elements of the set sort can be developed in VTC^0_2, with i-th element of a sequence S being $S^{[i]}$. It is also well-known that VTC^0_2 can prove the totality and basic properties of multiplication. Moreover, VTC^0_2 can Σ^B_1-define iterated addition $\sum_{i<n} X^{[i]}$ and prove

$$\sum_{i<0} X^{[i]} = 0,$$
$$\sum_{i<n+1} X^{[i+1]} = X^{[n]} + \sum_{i<n} X^{[i]}.$$

Only recently has Jeřábek [13] shown that VTC^0_2 can also Σ^B_1-define iterated multiplication and prove the analogous recursive properties. This also implies that it can define the division of integers.

Theorem 2.3 [13]. *VTC^0 can Σ^B_1-define iterated products $\prod_{i<n} X^{[i]}$ and prove the iterated multiplication axiom IMUL:*

$$\prod_{i<0} X^{[i]} = 1,$$
$$\prod_{i<n+1} X^{[i+1]} = X^{[n]} \cdot \prod_{i<n} X^{[i]}.$$

Moreover, VTC^0 can Σ^B_1-define a function $\lfloor X/Y \rfloor$ such that it proves

$$Y \neq 0 \to \lfloor X/Y \rfloor \cdot Y \leq X < (\lfloor X/Y \rfloor + 1) \cdot Y.$$

Finally, let us treat polynomials encoded by elements of the set sort as a sequence of coefficients, where each coefficient is an element in the number sort, which we shall call *high degree polynomials*. The totality of addition of high-degree polynomials is straightforward, and using iterated addition, the

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

totality of their multiplication can be proved in VTC^0. We will observe in Theorem 6.11 that the Kung-Sieveking TC^0-algorithm as presented in [9] for the division of polynomials can also be proved correct in VTC^0_2 which also implies the totality of division for high degree polynomials.

3. The AKS algorithm and its correctness

Algorithm 1 The AKS algorithm [1]

Input: $n \geq 0$
Output: Whether n is `COMPOSITE` or `PRIME`.

1: Check whether $n = p^k$ for some $p \geq 0, k > 1$, if yes output `COMPOSITE`.
2: Find the first r such that $\mathrm{ord}_r(n) > \lfloor \log n \rfloor^2$.
3: If some $a \leq r$ has $1 < \gcd(a, n) < n$, then output `COMPOSITE`.
4: If $n \leq r$, output `PRIME`.
5: For $a = 0, \ldots, \lfloor \sqrt{\phi(r)} \rfloor \cdot \lfloor \log n \rfloor$:
6: If $(\mathcal{X} + a)^n \not\equiv \mathcal{X}^n + a \bmod (\mathcal{X}^r - 1, n)$: output `COMPOSITE`.
7: Output `PRIME`.

3.1. *Proof of the correctness*

We begin by providing a high-level overview of the proof of correctness of the AKS algorithm (Algorithm 1) [1], here $\mathrm{ord}_r(n)$ is the multiplicative order of n modulo r and log is the base 2 logarithm. In doing so, we restate and give new alphabetical names to key Lemmas and Theorems of [1] to avoid confusion with the numbering in our work. The key number-theoretic statement behind the algorithm is the following:

Lemma (A) [1, Lemma 2.1]. *Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$ and $\gcd(a, n) = 1$. Then n is prime if and only if*

$$(\mathcal{X} + a)^n \equiv \mathcal{X}^n + a \pmod{n}.$$

The AKS algorithm essentially emerges as an effectivization of this characterization of primality. As testing for this equality explicitly requires comparing objects of size exponential in $|n|$, the AKS algorithm instead checks the equality modulo a low degree polynomial $\mathcal{X}^r - 1$ for polynomially many values of a. Since the statement of this lemma cannot even be expressed in the language of PV, in the formalization, we instead supplement it by the GFLT axiom. This axiom is what remains of Lemma A by keeping the only if direction and taking the equality mod $\mathcal{X}^r - 1$ for r polynomial in $|n|$.

This axiom implies the following direction of the correctness.

Lemma (B) [1, Lemma 4.2]. *If n is prime, the algorithm returns prime.*

Next, the goal is to prove that the number r, which is essentially found by brute force in the AKS algorithm, always exists and has size polynomial in $|n|$. This is Lemma D, which is, in turn, proved using Lemma C. Here, we use the symbol lcm to denote the function computing the least common multiple.

Lemma (C) [1, Lemma 3.1]. *Let $LCM(m)$ denote the lcm of the first m numbers. Then for $m \geq 7$:*

$$LCM(m) \geq 2^m.$$

Lemma (D) [1, Lemma 4.3]. *There exists an $r \leq max\{3, \lceil log^5 n \rceil\}$ such that $ord_r(n) > \lfloor log\, n \rfloor^2$.*

We use slightly different bounds in our formalization, but they are always polynomially related to the original ones.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

From now on, we assume that on the input n the AKS algorithm answered PRIME. We take r from the statement of Lemma D and fix some prime $p \mid n$ such that $\mathrm{ord}_r(p) > 1$, the rest of the proof consists of showing that $n = p$. Furthermore, we fix the number $\ell = \left\lfloor \sqrt{\phi(r)} \right\rfloor \cdot \lfloor \log n \rfloor$.

The proof then continues by defining the concept of *introspectivity*.

Definition [1, Definition 4.4]. For a polynomial $f(\mathcal{X})$ and a number $m \in \mathbb{N}$, we say that m is *introspective* for $f(\mathcal{X})$ if

$$[f(\mathcal{X})]^m \equiv [f(\mathcal{X}^m)] \pmod{\mathcal{X}^r - 1}.$$

Lemma (E) [1, Lemmas 4.5 and 4.6]. *If m and m' are introspective for $f(\mathcal{X})$, then so is $m \cdot m'$. Moreover if m is introspective for $f(\mathcal{X})$ and $g(\mathcal{X})$ then it is also introspective for $f(\mathcal{X}) \cdot g(\mathcal{X})$*

Together Lemma A and our assumptions about n and p imply that $\frac{n}{p}$ and p are both introspective for all $(\mathcal{X} + a)$, $0 \le a \le \ell$. Lemma F then allows us to show that for the sets $I = \{(\frac{n}{p})^i p^j; i, j \ge 0\}$ and $P = \{\prod_a (\mathcal{X}+a)^{e_a}; e_a \ge 0\}$ it holds that every number from I is introspective for every polynomial in P.

Now we finally define $G = I \bmod r$ and $\mathcal{G} = P \bmod h$, where h is an irreducible factor of the cyclotomic polynomial Q_r over the field $\mathbb{F}_p$. After setting $t = |G|$, we can state the last two technical Lemmas.

Lemma (F) [1, Lemma 4.7]. $|\mathcal{G}| \ge \binom{t+\ell}{t-1}$

Lemma (G) [1, Lemma 4.8]. *If n is not a power of p, then $|\mathcal{G}| \le n^{\lfloor \sqrt{t} \rfloor}$.*

Since the AKS algorithm checks whether n is a perfect power and we assume that it is not (otherwise, the algorithm outputs COMPOSITE), we get that both bounds on $\mathcal{G}$ hold. By showing they are incompatible we obtain:

Lemma (H) [1, Lemma 4.9]. *If the algorithm returns PRIME, then n is a prime.*

Putting Lemma B and Lemma H together, we get:

Theorem [1, Theorem 4.1]. *The AKS algorithm outputs PRIME if and only if the number n is a prime.*

3.2. Overview of our formalization

Let us start with the formalization of the AKS algorithm as a PV-symbol. The algorithm begins by checking whether the number on the input is not a perfect power; this can be checked in polynomial time, and the algorithm as a PV-symbol can be proved correct in PV_1.

Lemma 3.1. *There is a* PV*-symbol* PerfectPower *for which* PV_1 *proves:*

$$(\forall x)(\mathit{PerfectPower}(x) \leftrightarrow ((x \le 1) \vee (\exists a, y \le x)(|y| > 1 \wedge a^{|y|} = x)))$$

Proof. The PV-symbol PerfectPower can be constructed to follow the procedure: For each value of $b \in \{1, \ldots, |x| + 1\}$, use binary search to find a value of a such that $a^b = x$ or continue if no such value exists. Such values for a and b will be found if and only if such values exist, which is equivalent to the existence of a and $y = 1^{(b)}$ such that $a^{|y|} = x$. □

Next, one has to fix some upper bound for the number r, which is polynomial in $|n|$. We will later prove in S^1_2 that such a bound exists. For convenience, let us also assume that the algorithm actually checks for the slightly stronger $\mathrm{ord}_r(n) > |n|^2$. We show this stronger assumption is justified in Lemma 5.19 by the same argument as in [1]. For any natural number r, the function $\phi(r)$ is *Euler's totient function* which outputs the number of numbers less than r that are relatively prime to r. The value $\phi(r)$ can be computed by a PV-symbol which obtains $1^{(r)}$ on the input (see Lemma 4.5). The function $\lfloor \sqrt{x} \rfloor$ can be computed by a binary search for the value y which satisfies $y^2 \le x < (y+1)^2$. The function $\lfloor \log x \rfloor$ is exactly equal to $|x| - 1$. All of these algorithms can be straightforwardly formalized as PV-symbols.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Altogether, the AKS algorithm can be formalized as a PV-symbol AKSPrime, which outputs 1 if and only if the algorithm would output `PRIME`. By the correctness of the AKS algorithm, we mean the sentence AKSCorrect:

$$(\forall x)(\text{AKSPrime}(x) \leftrightarrow \text{Prime}(x))$$

We prove the correctness by following the outline of the proof as in the previous section. For each Lemma or Theorem used in the formalization, we always strive to use the weakest possible theory for the given argument.

In Section 4, we show that S^1_2 proves the existence of cyclotomic extensions of finite fields. This is important later in the argument to prove the existence of the polynomial h.

For the formalization, we will use the following congruence property. Recall that we fixed the number r from Lemma D satisfying $r \leq \max\{3, \lceil \log^5 n \rceil\}$ and $\text{ord}_r(n) > \lfloor \log n \rfloor^2$. We also fixed $\ell = \left\lfloor \sqrt{\phi(r)} \right\rfloor \cdot \lfloor \log n \rfloor$.

Lemma (Congruence). *Let n be a number such that AKSPrime(n) holds, i.e., the AKS algorithm asserts that n is prime, and let r be the value provided by the algorithm satisfying $ord_r(n) > |n|^2$. Assume p is a prime divisor of n such that $ord_r(p) > 1$. And let us fix $\ell = \left\lfloor \sqrt{\phi(r)} \right\rfloor \cdot \lfloor log\, n \rfloor$. In S^1_2 + GFLT it holds that for every $0 \leq a \leq \ell$*

$$(\mathcal{X} + a)^{\frac{n}{p}} \equiv \mathcal{X}^{\frac{n}{p}} + a \pmod{\mathcal{X}^r - 1, p}.$$

We provide most of our formalization of the original proof in Section 5 in the theory S^1_2 + iWPHP + RUB + GFLT. We start in Section 5.1 by proving Legendre's formula in PV_1; we use it in Section 5.2 to prove our version of Lemma C, which is used in Section 5.3 to prove Lemma D. In Section 5.4, we prove the Congruence Lemma and in Section 5.5, we formalize the concept of introspectivity and prove Lemma E.

Since the property of a polynomial being in the group $\mathcal{G}$ is not easily formulated by a PV-predicate, we instead use the predicate $\hat{P}$ recognizing all those polynomials over F with degree at most r. Our version of Lemma F instead of an inequality states that there exists a function τ from $\{1, \ldots, \binom{t+\ell}{t-1}\}$ into $\hat{P}$, which satisfies $x \neq y \rightarrow \tau(x) \not\equiv \tau(y) \pmod{h, p}$. To prove Lemma F in Section 5.6, we first formalize the Combinatorial Number System, which assigns to each number $i \leq \binom{m}{k}$ a unique k-element subset of $\{1, \ldots, m\}$, when m is given in unary. Our version of Lemma G, which again replaces inequality by an existence of a function $g : \hat{P} \rightarrow n^{\lfloor \sqrt{t} \rfloor}$, with the property $f_1 \not\equiv f_2 \pmod{h, p} \rightarrow g(f_1) \neq g(f_2)$, is proved in Section 5.7 using the axiom RUB. We finish in Section 5.8 by proving Lemma H: the composition of the functions from Lemmas F and G results in an injective function which is in contradiction with the axiom iWPHP.

The remainder of the formalization is done in Section 6, where we prove that VTC^0_2 proves the consequences of S^1_2 + iWPHP + RUB + GFLT. We thus obtain that both VTC^0_2 and T^{count}_2 prove AKSCorrect.

4. Cyclotomic polynomials over finite fields in PV_1

4.1. Formalization of algebraic structures

In this section, we shall prove in PV_1 that over the finite fields $\mathbb{Z}/p$, where p is prime, there are r-th cyclotomic polynomials for arbitrary $r < p$ represented in unary. We also define a concept of *bounded fields* and use S^1_2 + GFLT to prove that the r-th cyclotomic extension of $\mathbb{Z}/p$ exists. Bounded fields are simply finite fields on a domain $[b] = \{0, \ldots, b-1\}$ for some number b, such that their operations are computed by boolean circuits. An analogous definition was already provided by Jeřábek in [11]; here, we make the possibility of the field operation being coded by a circuit an explicit part of the definition to allow quantification over bounded fields.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Definition 4.1 (PV_1). A *bounded field* is a tuple $(b, \tilde{0}, \tilde{1}, C_i, C_o, C_a, C_m)$ of elements, where C_i is a circuit computing $i : [b] \to [b]$, C_o is a circuit computing $o : [b] \setminus \{\tilde{0}\} \to [b] \setminus \{\tilde{0}\}$, C_a is a circuit computing $a : [b]^2 \to [b]$ and C_m is a circuit computing $m : [b]^2 \to [b]$ such that a as addition, m as multiplication, i as additive inverse and o as multiplicative inverse satisfy the field axioms on the universe $[b]$ with $\tilde{1}$ as the 1 element, and $\tilde{0}$ as the 0 element. That is, for all $x, y, z \in [b]$ we have

$$\begin{aligned}
a(x, a(y, z)) &= a(a(x, y), z) && \text{(associativity of } a\text{)}\\
m(x, m(y, z)) &= m(m(x, y), z) && \text{(associativity of } m\text{)}\\
a(x, y) &= a(y, x) && \text{(commutativity of } a\text{)}\\
m(y, x) &= m(y, x) && \text{(commutativity of } m\text{)}\\
a(x, \tilde{0}) &= x && \text{(neutrality of } \tilde{0}\text{)}\\
m(x, \tilde{1}) &= x && \text{(neutrality of } \tilde{1}\text{)}\\
a(x, i(x)) &= \tilde{0} && (i \text{ is the additive inverse})\\
m(a(x, y), z) &= a(m(x, z), m(y, z)), && \text{(distributivity)}
\end{aligned}$$

and for all nonzero $x \in [b]$:

$$m(x, o(x)) = \tilde{1}. \qquad (o \text{ is the multiplicative inverse})$$

When a bounded ring/field is understood from the context, we shall denote $a(x, y)$ as $x + y$, $m(x, y)$ as $x \cdot y$, $o(x)$ as x^{-1}, $i(x)$ as $-x$, $\tilde{1}$ as 1, and $\tilde{0}$ as 0.

Lemma 4.2 (PV_1). *If p is a prime, then $\mathbb{Z}/p = (p, 1, 0, C_i, C_o, C_a, C_m)$, where C_i, C_o, C_a, C_m are the circuits computing the appropriate operations modulo p is a bounded field.*

Proof. The existence of a multiplicative inverse follows from Lemma 2.1 and the rest is immediate. □

In sections 4 and 5, the usual name for a bounded field is F. Low degree polynomials over a bounded field F are defined as usual in PV_1, that is as sequences of elements of F of length equal to the degree of the polynomial plus one, and do not require special treatment. That is, for each bounded field F there is a PV-symbol which naturally encodes a predicate $f \in F[\mathcal{X}]$, we will therefore freely use this notation.

The following is straightforward, as the correctness of the Euclid's algorithm for polynomials can be proved analogously to the variant for integers.

Lemma 4.3 (PV_1, Euclid's algorithm). *Let F be a bounded field, then there are* PV*-symbols* gcd *and xgcd such that for any $f, g \in F[\mathcal{X}]$ we have*

$$\begin{aligned}
\gcd(f, g) &\in F[\mathcal{X}]\\
xgcd(f, g) &= (h, u, v)\\
h, u, v &\in F[\mathcal{X}]\\
h &= \gcd(f, g)\\
h &= uf + vg,
\end{aligned}$$

and

$$\begin{aligned}
&\gcd(f, g) \mid f\\
&\gcd(f, g) \mid g\\
&(\forall t \in F[\mathcal{X}])((t \mid f \wedge t \mid g) \to t \mid \gcd(f, g)).
\end{aligned}$$

Moreover, $\gcd(f, g)$ *is monic, that is the coefficient of the highest degree monomial is* 1.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Lemma 4.4 (PV_1). *For a bounded field F, and $f \in F[\mathcal{X}]$ irreducible low degree polynomial, there is a bounded field $F[\mathcal{X}]/(f)$ such that the ring operations are interpreted as on polynomial operations modulo f.*

Proof. This is immediate after identifying polynomials of degree less than $k = \deg f$ with numbers below b^k, where b is the bound of the field F. The existence of multiplicative inverse follows from Lemma 4.3. □

4.2. Existence of Cyclotomic extensions

We will start by proving basic properties of the Euler's totient function ϕ, which is definable in PV_1 for numbers represented in unary.

Lemma 4.5 (PV_1). *There is a* PV*-symbol* Tot*, such that* PV_1*-proves*

$$\mathrm{Tot}(1^{(r)}) = \sum_{\substack{1 \le i \le r \\ \gcd(i,r)=1}} 1,$$

we will simply denote the value $\mathrm{Tot}(1^{(r)})$ *as* $\phi(r)$.

Lemma 4.6 (PV_1). *Let $1^{(r)}$ be a number, and r be a prime, then $\phi(r) = r - 1$.*

Proof. Since r is a prime, then for $1 \le i < r$ we have $\gcd(i, r) = 1$ and these elements simply form the set $\{1, \ldots, r-1\}$ consisting of $r - 1$ elements. □

Definition 4.7 (PV_1). Let $1^{(r)}$ be a number and let $d \le r$. We define S^r_d to be the number coding the set $\{0 < m \le r; \gcd(r, m) = d\}$.

Lemma 4.8 (PV_1). *Let $1^{(r)}$ be a number and $d \mid r$, then $|S^r_d| = \phi(r/d)$.*

Proof. We will prove the lemma by showing that division by d defines a bijection between S^r_d and the set $S^{r/d}_1 = \{0 < m \le r/d; \gcd(r/d, m) = 1\}$.

Indeed, assume $m \in S^r_d$, if $\gcd(m/d, r/d) = a > 1$, then $a \cdot d$ is a common divisor of m and r, a contradiction with d being a greatest common divisor.

On the other hand, assume $m \in S^{r/d}_1$, if $\gcd(r, m \cdot d) = a \cdot d$, we get that $a \cdot d$ divides both $(r/d) \cdot d$ and $m \cdot d$, then a is a common divisor of r/d and m and thus $a = 1$. □

Lemma 4.9 (PV_1). *Let $1^{(r)}$ be a number, then $\sum_{d|r} \phi(d) = r$.*

Proof. We start with the observation that $\{1, \ldots, r\} = \bigcup_{d|r} S^r_d$. By taking the cardinality of both sides, we get

$$\begin{aligned} r &= \sum_{d|r} |S^r_d| \\ &= \sum_{d|r} \phi(r/d) && (\dagger) \\ &= \sum_{d|r} \phi(d), && (\ddagger) \end{aligned}$$

where (†) follows from Lemma 4.8 and (‡) follows from the fact that the map $d \mapsto r/d$ is an involution on the set of all divisors of r. □

We will now prove basic properties of polynomials over bounded fields which are needed to prove the existence of cyclotomic polynomials.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Lemma 4.10 (PV_1). *Let* $1^{(k)}$ *and* $1^{(l)}$ *be numbers,* $k, l \geq 1$ *such that* $k \mid l$. *Then,* $\mathcal{X}^k - 1 \mid \mathcal{X}^l - 1$, *over any bounded field.*

Proof. Assume that $l = km$. Then we have

$$\begin{aligned}(\mathcal{X}^k - 1)(\sum_{i=1}^{m} \mathcal{X}^{(m-i)k}) &= (\sum_{i=1}^{m} \mathcal{X}^{(m-i)k+k}) - (\sum_{i=1}^{m} \mathcal{X}^{(m-i)k}) \\ &= (\sum_{i=1}^{m} \mathcal{X}^{(m-i+1)k}) - (\sum_{i=1}^{m} \mathcal{X}^{(m-i)k}) \\ &= \mathcal{X}^l + (\sum_{i=2}^{m} \mathcal{X}^{(m-i+1)k}) - (\sum_{i=1}^{m-1} \mathcal{X}^{(m-i)k}) - 1 \\ &= \mathcal{X}^l + (\sum_{i=1}^{m-1} \mathcal{X}^{(m-i-1+1)k}) - (\sum_{i=1}^{m-1} \mathcal{X}^{(m-i)k}) - 1 \\ &= \mathcal{X}^l - 1.\end{aligned}$$

□

Lemma 4.11 (PV_1). *Let* F *be a bounded field,* $f, g, h \in F[\mathcal{X}]$ *and* $\gcd(g, h) = 1$, *then* $\gcd(fg, h) = \gcd(f, h)$.

Proof. bounded Assume that

$$\begin{aligned}\mathrm{xgcd}(g, h) &= (1, u, v) \\ \mathrm{xgcd}(f, h) &= (g_1, u_1, v_1) \\ \mathrm{xgcd}(fg, h) &= (g_2, u_2, v_2),\end{aligned}$$

we will show that $g_1 = g_2$. To prove that $g_2 \mid g_1$, we will multiply the equality $ug + vh = 1$ by g_1 to obtain

$$\begin{aligned}(ug + vh)g_1 &= g_1 \\ (ug + vh)(u_1 f + v_1 h) &= g_1 \\ ugu_1 f + ugv_1 h + vhu_1 f + vv_1 h^2 &= g_1 \\ fg(uu_1) + h(ugv_1 + vu_1 f + vv_1 h) &= g_1,\end{aligned}$$

and since g_2 is a common divisor of both fg and h, it is a divisor of g_1. Analogously, by multiplying the equality $ug + vh = 1$ by g_2 we obtain

$$\begin{aligned}(ug + vh)g_2 &= g_2 \\ (ug + vh)(u_2 fg + v_2 h) &= g_2 \\ ug^2 u_2 f + ugv_2 h + vhu_2 fg + vv_2 h^2 &= g_2 \\ f(ug^2 u_2) + h(ugv_2 + vu_2 fg + vv_2 h) &= g_2,\end{aligned}$$

and g_1 is a common divisor of both f and h, therefore a divisor of g_2. □

Lemma 4.12 (PV_1). *Let* $1^{(k)}$ *and* $1^{(l)}$ *be numbers,* $k, l \geq 1$, *then*

$$\gcd(\mathcal{X}^k - 1, \mathcal{X}^l - 1) = \mathcal{X}^{\gcd(k,l)} - 1,$$

over any bounded field.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Proof. By induction on $\max\{k,l\}$. If $\max\{k,l\} = 1$, the equality is trivial.

Assume that the statement holds for all instances where $\max\{k,l\} < s$ for some s, where $1^{(s)}$ exist, we will prove it for the case $\max\{k,l\} = s$. Without loss of generality, we can assume $k < l$, as the case $k = l$ is trivial. Note that this is an instance of the second mathematical induction for open formulas and it is available in PV_1 because the number $\max\{k,l\}$ is a length as the corresponding quantifier in the induction formula is sharply bounded.

Let r, q be numbers such that $l = qk + r$, and $r < k$, by Lemma 4.10 there is a polynomial f, such that $f \cdot (\mathcal{X}^k - 1) = (\mathcal{X}^{kq} - 1)$. We have

$$\begin{aligned} \mathcal{X}^l - 1 &= \mathcal{X}^{kq+r} - 1 \\ &= \mathcal{X}^r(\mathcal{X}^{kq} - 1) + \mathcal{X}^r - 1 \\ &= \mathcal{X}^r \cdot f \cdot (\mathcal{X}^k - 1) + \mathcal{X}^r - 1, \end{aligned}$$

and thus by Lemma 4.11

$$\gcd(\mathcal{X}^k - 1, \mathcal{X}^l - 1) = \gcd(\mathcal{X}^k - 1, \mathcal{X}^r - 1) = \mathcal{X}^{\gcd(k,r)} - 1 = \mathcal{X}^{\gcd(k,l)} - 1. \qquad \square$$

Lemma 4.13 (PV_1). *Let $1^{(k)}$ be a number for $k \geq 1$ and F be a bounded field. Let $\langle f_1, \ldots, f_k \rangle$ be a sequence of elements of $F[\mathcal{X}]$ and let $g \in F[\mathcal{X}]$ such that for all $i \in \{1, \ldots, k\}$ we have $\gcd(g, f_i) = 1$. Then $\gcd(g, \prod_{i=1}^{k} f_i) = 1$.*

Proof. By induction on k. The case where $k = 1$ is trivial. Assume the lemma holds for $k-1$, then

$$\begin{aligned} \gcd(g, \prod_{i=1}^{k} f_i) &= \gcd(g, f_k \prod_{i=1}^{k-1} f_i) \\ &= \gcd(g, \prod_{i=1}^{k-1} f_i) && (\dagger) \\ &= 1, && (\ddagger) \end{aligned}$$

where (†) follows from the previous line by Lemma 4.11 and (‡) follows from the induction hypothesis. $\square$

Lemma 4.14 (PV_1). *Let $1^{(k)}$ be a number for $k \geq 1$ and F be a bounded field. Let $\langle f_1, \ldots, f_k \rangle$ be a sequence of elements of $F[\mathcal{X}]$, such that we have $\gcd(f_i, f_j) = 1$ whenever $i \neq j$, and $g \in F[\mathcal{X}]$. If for every $1 \leq i \leq k$ we have $f_i \mid g$, then $\prod_{i=1}^{k} f_i \mid g$.*

Proof. By induction on k. For $k = 1$ the statement is trivial.

Assume that the statement holds for $k-1$, and that we want to prove it for the sequence $\langle f_1, \ldots, f_k \rangle$ and $g \in F[\mathcal{X}]$ satisfying for every $1 \leq i \leq k : f_i \mid g$ and also that for $i \neq j$ we have $\gcd(f_i, f_j) = 1$. Then for $h = \prod_{i=1}^{k-1} f_i$ we have $h \mid g$ and by Lemma 4.13 also $\gcd(h, f_k) = 1$. Assume that $\mathrm{xgcd}(h, f_k) = (1, u, v)$, therefore $uh + vf_k = 1$ and fix polynomials $s, t \in F[\mathcal{X}]$ satisfying $sh = g$ and $tf_k = g$.

Then we have

$$\begin{aligned} uh + vf_k &= 1 \\ uhg + vf_k g &= g \\ uhtf_k + vf_k sh &= g \\ hf_k(ut + vs) &= g, \end{aligned}$$

and thus $\prod_{i=1}^{k} f_k = hf_k \mid g$. $\square$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Definition 4.15 (PV_1). Let $1^{(k)}$ be a number for $k \geq 1$ and F be a bounded field. If $f \in F[\mathcal{X}]$ and $f = \sum_{i=0}^{k} a_i \mathcal{X}^i$ we define its *derivative* $f' \in F[\mathcal{X}]$ to be given by $\sum_{i=0}^{k-1} (i+1) a_{i+1} \mathcal{X}^i$.

Lemma 4.16 (PV_1). *Let F be a bounded field. If $f, g \in F[\mathcal{X}]$, then*

$$(f+g)' = f' + g'$$
$$(fg)' = f'g + fg'.$$

Proof. Straightforward. □

Lemma 4.17 (PV_1). *Let F be a bounded field, $f \in F[\mathcal{X}]$, and $\gcd(f, f') = 1$. If for $g \in F[\mathcal{X}]$: $g^2 \mid f$, then $\deg g = 0$.*

Proof. We proceed by proving the contrapositive. Assume $g^2 \mid f$ and $\deg g$ is at least 1. Then $f = hg^2$ and by Lemma 4.16 we have $f' = h'g^2 + 2hg'g$. Therefore $g \mid f'$ and thus $g \mid \gcd(f, f')$. Hence, $\gcd(f, f') \neq 1$. □

We are now ready to prove the existence of cyclotomic polynomials in PV_1, the proof we use differs from the standard proof by only using elementary concepts and thus not needing the definition of cyclotomic polynomials which uses the field of complex numbers.

Theorem 4.18 (PV_1). *There is a* PV*-symbol Cyc_p such that* PV_1 *proves that for every prime p, and every number $1^{(r)}$, $1 \leq r < p$, we have that $\mathrm{Cyc}_p(1^{(r)}) = Q_r$ is a degree $\phi(r)$ polynomial over $\mathbb{Z}/p$, such that*

$$Q_r \mid \mathcal{X}^r - 1,$$
$$\forall r' \in \{1, \ldots, r-1\} : \gcd(Q_r, X^{r'} - 1) = 1.$$

Proof. Let us first define $\mathrm{Cyc}_p(1^{(r)})$ to be either $\mathcal{X} - 1$ in the case that $r = 1$ and otherwise $\mathcal{X}^r - 1 / (\prod_{d|r, d<r} \mathrm{Cyc}_p(1^{(d)}))$, possibly discarding the remainder. In the rest of this proof, we will denote the value of $\mathrm{Cyc}_p(1^{(a)})$ by Q_a. We will later show that the product $\prod_{d|r, d<r} Q_d$ indeed divides $\mathcal{X}^r - 1$.

The proof continues by induction on the sharply bounded formula $\psi(r)$ which is formed as a conjunction of the following formulas:

- $(\forall r' \leq |1^{(r)}|)(r' \geq 1 \rightarrow (\mathcal{X}^{r'} - 1 = \prod_{d|r'} Q_d))$
- $(\forall r' \leq |1^{(r)}|)(r' \geq 1 \rightarrow (\deg Q_{r'} = \phi(r')))$
- $(\forall r_1, r_2 \leq |1^{(r)}|)((r_1 \neq r_2 \wedge r_1 \geq 1 \wedge r_2 \geq 1) \rightarrow \gcd(Q_{r_1}, Q_{r_2}) = 1)$.

The formula $\psi(r)$ is valid when $r = 1$, as $Q_1 = \mathcal{X} - 1$, and the third conjunct of $\psi(1)$ is vacuously true.

Now for the induction step assume that $\psi(r-1)$ is true. We will use it to prove $\psi(r)$. For distinct divisors d_1, d_2 of r which are not equal to r we have that $\gcd(Q_{d_1}, Q_{d_2}) = 1$ and by Lemma 4.10 every $d \mid r, d < r$ satisfies $Q_d \mid \mathcal{X}^d - 1 \mid \mathcal{X}^r - 1$, we can obtain by Lemma 4.14 that $\prod_{d|r, d<r} Q_d \mid \mathcal{X}^r - 1$.

Regarding the second conjunct, the induction hypothesis implies that

$$\deg \prod_{d|r, d<r} Q_d = \sum_{d|r, d<r} \phi(r),$$

by the definition of Q_r, we have that $\deg Q_r = r - \sum_{d|r, d<r} \phi(r)$ which is equal to $\phi(r)$ by Lemma 4.9.

To finish the induction step it remains to show that $\gcd(Q_r, Q_{r'}) = 1$ for every $1 \leq r' < r$. Assume that $g = \gcd(Q_r, Q_{r'})$, then

$$g \mid Q_r = \frac{\mathcal{X}^r - 1}{\prod_{d|r, d<r} Q_d} \qquad (\dagger)$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Let $r'' = \gcd(r, r')$, by Lemma 4.12 and the properties of gcd we have

$$g = \gcd(Q_r, Q_{r'}) \mid \gcd(\mathcal{X}^r - 1, \mathcal{X}^{r'} - 1) = \mathcal{X}^{\gcd(r,r')} - 1 = \prod_{d|r''} Q_d,$$

thus $g \mid \prod_{d|r''} Q_d \mid \prod_{d|r, d<r} Q_d$, combining this with (†) gives $g^2 \mid \mathcal{X}^r - 1$. This implies by Lemma 4.17 that $\deg g = 0$, as $r < p$ gives us $\gcd(\mathcal{X}^r - 1, r\mathcal{X}^{r-1}) = 1$. This concludes the induction step.

To obtain the statement of the theorem, it remains to prove the equality $\gcd(Q_r, \mathcal{X}^{r'} - 1) = 1$ for any $0 < r' < r$. By the third conjunct of $\psi(r)$ and Lemma 4.13 we have

$$\gcd(Q_r, \mathcal{X}^{r'} - 1) = \gcd(Q_r, \prod_{d|r'} Q_d) = 1.$$

□

Lemma 4.19 (S^1_2). *Let $1^{(k)}$ be a number for $k \geq 1$, F be a bounded field and $f \in F[\mathcal{X}]$. Then there is a sequence $\langle h_1, \ldots, h_k \rangle$ such that each h_i is a nonconstant irreducible member of $F[\mathcal{X}]$ and $\prod_{i=1}^k h_i = f$.*

Proof. By Σ^b_1-LMAX there is a longest sequence of nonconstant polynomials $\langle h_1, \ldots, h_n \rangle$ such that $\prod_{i=1}^n h_i = f$. The irreducibility of h_i's follows from the maximality of the length of the sequence. □

To prove the existence of the polynomial h from the proof of the correctness in [1], we will first prove some basic properties of exponentiation by squaring.

Lemma 4.20 (PV_1, Recursive property of the exponentiation by squaring). *Let $m \geq 1$ be a number, let p be a prime and let $1^{(r)}$ be a number and let f and g be polynomials, then $f^m \equiv f^{m-1} \cdot f \pmod{g, p}$.*

Proof. We will proceed by open polynomial induction on m. If $m = 1$, the statement is trivial.

For the induction step, we will assume the statement for $\lfloor m/2 \rfloor$. The case where there is l such that $m - 1 = 2l$ is trivial, as by the definition of exponentiation by squaring we have

$$f^m \equiv (f^l)^2 f \equiv f^{m-1} \cdot f \pmod{g, p}.$$

In the case where there is l such that $m = 2l$, then we have by definition of exponentiation by squaring

$$\begin{aligned} f^m &\equiv (f^l)^2 \pmod{g, p} \\ f^{m-1} &\equiv (f^{l-1})^2 \cdot f \pmod{g, p}, \end{aligned}$$

which implies

$$\begin{aligned} f^{m-1} f &\equiv (f^{l-1})^2 \cdot f^2 \\ &\equiv (f^{l-1} f)^2 \\ &\equiv (f^l)^2 \qquad (\dagger) \\ &\equiv f^m \pmod{g, p}, \end{aligned}$$

where (†) follows from the induction hypothesis. The second congruence can be proved analogously. □

Lemma 4.21 (PV_1, Divisor lemma). *Let p be a prime, l be a number and let f, g and g_0 be polynomials. If $g_0 \mid g$, then*

$$[f]^l_g \equiv [f]^l_{g_0} \pmod{g_0, p},$$

where $[f]^l_g$ and $[f]^l_{g_0}$ denote exponentiation by squaring modulo g and g_0 respectively.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Proof. By induction on l, if $l = 0$ the statement is trivial.

For the induction step, assume the statement holds for l. Then by Lemma 4.20 we have

$$[f]_g^{l+1} \equiv [f]_g^l \cdot f \pmod{g, p},$$

since $g_0 \mid g$, then also

$$\begin{aligned} [f]_g^{l+1} &\equiv [f]_g^l \cdot f \pmod{g_0, p} \\ &\equiv [f]_{g_0}^l \cdot f \pmod{g_0, p} && (*) \\ &\equiv [f]_{g_0}^{l+1} \pmod{g_0, p}, && (\ddagger) \end{aligned}$$

where (†) follows from Lemma 4.20 and (*) follows from the induction hypothesis. □

Lemma 4.22 (PV_1, Composition of congruences). *Let p be a prime and let l and k be numbers, and let f_1, f_2 and g be polynomials. If $f_1^l \equiv f_2 \pmod{g, p}$ then,*

$$(f_1^l)^k \equiv f_2^k \pmod{g, p}.$$

Proof. By induction on k. The case where $k = 0$ is true trivially.

Assume the statement holds for k. Then by Lemma 4.20

$$\begin{aligned} (f_1^l)^{k+1} &\equiv (f_1^l)^k \cdot f_1^l \\ &\equiv f_2^k \cdot f_1^l \\ &\equiv f_2^k \cdot f_2 \equiv f_2^{k+1} \pmod{g, p}. \end{aligned}$$

□

Lemma 4.23 (PV_1, Factor Theorem). *Let F be a finite field, $\alpha \in F$ and $f \in F[\mathcal{X}]$. Then $f(\alpha) = 0$ if and only if $\mathcal{X} - \alpha \mid f$.*

Proof. We will assume that $f(\alpha) = 0$ and prove that $\mathcal{X} - \alpha \mid f$, the other direction is immediate. By long division, there are $q, r \in F[\mathcal{X}]$, $\deg r < 1$ such that $f = q \cdot (\mathcal{X} - \alpha) + r$. After evaluating both sides at α, we get $0 = f(\alpha) = q(\alpha) \cdot (\mathcal{X} - \alpha) + r(\alpha) = r(\alpha)$, since $\deg r = 0$ it is a constant and therefore $r(\alpha) = r = 0$. Thus, $f = q \cdot (\mathcal{X} - \alpha)$. □

Corollary 4.24 ($S_2^1 + \mathrm{GFLT}$). *Let p be a prime and $1^{(r)}$ be a number such that $1 \leq r < p$ and $r \nmid p - 1$. Then there is an irreducible divisor h of $\mathcal{X}^r - 1$ over $\mathbb{Z}/p$, which does not divide $\mathcal{X}^{r'} - 1$ for any $0 < r' < r$ and $\deg h$ is at least 2.*

Proof. By Theorem 4.18, there is a polynomial Q_r which divides $\mathcal{X}^r - 1$ while satisfying $\gcd(Q_r, \mathcal{X}^{r'} - 1) = 1$ for any $0 < r' < r$. By Lemma 4.19 there is an irreducible factorization of $Q_r = \prod_{i=1}^k h_i$. The $h = h_1$ satisfies that it is a divisor of $\mathcal{X}^r - 1$ but not of any $\mathcal{X}^{r'} - 1$, where $0 < r' < r$. It remains to show that h is of degree at least 2.

Assume for contradiction that $\deg h = 1$, thus without loss of generality $h = \mathcal{X} - \alpha$, for some $\alpha \in \mathbb{Z}/p$. By the GFLT axiom, we have

$$(\mathcal{X} + \beta)^p \equiv \mathcal{X}^p + \beta \pmod{\mathcal{X}^r - 1, p},$$

for every $\beta \in \{0, \ldots, p - 1\}$. Since $\mathcal{X} - 1 \mid \mathcal{X}^r - 1$, Lemma 4.21 gives us

$$(\mathcal{X} + \beta)^p \equiv \mathcal{X}^p + \beta \pmod{\mathcal{X} - 1, p}. \qquad (*)$$

We also trivially have

$$\begin{aligned} \mathcal{X} &\equiv 1 \pmod{\mathcal{X} - 1, p} \\ \mathcal{X} + \beta &\equiv 1 + \beta \pmod{\mathcal{X} - 1, p}, \end{aligned}$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

by Lemma 4.22, we have that

$$\mathcal{X}^p \equiv 1^p \equiv 1 \pmod{\mathcal{X}-1, p}$$
$$(\mathcal{X}+\beta)^p \equiv (1+\beta)^p \pmod{\mathcal{X}-1, p},$$

which together with (*) gives us

$$(1+\beta)^p \equiv 1+\beta \pmod{\mathcal{X}-1, p}.$$

Thus, by a linear substitution we have in $\mathbb{Z}/p$ that $\beta^p = \beta$, which implies $\beta^{p-1} = 1$ for every $\beta \in \{0, \dots, p-1\}$.

Since $p - 1 = qr + m$, for some q and m, where $0 < m < r$, we have in $\mathbb{Z}/p$ that

$$1 = \alpha^{p-1} = \alpha^{qr} \cdot \alpha^m = \alpha^m,$$

and $\alpha^m \neq 1$ as this would imply by Lemma 4.23 that $h = \mathcal{X} - \alpha$ divides $\mathcal{X}^m - 1$, which is a contradiction with the fact that h does not divide $\mathcal{X}^{r'} - 1$ for any $0 < r < r'$. □

4.3. The Root Upper Bound axiom

In the proof of Lemma G in [1], polynomials of degree polynomial in n are considered, as such they are not covered by the formalism of low degree polynomials. Polynomials with unrestricted degree can be defined over PV_1 in a limited way as follows.

A *sparse polynomial* is a list of pairs of monomials and coefficients, with the intended meaning being the polynomial consisting of the sum of those monomials with those coefficients. Note that the number of monomials in a sparse polynomial is bounded by the length of the list, therefore by a length of some number. For sparse polynomials, we can define addition, multiplication and evaluation at an element of a bounded field in PV_1. We will also use the notation $\deg f$ to denote the highest exponent of a monomial in the sparse polynomial f. In the rest of this section, we define the second algebraic axiom needed for our formalization which facilitates reasoning about sparse polynomials. It uses a new function symbol to provide the injection replacing the inequality between the number of roots of a polynomial over a field and the degree of the polynomial.

Definition 4.25 (Root Upper Bound). Let $\mathrm{PV}(\iota)$ denote the language of PV extended by a new ternary function symbol ι. The axiom RUB is the universal $\mathrm{PV}(\iota)$-sentence naturally formalizing the following statement.

> Let F be a bounded field and $f \in F[\mathcal{X}]$ be a sparse polynomial, then
>
> $$\iota(F, f, x) : \{\alpha \in F; f(\alpha) = 0\} \to [\deg f]$$
>
> is an injective function in the parameter x.

The injective function obtained from ι by fixing a bounded field F and a sparse polynomial $f \in F[\mathcal{X}]$ will be denoted $\iota_{F,f}$.

Since the axiom RUB introduces a new function symbol, we need to extend the axiom schemas to allow this new function symbol in the formulas that appear in them.

Definition 4.26. The theory $S^1_2(\iota) + \mathrm{RUB}(\iota)$ is the $\mathrm{PV}(\iota)$-theory extending S^1_2 by the axiom RUB and allowing the function symbol ι in the Σ^b_1-LMIN axiom scheme. The theory $S^1_2(\iota) + \mathrm{iWPHP}(\iota) + \mathrm{RUB}(\iota)$ is the $\mathrm{PV}(\iota)$-theory extending $S^1_2 + \mathrm{iWPHP}$ by the axiom RUB and by allowing the function symbol ι to be used in the formulas of the axiom scheme Σ^b_1-LMIN and extending iWPHP to allow $\mathrm{PV}(\iota)$-terms instead of just PV-symbols.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

For simplicity, we shall omit ι in the name of these theories and simply refer to them as $S^1_2 + \mathrm{RUB}$ and $S^1_2 + \mathrm{iWPHP} + \mathrm{RUB}$. By the name $S^1_2 + \mathrm{iWPHP} + \mathrm{RUB} + \mathrm{GFLT}$ we simply mean the theory extending $S^1_2 + \mathrm{iWPHP} + \mathrm{RUB}$ by the GFLT axiom.

5. The correctness in $S^1_2 + \mathrm{iWPHP} + \mathrm{RUB} + \mathrm{GFLT}$

5.1. $\mathrm{PV}_1 \vdash$ *Legendre's formula*

We start by proving Legendre's formula in PV_1; this is subsequently used to prove our variant of Lemma C — a lower bound on the value of $\mathrm{lcm}(1, \ldots, 2n)$ which is then used to prove our variant of Lemma D.

The following two Lemmas are straightforward and thus we omit their proofs.

Lemma 5.1. *There is a binary* PV*-symbol* $\nu_p(x)$ *for which* PV_1 *proves*

$$\begin{aligned} \nu_p(0) &= 0 \\ \nu_p(x) &= \begin{cases} \nu_p(\lfloor x/p \rfloor) + 1 & x \equiv 0 \pmod p \\ 0 & \textit{otherwise.} \end{cases} \end{aligned}$$

The value for $\nu_p(0)$ is often assigned to be ∞, but since we never use 0 as an argument, we simply defined it to be 0 to keep the function total.

The following lemma defines the bit-length factorial.

Lemma 5.2. *There is a* PV*-symbol* $Fact(x)$ *for which* PV_1 *proves*

$$\begin{aligned} Fact(0) &= 1, \\ Fact(x) &= Fact(\lfloor x/2 \rfloor) \cdot |x|, \end{aligned}$$

that is:

$$\mathbb{N} \models Fact(x) = |x|!$$

Lemma 5.3 (PV_1). *Let p be a prime and $x \cdot y \equiv 0 \pmod p$ then either $x \equiv 0 \pmod p$ or $y \equiv 0 \pmod p$.*

Proof. Assume that p is a prime, $xy \not\equiv 0 \pmod p$ and $x \not\equiv 0 \pmod p$. Then by the fact that p is prime we have $\gcd(x, p) = 1$ and $\mathrm{xgcd}(x, p) = (1, u, v)$ such that $ux + vp = 1$. Hence, $uxy + vpy = y$ and

$$y \equiv (uxy + vpy) \equiv uxy \equiv 0 \pmod p. \qquad \square$$

Lemma 5.4 (PV_1). *For every prime p and a number x there is x' such that $x = x' \cdot p^{\nu_p(x)}$, and $p \nmid x'$.*

Proof. We will first use induction on the formula $\psi_1(x)$:

$$i \le \nu_p(x) \to p^i \mid x.$$

The case where $i = 0$ is trivial. Assume $\psi(i)$ and $i + 1 \le \nu_p(x)$. By the inductive definition of $\nu_p(x)$, the case where $p^i \mid x$ but $p^{i+1} \nmid x$ is contradictory.

We will now use induction on the formula $\psi_2(x)$:

$$p^i \mid x \to \nu_p(x) = i + \nu_p(\lfloor x/p^i \rfloor).$$

Again, the case where $i = 0$ is trivial. Assume $\psi(i)$ and $p^{i+1} \mid x$, then

$$\begin{aligned} \nu_p(x) &= i + \nu_p(\lfloor x/p^i \rfloor) && (\dagger) \\ &= i + 1 + \nu_p(\lfloor x/p^{i+1} \rfloor). && (\ddagger) \end{aligned}$$

where (†) follows from the induction hypothesis, and (‡) follows from the definition of ν_p.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Together, we have established that

$$(\forall i)(i \leq \nu_p(x) \leftrightarrow p^i \mid x). \tag{$*$}$$

Let $k = \nu_p(x)$ and $x' = \lfloor x/p^k \rfloor$. From $(*)$ we get that $p^k \mid x$, thus $x = x'p^k$. Finally, if $p \mid x'$, then $p^{k+1} \mid x'p^k = x$, which by $(*)$ implies that $k = k + 1$, a contradiction. □

Lemma 5.5 (PV_1). *Let p be a prime, let x and y be numbers and let $\nu_p(y) = 0$. Then, $\nu_p(xy) = \nu_p(x)$.*

Proof. By Lemma 5.4 there is x' which is not divisible by p, such that $x = x'p^k$, where $k = \nu_p(p)$. We will proceed by induction on i on the formula

$$\nu_p(x'yp^i) = i.$$

Assume that $i = 0$. Since $p \nmid x'$ and $p \nmid y$, then by Lemma 5.3 $p \nmid x'y$, and thus $\nu_p(x'y) = 0$.
Now assume that $\nu_p(x'yp^i) = i$, then

$$\nu_p(x'yp^{i+1}) = \nu_p(\lfloor x'yp^{i+1}/p \rfloor) + 1 = \nu_p(x'yp^i) + 1 = i + 1,$$

which completes the induction step. By putting $i = k$, we get that

$$\nu_p(xy) = \nu_p(x'yp^k) = k = \nu_p(x).$$ □

Lemma 5.6 (PV_1). *For a prime p and $x, y > 0$ we have*

$$\nu_p(x \cdot y) = \nu_p(x) + \nu_p(y).$$

Proof. By Lemma 5.4 there are x' and y' not divisible by p such that

$$x = x'p^{\nu_p(x)}, \quad y = y'p^{\nu_p(y)}.$$

Then

$$\nu_p(xy) = \nu_p(x'y'p^{\nu_p(x)+\nu_p(y)}) = \nu_p(x) + \nu_p(y),$$

where the last equality follows from Lemma 5.5. □

Lemma 5.7 (PV_1). *For every $1^{(n)}$ and a prime p we have*

$$\nu_p(Fact(1^{(n)})) = \sum_{i=1}^{n} \nu_p(i).$$

Proof. By induction on n. The case $n = 0$ is obvious.
Assume the statement holds for n, then by Lemma 5.6:

$$\begin{aligned}
\nu_p(\mathrm{Fact}(1^{(n+1)})) &= \nu_p(\mathrm{Fact}(1^{(n)}) \cdot (n+1)) \\
&= \nu_p(\mathrm{Fact}(1^{(n)})) + \nu_p(n+1) \\
&= \sum_{i=1}^{n} \nu_p(i) + \nu_p(n+1) \\
&= \sum_{i=1}^{n+1} \nu_p(i).
\end{aligned}$$ □

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Lemma 5.8 (PV_1). *Let p be a prime and x be a number, then*

$$\nu_p(x) = \sum_{1 \le j \le |x|,\ p^j | x} 1.$$

Proof. By Lemma 5.4 there is x' such that $x = x' p^{\nu_p(x)}$. We will proceed by induction on the formula

$$\nu_p(x' p^i) = \sum_{1 \le j \le i;\ p^j | x} 1.$$

The case where $i = 0$ is trivial. Assume that the statement holds for i. Then, $\nu_p(x' p^{i+1}) = \nu_p(x' p^i) + 1 = i + 1$, which completes the induction step. The statement of the lemma is obtained by taking $i = \nu_p(x)$. □

Lemma 5.9 (PV_1). *Let $1^{(a)}$ and b be numbers, and $b \neq 0$. Then*

$$\sum_{i=1, b|i}^{a} 1 = \lfloor a/b \rfloor.$$

Proof. By induction on a. The case where $a = 0$ is trivial.

Assume that

$$\sum_{i=1, b|i}^{a} 1 = \lfloor a/b \rfloor,$$

if $b \mid a + 1$, then

$$\sum_{i=1, b|i}^{a+1} 1 = 1 + \sum_{i=1, b|i}^{a} 1 = 1 + \lfloor a/b \rfloor = \lfloor (a+1)/b \rfloor,$$

and if $b \nmid a + 1$, then

$$\sum_{i=1, b|i}^{a+1} 1 = \sum_{i=1, b|i}^{a} 1 = \lfloor a/b \rfloor = \lfloor (a+1)/b \rfloor.$$

□

We are now ready to prove Legendre's formula in PV_1. Our proof is a direct adaptation of a standard proof.

Theorem 5.10 (PV_1, Legendre's formula). *For every $1^{(n)}$ and a prime p we have*

$$\nu_p(\mathit{Fact}(1^{(n)})) = \sum_{i=1}^{|n|} \lfloor n/p^i \rfloor.$$

Proof. By direct computation:

$$\nu_p(\mathrm{Fact}(1^{(n)})) = \sum_{j=1}^{n} \nu_p(j) \tag{A}$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

$$= \sum_{j=1}^{n} \sum_{i, p^i \mid j} 1 \tag{B}$$

$$= \sum_{i=1}^{|n|} \sum_{1 \le j \le n; p^i \mid j} 1$$

$$= \sum_{i=1}^{|n|} \lfloor n/p^i \rfloor, \tag{C}$$

where (A) follows from Lemma 5.7, (B) follows from Lemma 5.8 and (C) follows from Lemma 5.9. □

5.2. *Lemma C*

Lemma 5.11 (S_2^1). *For every $n \geq 2$ there is a prime $p \leq n$ such that $p \mid n$.*

Proof. By Σ_1^b-LMIN we have

$$(\forall n)(\exists m \leq n)(\forall m' \leq n)((1 < n \wedge |m'| < |m|) \rightarrow (1 < m \wedge m \mid n \wedge m' \nmid n)).$$

Let $n > 1$ be a number, then we obtain m by the above formula. If m is not a prime, then there is $m' \mid m$, $1 < m'$ and $|m'| < |m|$, which is in contradiction with the formula. □

Lemma 5.12 (S_2^1). *For every n and m: if every prime $p \leq n$ satisfies that $\nu_p(n) \leq \nu_p(m)$, then $n \mid m$.*

Proof. Assume that n and m satisfy that $\nu_p(n) \leq \nu_p(m)$ for every prime $p \leq n$. Let $n' = \lfloor n/\gcd(m,n) \rfloor$ and $m' = \lfloor m/\gcd(m,n) \rfloor$. If $n' = 1$ then $n \mid m$, and we are done. We now prove that $n' > 1$ is impossible.

Assume for contradiction that $n' > 1$, therefore by Lemma 5.11 there is a prime p such that $p \mid n'$ and therefore $p \mid n$. If $\nu_p(m') > 0$, then $\gcd(m,n) \cdot p$ is a common divisor of both m and n, a contradiction with $\gcd(m,n)$ being the greatest common divisor. Therefore, we obtain that $\nu_p(m') = 0$.

Let $k = \nu_p(\gcd(m,n))$. Then by Lemma 5.6,

$$\nu_p(n) = \nu_p(n' \cdot \gcd(m,n)) \geq k+1 > k+0 = \nu_p(m' \cdot \gcd(m,n)) = \nu_p(m)$$

a contradiction. □

Lemma 5.13 (S_2^1). *For every $1^{(n)}$ we have that $(Fact(1^{(n)}))^2$ divides $Fact(1^{(2n)})$.*

Proof. Let p be a prime. By Lemma 5.6 and Theorem 5.10 we have

$$\nu_p(\mathrm{Fact}(1^{(n)})^2) = 2 \cdot \sum_{i=1}^{|n|} \lfloor n/p^i \rfloor.$$

Again by Theorem 5.10

$$\begin{aligned} \nu_p(\mathrm{Fact}(1^{(2n)})) &= \sum_{i=1}^{|2n|} \lfloor 2n/p^i \rfloor \\ &\geq \sum_{i=1}^{|2n|} 2 \cdot \lfloor n/p^i \rfloor \\ &\geq \nu_p(\mathrm{Fact}(1^{(n)})^2), \end{aligned}$$

which by Lemma 5.12 gives $\mathrm{Fact}(1^{(n)})^2 \mid \mathrm{Fact}(1^{(2n)})$. □

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Lemma 5.14. *There is a* PV*-symbol* $lcm(\langle x_1, \ldots, x_m\rangle)$*, such that* PV_1 *proves*

$$(\forall i \le m)\ (x_i \mid lcm(\langle x_1, \ldots, x_m\rangle))$$

and

$$(\forall y)((\forall i \le m)(x_i \mid y) \to lcm(\langle x_1, \ldots, x_m\rangle) \mid y).$$

Proof (Sketch). We can see that by putting

$$\mathrm{lcm}(\langle x_1, \ldots, x_m\rangle) = \begin{cases} 1 & m = 0, \\ 0 & \exists 1 \le i \le m : x_i = 0, \\ \left\lfloor \frac{\mathrm{lcm}(\langle x_1,\ldots,x_{m-1}\rangle)\cdot x_m}{\gcd(\mathrm{lcm}(\langle x_1,\ldots,x_{m-1}\rangle),x_m)} \right\rfloor & \text{otherwise,} \end{cases}$$

the required properties are satisfied. □

Lemma 5.15 (S^1_2). *For every* $1^{(n)}$*, we have*

$$\left\lfloor Fact(1^{(2n)})/Fact(1^{(n)})^2 \right\rfloor \mid lcm(1, \ldots, 2n).$$

Proof. Let p be a prime. By the length minimization principle for open PV-formulas[3], there is a minimal r such that $2n < p^{r+1}$. Notice that $r < |n| + 1$ and that $p^r \le 2n$.

By Lemma 5.13 we have

$$\mathrm{Fact}(1^{(2n)}) = \left\lfloor \mathrm{Fact}(1^{(2n)})/\mathrm{Fact}(1^{(n)})^2 \right\rfloor \cdot \mathrm{Fact}(1^{(n)})^2,$$

thus by Lemma 5.6

$$\nu_p(\left\lfloor \mathrm{Fact}(1^{(2n)})/\mathrm{Fact}(1^{(n)})^2 \right\rfloor) = \nu_p(\mathrm{Fact}(1^{(2n)})) - 2 \cdot \nu_p(\mathrm{Fact}(1^{(n)})).$$

Now by Theorem 5.10 we have

$$\begin{aligned} \nu_p(\left\lfloor \mathrm{Fact}(1^{(2n)})/\mathrm{Fact}(1^{(n)})^2 \right\rfloor) &= \sum_{i=1}^{|2n|} \lfloor 2n/p^i \rfloor - 2\sum_{i=1}^{|n|} \lfloor n/p^i \rfloor \\ &= \sum_{i=1}^{|n|+1} \lfloor 2n/p^i \rfloor - 2\sum_{i=1}^{|n|} \lfloor n/p^i \rfloor \\ &= \sum_{i=1}^{r} \lfloor 2n/p^i \rfloor - 2\sum_{i=1}^{r} \lfloor n/p^i \rfloor \qquad (*) \\ &= \sum_{i=1}^{r} (\lfloor 2n/p^i \rfloor - 2\lfloor n/p^i \rfloor) \\ &\le r, \qquad (\ddagger) \end{aligned}$$

where (*) follows because $\lfloor 2n/p^i \rfloor = 0$ for $i > r$ and (†) follows from the fact that $\lfloor 2n/p^i \rfloor - 2\lfloor n/p^i \rfloor \le 1$ for every $i \ge 0$. By the fact that $p^r \le 2n$ we have

[3]This is available in PV_1 by interating over the interval where we are checking for the least length.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

$$\nu_p(\mathrm{lcm}(1,\ldots,2n)) \geq r$$

and therefore by Lemma 5.12 the statement follows. □

Theorem 5.16 (S^1_2). *For every* $1^{(n)}$ *we have*

$$2^n \leq lcm(1,\ldots,2n).$$

Proof. By Lemma 5.15 it is enough to prove $2^n \leq \left\lfloor \mathrm{Fact}(1^{(2n)})/(\mathrm{Fact}(1^{(n)})^2) \right\rfloor$. We proceed by induction on n. For $n = 1$ the statement holds as

$$2^1 \leq 2!/(1!)^2 = 2.$$

Assume the inequality holds for n. Then

$$\begin{aligned}
\left\lfloor \mathrm{Fact}(1^{(2(n+1))})/\mathrm{Fact}(1^{(n+1)})^2 \right\rfloor 2 &= \left\lfloor \frac{\mathrm{Fact}(1^{(2n)})(2n+2)(2n+1)}{\mathrm{Fact}(1^{(n)})^2(n+1)^2} \right\rfloor \\
&\geq \left\lfloor \frac{\mathrm{Fact}(1^{(2n)})(2n+2)}{\mathrm{Fact}(1^{(n)})^2(n+1)} \right\rfloor \\
&= 2 \cdot \left\lfloor \mathrm{Fact}(1^{(2n)})/(\mathrm{Fact}(1^{(n)})^2) \right\rfloor \\
&\geq 2 \cdot 2^n = 2^{n+1}.
\end{aligned}$$

□

Corollary 5.17 (S^1_2, Lemma C). *For every* $1^{(m)}$ *we have*

$$2^{\lfloor m/2 \rfloor} \leq lcm(1,\ldots,m).$$

Proof. If $m = 2n$ for some n, then this is Theorem 5.16. Otherwise, $m = 2n+1$ for some n and $2^n \leq \mathrm{lcm}(1,\ldots,2n) \leq \mathrm{lcm}(1,\ldots,2n+1)$. □

5.3. Lemma D

The following Lemma defines order for multiplicative groups whose universe is bounded by a length. The restriction on the size makes all relevant arguments easily formalizable in PV_1 and thus we omit its proof.

Lemma 5.18. *There is a* PV*-symbol ORD such that* PV_1 *proves for every y and x satisfying* $\gcd(x,|y|) = 1$ *that*

$$ORD(y,x) = i \iff i > 0 \wedge y^i \equiv 1 \pmod{|x|} \wedge (\forall j < i)(y^j \not\equiv 1 \pmod{|x|}).$$

We will write $ord_r(y)$ *to denote* $ORD(y, 1^{(r)})$.

Lemma 5.19 (S^1_2, Lemma D). *For every* $x \geq 2$*, there is* $r \leq 2|x|^6$*, such that* $ord_r(x) > |x|^2$.

Proof. Notice, that $\mathrm{ord}_r(x) = i$ implies $r \mid (x^i - 1)$. Let

$$a = x^b \prod_{i=1}^{|x|^2} (x^i - 1) < x \cdot x^{|x|^4} < 2^{|x|^6},$$

where $b = |2|x|^6|$. By Corollary 5.17 we have

$$2^{|x|^6} \leq \mathrm{lcm}(1,\ldots,2\cdot|x|^6).$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Hence, $\operatorname{lcm}(1,\dots,2\cdot|x|^6)$ does not divide a. By Lemma 5.14 we have that there is $r \le 2\cdot|x|^6$ such that r does not divide a, and since this value is bounded by a length, we can take the smallest such r.

We will show that $\gcd(r,x)=1$. First, notice that from $r \le 2|x|^6$ it follows that for any prime p that $\nu_p(r) \le b$. Also for any prime p we have that $\nu_p(x) \ge 1$ implies $\nu_p(x^b) \ge b$.

Claim. There is a prime p such that $\nu_p(r) > \nu_p(a)$ and $\nu_p(x) = 0$.

Proof of claim. First, if $\nu_p(r) \ge 1$ and $\nu_p(x) \ge 1$, then

$$\nu_p(r) \le b \le \nu_p(x^b) \le \nu_p(a).$$

Since $r \nmid a$, then by Lemma 5.12 there is a prime p such that $\nu_p(r) > \nu_p(a)$, which cannot happen if $\nu_p(x) \ge 1$. This proves the claim.

Consider the value $r/\gcd(r,x)$, we have

$$\nu_p(r/\gcd(r,x)) = \nu_p(r) > \nu_p(a),$$

thus by Lemma 5.12 we have that $r/\gcd(r,x) \nmid a$. Since r was chosen as the smallest nondivisor of a, then $\gcd(r,x)=1$.

We claim that r has $\operatorname{ord}_r(x) > |x|^2$. If $\operatorname{ord}_r(x) \le |x|^2$ then there is $i \le |x|^2$ such that

$$r \mid (x^i - 1) \mid \prod_{i=1}^{|x|^2} (x^i - 1),$$

a contradiction. □

This lemma implies, that the `if` statement on line 4 of the AKS algorithm is relevant only for finitely many values. The case of correctness where this `if` statement results in the answer `COMPOSITE` can be ignored, because it can be expressed a true bounded sentence and thus proved in PV_1.

5.4. Congruence Lemma

Let us denote by $H_0(n,r)$ the following assumptions: n is a number such that $\mathrm{AKSPrime}(n)$ holds, i.e., the AKS algorithm asserts that n is prime, and r is the value provided by the algorithm satisfying $\operatorname{ord}_r(n) > |n|^2$.

We show that there is a prime divisor of n called p such that $\operatorname{ord}_r(p) > 1$.

Lemma 5.20 (S^1_2). *Assuming $H_0(n,r)$, there exists a sequence coding the prime factorization of n.*

Proof. By Σ^b_1-LMAX there is a longest sequence of numbers $\langle p_1,\dots,p_m\rangle$ such that $\prod_{i=1}^m p_i = n$ and for all i we have $p_i > 1$. The primality of p_i's follows from the maximality of the length of the sequence. □

Lemma 5.21 (S^1_2). *Assuming $H_0(n,r)$, there exists a prime divisor p of n such that $ord_r(p) > 1$.*

Proof. Assume that $\langle p_1,\dots,p_k\rangle$ is the prime factorization given by the previous lemma and assume for contradiction, that $\operatorname{ord}_r(p_i) = 1$ for all $i \le k$. Then $n = \prod_{i=1}^k p_i \equiv \prod_{i=1}^k 1 \equiv 1 \pmod r$, a contradiction. □

Let us fix p to be a prime divisor of n such that $\operatorname{ord}_r(p) > 1$. The rest of Section 5 is dedicated to showing that n satisfies $\mathrm{Prime}(n)$. To prove the congruence lemma we will use two simple properties of exponentiation by squaring.

Lemma 5.22 (PV_1, Evaluation lemma). *Let p be a prime, l be a number and let f_1, f_2 and g be low degree polynomials. Then,*

$$[f_1^l](f_2) \equiv ([f_1](f_2))^l \pmod{[g](f_2), p},$$

where $[g_1](g_2)$ denotes the composition of a polynomial g_2 with a polynomial g_1.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Proof. By induction on l. The case where $l = 0$ is true trivially.
Assume the statement holds for l. Then by Lemma 4.20

$$\begin{aligned}[f_1^{l+1}](f_2) &\equiv [f_1^l](f_2) \cdot [f_1](f_2)\\ &\equiv ([f_1](f_2))^l \cdot [f_1](f_2)\\ &\equiv ([f_1](f_2))^{l+1} \pmod{[g](f_2), p}.\end{aligned}$$

□

Lemma 5.23 (PV_1, Composition of exponentiation). *Let p be a prime and let l and k be numbers, and let f and g be low degree polynomials. Then,*

$$((f)^l)^k \equiv f^{l\cdot k} \pmod{g, p}.$$

Proof. By induction on k. The case where $k = 0$ is true trivially.
Assume the statement holds for k. Then by Lemma 4.20

$$\begin{aligned}((f)^l)^{k+1} &\equiv (f^l)^k \cdot f^l\\ &\equiv f^{l\cdot k} \cdot f^l\\ &\equiv f^{l\cdot k+l} \equiv f^{l\cdot(k+1)} \pmod{g, p},\end{aligned}$$

where the additivity of exponents also follows from Lemma 4.20 by straightforward induction. □

Lemma 5.24 (S_2^1 + GFLT, Congruence Lemma). *Assuming $H_0(n, r)$ and a being a number such that* $\gcd(a, p) = 1$*, we have:*

$$(\mathcal{X} + a)^{\frac{n}{p}} \equiv \mathcal{X}^{\frac{n}{p}} + a \pmod{\mathcal{X}^r - 1, p}.$$

Proof. By the notation $x \equiv y$, we mean $x \equiv y \pmod{\mathcal{X}^r - 1, p}$ throughout this proof. By $\mathrm{AKSPrime}(n)$ we have $(\mathcal{X} + a)^n \equiv \mathcal{X}^n + a \pmod{\mathcal{X}^r - 1, n}$. We have

$$(\mathcal{X} + a)^n \equiv \mathcal{X}^n + a \tag{1}$$

$$(\mathcal{X} + a)^p \equiv \mathcal{X}^p + a \tag{2}$$

The equivalence (1) follows from the fact that p is a prime divisor of n and (2) is an instance of the axiom GFLT. Since $r < p$ and p is prime, there exist u and v such that $\mathrm{xgcd}(r, p) = (1, u, v)$. Thus, $pv \equiv 1 \pmod{r}$. Without loss of generality, we can assume that $v > 0$, because otherwise, we can take $v' = v - rv > 0$. Since $\mathcal{X}^v$ is a low degree polynomial (as $v < r$), by substituting $\mathcal{X}^v$ for $\mathcal{X}$ in (1) using Lemma 4.21 and Lemma 5.22 we get

$$(\mathcal{X}^v + a)^n \equiv \mathcal{X}^{v\cdot n} + a.$$

To be concrete, by (1) we have:

$$[\mathcal{X} + a]^n_{\mathcal{X}^r-1} \equiv [\mathcal{X}]^n_{\mathcal{X}^r-1} + a \pmod{\mathcal{X}^r - 1, p} \tag{3}$$

By substituting $\mathcal{X}^v$ we get

$$[\mathcal{X} + a]^n_{\mathcal{X}^r-1}(\mathcal{X}^v) \equiv [\mathcal{X}]^n_{\mathcal{X}^r-1}(\mathcal{X}^v) + a \pmod{\mathcal{X}^{vr} - 1, p} \tag{4}$$

By Lemma 5.22:

$$[\mathcal{X} + a]^n_{\mathcal{X}^{vr}-1}(\mathcal{X}^v) \equiv [\mathcal{X}^v + a]^n_{\mathcal{X}^{vr}-1} \pmod{\mathcal{X}^{vr} - 1, p} \tag{5}$$

$$[\mathcal{X}]^n_{\mathcal{X}^{vr}-1}(\mathcal{X}^v) \equiv [\mathcal{X}^v]^n_{\mathcal{X}^{vr}-1} \pmod{\mathcal{X}^{vr} - 1, p} \tag{6}$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

By Lemma 4.21:

$$[\mathcal{X}^v + a]^n_{\mathcal{X}^{vr}-1} \equiv [\mathcal{X}^v + a]^n_{\mathcal{X}^r-1} \ (\mathrm{mod}\ \mathcal{X}^r - 1, p) \tag{7}$$

$$[\mathcal{X} + a]^n_{\mathcal{X}^{vr}-1} \equiv [\mathcal{X} + a]^n_{\mathcal{X}^r-1} \ (\mathrm{mod}\ \mathcal{X}^r - 1, p) \tag{8}$$

$$[\mathcal{X}^v]^n_{\mathcal{X}^{vr}-1} \equiv [\mathcal{X}^v]^n_{\mathcal{X}^r-1} \ (\mathrm{mod}\ \mathcal{X}^r - 1, p) \tag{9}$$

$$[\mathcal{X}]^n_{\mathcal{X}^{vr}-1} \equiv [\mathcal{X}]^n_{\mathcal{X}^r-1} \ (\mathrm{mod}\ \mathcal{X}^r - 1, p) \tag{10}$$

Therefore

$$\begin{aligned}
[\mathcal{X}^v + a]^n_{\mathcal{X}^r-1} &\equiv [\mathcal{X}^v + a]^n_{\mathcal{X}^{vr}-1} && \text{(by (7))}\\
&\equiv [\mathcal{X} + a]^n_{\mathcal{X}^{vr}-1}(\mathcal{X}^v) && \text{(by (5))}\\
&\equiv [\mathcal{X} + a]^n_{\mathcal{X}^r-1}(\mathcal{X}^v) && \text{(by (8))}\\
&\equiv [\mathcal{X}]^n_{\mathcal{X}^r-1}(\mathcal{X}^v) + a && \text{(by (4))}\\
&\equiv [\mathcal{X}]^n_{\mathcal{X}^{vr}-1}(\mathcal{X}^v) + a && \text{(by (10))}\\
&\equiv [\mathcal{X}^v]^n_{\mathcal{X}^{vr}-1} + a && \text{(by (6))}\\
&\equiv [\mathcal{X}^v]^n_{\mathcal{X}^r-1} + a \ (\mathrm{mod}\ \mathcal{X}^r - 1, p), && \text{(by (9))}
\end{aligned}$$

or simply $(\mathcal{X}^v + a)^n \equiv \mathcal{X}^{v\cdot n} + a$. By an analogous argument, we can use (2), Lemma 4.21 and Lemma 5.22 to get

$$(\mathcal{X}^v + a)^p \equiv \mathcal{X}^{v\cdot p} + a \equiv \mathcal{X} + a.$$

By Lemma 5.23, we obtain

$$((\mathcal{X}^v + a)^p)^{\frac{n}{p}} \equiv \mathcal{X}^{v\cdot n} + a. \tag{$*$}$$

Moreover, using Lemmas 4.22 and 5.23 we get:

$$\mathcal{X}^{v\cdot n} \equiv \mathcal{X}^{v\cdot p\cdot \frac{n}{p}} \equiv (\mathcal{X}^{v\cdot p})^{\frac{n}{p}} \equiv \mathcal{X}^{\frac{n}{p}}.$$

Therefore, by Lemma 4.22, $(*)$ will become

$$(\mathcal{X} + a)^{\frac{n}{p}} \equiv \mathcal{X}^{\frac{n}{p}} + a. \qquad \square$$

5.5. Lemma E

To prove Lemma E, let us first fix some notation. Let p be a prime divisor of n such that $\mathrm{ord}_r(p) > 1$. For the ease of notation, we will denote $\mathbb{Z}/p$ by F_p. By Corollary 4.24, for $F_p[\mathcal{X}]$ and r, there exists an irreducible divisor h of $\mathcal{X}^r - 1$ in $F_p[\mathcal{X}]$ such that $h \nmid \mathcal{X}^{r'} - 1$ for all $r' < r$ and $1 < \deg(h) < r$. Take such h and fix it and take $F = F_p[\mathcal{X}]/h(\mathcal{X})$. The following lemma introduces a set G_r represented by a PV-predicate, which will be used in the rest of the paper.

Lemma 5.25. *Assuming $H_0(n, r)$, there is a* PV*-symbol $G_r(x)$ such that* PV_1 *proves:*

$$G_r(x) \leftrightarrow (x < r) \wedge (\exists i, j \le r)(x \equiv (n/p)^i \cdot p^j \ (\mathrm{mod}\ r)).$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Proof. Suppose that the number x is given. First, we check that $x < r$. Then, for each $i, j \leq r$, check whether $x \equiv (n/p)^i \cdot p^j \pmod{r}$. If such i and j exist, then $G_r(x)$ holds. This argument can be formalized in PV_1 since by Lemma 5.19 we have $r \leq |n|^{10}$. □

We sometimes use the notation $m \in G_r$ to mean $G_r(m)$. By Lemma 5.19, the number r is bounded by $|n|^{10}$. The theory PV_1 can assign a cardinality to sets bounded by a length (and $|m|^{10}$ is the length of $s(m)$ for a suitable term s). We denote the cardinality of the set $\{x; G_r(x)\}$ by t, where $t < r$.

Lemma 5.26 (PV_1). *Assuming $H_0(n,r)$, we have $t = |G_r| \leq \phi(r)$.*

Proof. We already know

$$\gcd(n,r) = \gcd(p,r) = 1 \qquad \text{and hence} \qquad \gcd(n/p,r) = 1 \tag{*}$$

We claim that for any x such that $G_r(x)$ we have $\gcd(x,r) = 1$. As $G_r(x)$, there exist $i, j \leq r$ such that $x \equiv (n/p)^i \cdot p^j \pmod{r}$. Suppose for the sake of contradiction that $\gcd(x,r) = c$ where $c \neq 1$. Thus,

$$c \mid r \qquad \text{and} \qquad c \mid (n/p)^i \cdot p^j$$

If $i \leq j$ then $c \mid (n/p)^{i-j}$ which is a contradiction with $\gcd(n/p,r) = 1$. If $i < j$, then $c \mid n^i p^{j-i}$, which is a contradiction with the left side of (*). □

Lemma 5.27 (S^1_2). *Assume $H_0(n,r)$. Let f be a sparse polynomial and m a number. There is a ternary* PV*-predicate* $\mathrm{int}_{\mathcal{X}^r-1}(f,p,m)$ *for which S^1_2 proves*

$$\mathrm{int}_{\mathcal{X}^r-1}(f,p,m) \leftrightarrow \big(f(\mathcal{X})\big)^m \equiv f(\mathcal{X}^m) \pmod{\mathcal{X}^r - 1, p}.$$

The number m is called *introspective* for $f(\mathcal{X})$.

Let us fix $\ell = \left\lfloor \sqrt{\phi(r)} \right\rfloor \cdot \lfloor \log n \rfloor$. We have the following easy observation.

Lemma 5.28 (S^1_2+GFLT). *Assuming $H_0(n,r)$, both p and $\frac{n}{p}$ are introspective for $\mathcal{X}+a$ for any $0 \leq a \leq \ell$.*

Proof. By the axiom GFLT and Lemma 5.24. □

The following lemma combines Lemmas 4.5 and 4.6 in [1]. It proves the closure of introspective numbers under multiplication and also shows that the set of polynomials for which m is introspective is closed under multiplication.

Lemma 5.29 (S^1_2, Lemma E). *Assume $H_0(n,r)$. For any $f \in F[\mathcal{X}]$ and numbers m and m' if m and m' are introspective for $f(\mathcal{X})$ then so is $m \cdot m'$. Moreover, for any $f, g \in F[\mathcal{X}]$ and number m, if m is introspective for $f(\mathcal{X})$ and $g(\mathcal{X})$ then it is also introspective for $f(\mathcal{X}) \cdot g(\mathcal{X})$.*

Proof. As m is introspective for $f(\mathcal{X})$ we have by Lemma 4.22 and Lemma 5.23:

$$\big(f(\mathcal{X})\big)^{m \cdot m'} \equiv \big(f(\mathcal{X}^m)\big)^{m'} \pmod{\mathcal{X}^r - 1, p}. \tag{†}$$

Let $m = q \cdot r + m_r$, where $0 \leq m_r < r$. Then, by Lemma 4.20, Lemma 4.22, Lemma 5.23, and $\mathcal{X}^r \equiv 1 \pmod{\mathcal{X}^r - 1, p}$, we have:

$$\mathcal{X}^m \equiv \mathcal{X}^{q \cdot r + m_r} \equiv \mathcal{X}^{q \cdot r} \mathcal{X}^{m_r} \equiv (\mathcal{X}^r)^q \mathcal{X}^{m_r} \equiv 1^q \cdot \mathcal{X}^{m_r} \equiv \mathcal{X}^{m_r} \pmod{\mathcal{X}^r - 1, p},$$

which implies by Lemma 5.23

$$\mathcal{X}^{m_r \cdot m'} \equiv (\mathcal{X}^{m_r})^{m'} \equiv (\mathcal{X}^m)^{m'} \equiv \mathcal{X}^{m \cdot m'} \pmod{\mathcal{X}^r - 1, p}.$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

By Lemma 5.22 we have

$$[f(\mathcal{X}^{m_r})]^{m'}_{\mathcal{X}^{m_r\cdot r}-1} \equiv [f]^{m'}_{\mathcal{X}^{m_r\cdot r}-1}(\mathcal{X}^{m_r}) \pmod{\mathcal{X}^{m_r\cdot r}-1} \tag{A}$$
$$[\mathcal{X}^{m_r}]^{m'}_{\mathcal{X}^{m_r\cdot r}-1} \equiv [\mathcal{X}]^{m'}_{\mathcal{X}^{m_r\cdot r}-1}(\mathcal{X}^{m_r}) \pmod{\mathcal{X}^{m_r\cdot r}-1}. \tag{B}$$

As $\mathcal{X}^r - 1 \mid \mathcal{X}^{m_r\cdot r} - 1$, by Lemma 4.21:

$$[f]^{m'}_{\mathcal{X}^{m_r\cdot r}-1} \equiv [f]^{m'}_{\mathcal{X}^r-1} \pmod{\mathcal{X}^r-1, p}$$
$$[\mathcal{X}]^{m'}_{\mathcal{X}^{m_r\cdot r}-1} \equiv [\mathcal{X}]^{m'}_{\mathcal{X}^r-1} \pmod{\mathcal{X}^r-1, p}.$$

Moreover, by general algebra

$$[f]^{m'}_{\mathcal{X}^{m_r\cdot r}-1}(\mathcal{X}^{m_r}) \equiv [f]^{m'}_{\mathcal{X}^r-1}(\mathcal{X}^{m_r}) \pmod{\mathcal{X}^{m_r\cdot r}-1, p} \tag{C}$$
$$[\mathcal{X}]^{m'}_{\mathcal{X}^{m_r\cdot r}-1}(\mathcal{X}^{m_r}) \equiv [\mathcal{X}]^{m'}_{\mathcal{X}^r-1}(\mathcal{X}^{m_r}) \pmod{\mathcal{X}^{m_r\cdot r}-1, p}. \tag{D}$$

By the introspectivity of m'

$$[f]^{m'}_{\mathcal{X}^r-1} \equiv f([\mathcal{X}]^{m'}_{\mathcal{X}^r-1}) \pmod{\mathcal{X}^r-1, p}.$$

Then,

$$[f]^{m'}_{\mathcal{X}^r-1}(\mathcal{X}^{m_r}) \equiv f([\mathcal{X}]^{m'}_{\mathcal{X}^r-1})(\mathcal{X}^{m_r}) \pmod{\mathcal{X}^{m_r\cdot r}-1, p}.$$

By (C) and (A)

$$[f]^{m'}_{\mathcal{X}^r-1}(\mathcal{X}^{m_r}) \equiv [f]^{m'}_{\mathcal{X}^{m_r\cdot r}-1}(\mathcal{X}^{m_r}) \equiv [f(\mathcal{X}^{m_r})]^{m'}_{\mathcal{X}^{m_r\cdot r}-1} \pmod{\mathcal{X}^{m_r\cdot r}-1, p},$$

and by (D) and (B)

$$\begin{aligned} f([\mathcal{X}]^{m'}_{\mathcal{X}^r-1})(\mathcal{X}^{m_r}) &\equiv f([\mathcal{X}]^{m'}_{\mathcal{X}^{m_r\cdot r}-1}(\mathcal{X}^{m_r})) \\ &\equiv f([\mathcal{X}^{m_r}]^{m'}_{\mathcal{X}^{m_r\cdot r}-1}) \pmod{\mathcal{X}^{m_r\cdot r}-1, p}. \end{aligned}$$

Therefore, we have

$$\big(f(\mathcal{X}^{m_r})\big)^{m'} \equiv f((\mathcal{X}^{m_r})^{m'}) \pmod{\mathcal{X}^{m_r\cdot r}-1, p}.$$

Thus, by $\mathcal{X}^r - 1 \mid \mathcal{X}^{m_r\cdot r} - 1$ and Lemma 4.21 we have

$$\big(f(\mathcal{X}^{m_r})\big)^{m'} \equiv f(\mathcal{X}^{m_r\cdot m'}) \pmod{\mathcal{X}^r-1, p}.$$

By (†) we get $m \cdot m'$ is introspective for $f(\mathcal{X})$:

$$\begin{aligned} \big(f(\mathcal{X})\big)^{m\cdot m'} \equiv (f(\mathcal{X}^m))^{m'} &\equiv (f(\mathcal{X}^{m_r}))^{m'} \\ &\equiv f(\mathcal{X}^{m_r\cdot m'}) \equiv f(\mathcal{X}^{m\cdot m'}) \pmod{\mathcal{X}^r-1, p}. \end{aligned}$$

For the second part of the lemma, by Lemma 4.20 we have:

$$\big(f(\mathcal{X})\cdot g(\mathcal{X})\big)^m \equiv \big(f(\mathcal{X})\big)^m \cdot \big(g(\mathcal{X})\big)^m \equiv f(\mathcal{X}^m)\cdot g(\mathcal{X}^m) \pmod{\mathcal{X}^r-1, p}. \qquad \square$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

5.6. Lemma F

Recall that $H_0(n,r)$ denotes the following assumptions: n is a number such that AKSPrime(n) holds, i.e., the AKS algorithm asserts that n is prime, and r is the value provided by the algorithm satisfying $\mathrm{ord}_r(n) > |n|^2$. From now on, we let $H(n,r)$ denote the assumption $H_0(n,r)$ extended by fixing the following values:

- $\ell = \left\lfloor \sqrt{\phi(r)} \right\rfloor \cdot \lfloor \log n \rfloor$;
- $t = |G_r|$;
- p as a prime divisor of n such that $\mathrm{ord}_r(p) > 1$;
- $F_p = \mathbb{Z}/p$;
- an irreducible divisor h of $\mathcal{X}^r - 1$ in $F_p[\mathcal{X}]$ such that $h \nmid \mathcal{X}^{r'} - 1$ for all $r' < r$ and $1 < \deg(h) < r$;
- $F = F_p[\mathcal{X}]/h(\mathcal{X})$.

Recall that G_r is the set introduced in Lemma 5.25. We start with an easy observation about G_r.

Lemma 5.30 (S_2^1 + GFLT). *Assume $H(n,r)$. For any distinct elements m and m' of G_r we have*

$$\mathcal{X}^m \not\equiv \mathcal{X}^{m'} \pmod{h(\mathcal{X}), p}.$$

Proof. We prove the lemma by contraposition. Suppose

$$\mathcal{X}^m \equiv \mathcal{X}^{m'} \pmod{h(\mathcal{X}), p}.$$

Then, $h \mid \mathcal{X}^{m'} - \mathcal{X}^m$ and hence

$$h \mid \mathcal{X}^m \cdot (\mathcal{X}^{m'-m} - 1).$$

However, since $m' < r$ and $m \neq m'$, by Corollary 4.24 we have

$$h \nmid \mathcal{X}^{m'-m} - 1.$$

Therefore, $h \mid \mathcal{X}^m$. Since h is an irreducible polynomial, this means that $h(\mathcal{X}) = \mathcal{X}$. However, this contradicts the fact that $\deg(h) > 1$. Thus, we must have $m = m'$. □

The following are a series of lemmas necessary for the proof of Lemma F. To state the next lemma, we use the PV-symbol NumOnes(x) which counts the number of ones in the binary expansion of its argument.

Lemma 5.31 (PV_1). *There is a* PV*-symbol $c_k^m(x)$ such that* PV_1 *proves for any numbers $1^{(k)}$ and $1^{(m)}$*

$$c_k^m(x) \leftrightarrow |x| \leq m \wedge \mathit{NumOnes}(x) = k.$$

Lemma 5.32 (PV_1). *There is a* PV*-symbol $f_k^m(i)$ such that* PV_1 *proves for any numbers $1^{(k)}$ and $1^{(m)}$, where $0 \leq k \leq m$,*

$$f_k^m : \left\{ 0 < i \leq \binom{m}{k} \right\} \to \{x; c_k^m(x) = 1\},$$

is an injective function.

Proof. By recursion (simultaneously on k and m) define the function f_k^m as:

$$f_0^0(1) = 0 \quad \text{and} \quad f_k^{m+1}(i) = \begin{cases} f_k^m(i) & 0 < i \leq \binom{m}{k} \\ f_{k-1}^m(i - \binom{m}{k}) + 2^m & \binom{m}{k} < i \leq \binom{m+1}{k} \end{cases}$$

Now, we prove the following claim.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Claim. If $0 < i \leq \binom{m+1}{k}$ then we have $c_k^{m+1}(f_k^{m+1}(i))$.

We prove the claim by induction on k and m. For $k = m = 0$ the claim trivially holds. Suppose by the induction step, for any $0 < i \leq \binom{m+1}{k}$, we have $c_k^m(f_k^m(i))$ and $c_{k-1}^m(f_{k-1}^m(i))$. Using the equality $\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1}$ and the definition of the predicate $c_k^{m+1}(x)$, it is easy to see that the following holds for any $x < 2^{m+1}$

$$c_k^{m+1}(x) = c_k^m(x) \vee c_k^m(2^m + x) \tag{*}$$

Now, if $0 < i \leq \binom{m+1}{k}$ then either $i \leq \binom{m}{k}$ or $\binom{m}{k} < i \leq \binom{m+1}{k}$.

- If $0 < i \leq \binom{m}{k}$, we have $f_k^{m+1}(i) = f_k^m(i)$ and by the induction step we have $c_k^m(f_k^m(i))$. By (*), we get $c_k^{m+1}(f_k^m(i))$.
- If $\binom{m}{k} < i \leq \binom{m+1}{k}$, we have $f_k^{m+1}(i) = f_{k-1}^m(i - \binom{m}{k}) + 2^m$. By the induction step, $c_{k-1}^m(f_{k-1}^m(i - \binom{m}{k}))$. Therefore, we get $c_k^{m+1}(f_{k-1}^m(i - \binom{m}{k}) + 2^m)$ and hence, by (*), we get $c_k^{m+1}(f_k^{m+1}(i))$.

This finishes the proof of the claim. Now, it remains to prove that f_k^m is injective. By induction on k and m we prove that if $f_k^{m+1}(i) = f_k^{m+1}(j)$ then $i = j$. By the induction step, we know that

$$\text{if } f_k^m(i) = f_k^m(j) \text{ then } i = j \qquad \text{if } f_{k-1}^m(i) = f_{k-1}^m(j) \text{ then } i = j$$

There are three cases:

1. If $i, j \leq \binom{m}{k}$, then $f_k^{m+1}(i) = f_k^{m+1}(j) = f_k^m(i) = f_k^m(j)$. Therefore, by the induction step, we have $i = j$.
2. If $\binom{m}{k} < i, j \leq \binom{m+1}{k}$, then $f_k^{m+1}(i) = f_k^{m+1}(j) = f_{k-1}^m(i - \binom{m}{k}) + 2^m = f_{k-1}^m(j - \binom{m}{k}) + 2^m$. Again, by the induction step, we have $i = j$.
3. We show that the case where $i \leq \binom{m}{k}$ and $\binom{m}{k} < j \leq \binom{m+1}{k}$ is not possible. For the sake of contradiction, suppose otherwise. Then,

$$\begin{aligned} f_k^{m+1}(i) &= f_k^{m+1}(j) && \text{(By the assumption)} \\ f_k^{m+1}(i) &= f_k^m(i) && \text{as } i \leq \binom{m}{k} \\ f_k^{m+1}(j) &= f_{k-1}^m(j - \binom{m}{k}) + 2^m && \text{as } \binom{m}{k} < j \leq \binom{m+1}{k} \end{aligned}$$

By the claim $c_k^m(f_k^m(i))$ holds, which by definition we get $|f_k^m(i)| \leq m$. We have,

$$|f_k^m(i)| = |f_{k-1}^m(j - \binom{m}{k}) + 2^m|.$$

However, $|f_k^m(i)| \leq m$, which is a contradiction with

$$|f_{k-1}^m(j - \binom{m}{k}) + 2^m| > m.$$

□

Definition 5.33. A function $f : \{1, \ldots, m\} \to \{1, \ldots, m'\}$ is called *strictly order-preserving (s.o.p.)* if for any $x, y \leq m$ it satisfies

$$\text{if} \quad x < y \quad \text{then} \quad f(x) < f(y).$$

Recall that $\ell = \left\lfloor \sqrt{\phi(r)} \right\rfloor \cdot \lfloor \log n \rfloor$ and r is a length of a string. By Lemma 5.26, we have $t = |G_r| \leq \phi(r)$, which means that both t and ℓ are lengths. Lemmas 5.32, 5.35, 5.34, and 5.36 are the ingredients needed

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

to prove the original Lemma F in [1]. In the former three lemmas, we provide injective functions, which we will compose to get the main result in Corollary 5.38.

Lemma 5.34 (PV_1). *Assume $H(n,r)$. There is a* PV*-symbol $h_t^\ell(x)$ such that* PV_1 *proves that the function h_t^ℓ with the domain*

$$\{x; c_{\ell+1}^{t+\ell}(x) = 1\}$$

and the codomain

$$\{f \mid f \text{ is a s.o.p. function}, f : \{1,2,\dots,\ell+1\} \to \{1,2,\dots,t+\ell\}\}$$

is an injective function.

Proof. The function $h_t^\ell(x)$ is defined by recursion, sending each x to a function f of the above form. The idea is as follows. Suppose x is given. Let $x_1 = x$. We start by defining $f(1) = j$ where j is the smallest bit of x_1 that is one, i.e, for any $j' < j$ the j'th bit of x_1 is zero. This is possible in PV_1 because of the following: there is a PV-symbol enumerating small sets and going through it to find the smallest nonzero bit and output the index. To define $f(2)$, we first calculate $x_2 = x_1 - 2^{j-1}$. Then, $f(2) = k$ where k is the smallest bit of x_2 that is one. We continue till reaching $f(\ell+1)$. Note that in each step the number of ones in x_{i+1} is one less than the number of ones in x_i. The function f with the domain $\{1,\dots,\ell+1\}$ is well-defined since there are $\ell+1$ ones in x. Moreover, $f(i) \in \{1,\dots,t+\ell\}$ and it is a s.o.p. function. It is clear that the function h_t^ℓ defined this way is injective. □

Lemma 5.35 (PV_1). *Assume $H(n,r)$. There is a* PV*-symbol $g_t^\ell(f)$ such that* PV_1 *proves that the function g_t^ℓ with the domain*

$$\{f \mid f \text{ is a s.o.p. function}, f : \{1,2,\dots,\ell+1\} \to \{1,2,\dots,t+\ell\}\}$$

and the codomain $\{(e_0,\dots,e_\ell); \Sigma_{i=0}^{\ell} e_i \le t-1\}$ is an injective function.

Proof. The function g_t^ℓ behaves as follows. It takes an f of the above form and sends it to a tuple $(e_0,\dots,e_\ell)$. Take subsets $s_i \subseteq \{1,\dots,t+\ell\}$ for $0 \le i \le \ell$ as follows:

$$\begin{aligned} s_0 &:= \{j \in \{1,\dots,t+\ell\}; j < f(1)\} \\ s_i &:= \{j \in \{1,\dots,t+\ell\}; f(i) < j < f(i+1)\} \quad \text{for } 1 \le i \le \ell \end{aligned}$$

Now, we take $g_t^\ell(f) := (|s_0|,\dots,|s_\ell|)$, i.e., $e_i := |s_i|$ for each $0 \le i \le \ell$. We have to show that $\Sigma_{i=0}^{\ell}|s_i| \le t-1$. Note that

$$\begin{aligned} \Sigma_{i=0}^{\ell}|s_i| &= |s_0| + \Sigma_{i=1}^{\ell}|s_i| \\ &= f(1) - 1 + \Sigma_{i=1}^{\ell}(f(i+1) - f(i) - 1) \\ &= f(\ell+1) - (\ell+1) \\ &\le (t+\ell) - (\ell+1) \qquad (*) \\ &\le t-1 \end{aligned}$$

where the inequality (*) is derived by the fact that the codomain of f is $\{1,\dots,t+\ell\}$.

We prove that g_t^ℓ is injective. Suppose $g_t^\ell(f) = g_t^\ell(f')$. Therefore, there exist sets $s_0,\dots,s_\ell$ and $s_0',\dots,s_\ell'$ such that $(|s_0|,\dots,|s_\ell|) = (|s_0'|,\dots,|s_\ell'|)$. By induction on $1 \le i \le \ell+1$, we will show that $f(i) = f'(i)$. Since $|s_0| = |s_0'|$ we get

$$|\{j \in \{1,\dots,t+\ell\}; j < f(1)\}| = |\{k \in \{1,\dots,t+\ell\}; k < f'(1)\}|,$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

which means that $f(1) = f'(1)$. Now, suppose for an $i \leq \ell$ we have $f(i) = f'(i)$. Since $|s_i| = |s'_i|$ we have:

$$|\{j \in \{1, \dots, t+\ell\}; f(i) < j < f(i+1)\}| = |\{k \in \{1, \dots, t+\ell\}; f'(i) < k < f'(i+1)\}|.$$

Therefore, $f(i+1) = f'(i+1)$. □

Lemma 5.36 (PV_1). *Let u and v be sets with cardinality bounded by a length. Then we have:*

$$\textit{if} \quad u \neq v \quad \textit{then} \quad \Pi_{b \in u}(\mathcal{X} + b) \neq \Pi_{b \in v}(\mathcal{X} + b)$$

Proof. For the sake of contradiction, suppose $\Pi_{b \in u}(\mathcal{X} + b) = \Pi_{b \in v}(\mathcal{X} + b)$ and $u \neq v$. Then, without loss of generality we can assume that there is an element $c \in u$ such that $c \notin v$. Therefore,

$$\Pi_{b \in u}(\mathcal{X} + b) \equiv 0 \pmod{\mathcal{X} + c}$$

and

$$\begin{aligned} \Pi_{b \in u}(\mathcal{X} + b) &\equiv \Pi_{b \in v}(\mathcal{X} + b) \\ &\equiv \Pi_{b \in v}\big((\mathcal{X} + c) + (b - c)\big) \\ &\equiv \Pi_{b \in v}(b - c) \pmod{\mathcal{X} + c} \end{aligned}$$

Therefore,

$$\Pi_{b \in v}(b - c) \equiv 0 \pmod{\mathcal{X} + c}.$$

Hence, there exists $b \in v$ such that $b = c$, a contradiction with $c \notin v$. □

The following lemma introduces a set $\hat{P}_t$, which will be used later.

Lemma 5.37. *Assuming $H(n, r)$, there is a* PV*-symbol $\hat{P}_t(f)$ such that* PV_1 *proves:*

$$\begin{aligned} \hat{P}_t(f) \leftrightarrow \textit{there is a sequence } \langle e_0, \dots, e_\ell \rangle \textit{ such that:} \\ \sum_{a=0}^{\ell} e_a < t, f \equiv \Pi_{a=0}^{\ell}(\mathcal{X} + a)^{e_a} \pmod{h, p}; \quad \deg f < \deg h. \end{aligned}$$

Proof. Let f be a given polynomial of degree t. The truth value of $\hat{P}_t(f)$ is computed as follows,

- if $f \not\equiv 0 \pmod{\mathcal{X} + a}$ for all $0 \leq a \leq \ell$, then $\hat{P}_t(f)$ is false.
- Otherwise, take the smallest a such that $f \equiv 0 \pmod{\mathcal{X} + a}$ and assign $f_1 = \frac{f}{\mathcal{X}+a}$.

Repeat the step for f_1, i.e.,

- if $f_1 \not\equiv 0 \pmod{\mathcal{X} + a}$ for all $0 \leq a \leq \ell$, then $\hat{P}_t(f)$ is false.
- Otherwise, take the smallest a such that $f \equiv 0 \pmod{\mathcal{X} + a}$ and assign $f_2 = \frac{f_1}{\mathcal{X}+a}$.

Repeat the step at most t many times, where each step takes ℓ many divisions. If we reach some i such that $f_i \equiv 1 \pmod{\mathcal{X} + a}$ for some $0 \leq a \leq \ell$, then $\hat{P}_t(f)$ is true. Otherwise, $\hat{P}_t(f)$ is false. To compute the sequence $\langle e_0, \dots, e_\ell \rangle$ from the process, initially assign $s_0 = \langle e_0, \dots, e_\ell \rangle = \langle 0, \dots, 0 \rangle$. In step $i + 1$

$$\begin{aligned} \text{if} \quad f_i = \frac{f_{i-1}}{\mathcal{X} + a} \quad \text{and} \quad s_i = \langle e_0, \dots, e_a, \dots, e_\ell \rangle \quad \text{then} \\ s_{i+1} = \langle e_0, \dots, e_a + 1, \dots, e_\ell \rangle \end{aligned}$$

Now, to finish the proof, we need the following easy facts:

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

1. For all $1 \leq a \leq \ell$ we have $\mathcal{X} + a \neq 0$ in F, because by Corollary 4.24 we have $\deg(h) > 1$.
2. The polynomials $\mathcal{X}, \mathcal{X}+1, \cdots, \mathcal{X}+\ell$ are all distinct in F. The reason is as follows. Let $1 \leq i \neq j \leq \ell$. Since

$$\ell = \left\lfloor \sqrt{\phi(r)} \right\rfloor \cdot \lfloor \log n \rfloor < \lfloor \sqrt{r} \rfloor \cdot \lfloor \log n \rfloor < r \quad \text{and} \quad r < p,$$

then $i \neq j$ in F_p.

Moreover, the argument can be formalized in PV_1 as $\ell = \left\lfloor \sqrt{\varphi(r)} \right\rfloor \cdot \lfloor \log n \rfloor$ and by Lemma 5.19 we have $r \leq |n|^{10}$. □

Corollary 5.38 (PV_1). *Assume $H(n, r)$. There is a* PV*-symbol $\sigma_t^\ell(i)$ such that* PV_1 *proves*

$$\sigma_t^\ell : \binom{t+\ell}{\ell+1} \to \hat{P}_t$$

is an injective function.

Proof. Take the functions $f_{\ell+1}^{t+\ell}, g_t^\ell$, and h_t^ℓ as in Lemmas 5.32, 5.35, and 5.34, respectively. By composing these functions, we get $e_0, \ldots, e_\ell$ such that

$$g_t^\ell(h_t^\ell(f_{\ell+1}^{t+\ell}(i))) = (e_0, \ldots, e_\ell) \quad \text{and} \quad \Sigma_{i=0}^{\ell} e_i \leq t - 1.$$

Define $\sigma_t^\ell(i) = \prod_{a=0}^{\ell} (\mathcal{X} + a)^{e_a}$. The function σ_t^ℓ is injective by Lemma 5.36 and by the fact that the functions $f_{\ell+1}^{t+\ell}$, g_t^ℓ, and h_t^ℓ are all injective. □

Lemma 5.39 (PV_1, Lemma F). *Assume $H(n, r)$. There is a* PV*-symbol $\tau_t^\ell(x)$ such that* PV_1 *proves that the function*

$$\tau_t^\ell : \binom{t+\ell}{t-1} \to \hat{P}_t$$

satisfies the following condition:

$$\textit{if} \quad x \neq y \quad \textit{then} \quad \tau_t^\ell(x) \not\equiv \tau_t^\ell(y) \pmod{h, p}.$$

Proof. We know that $\binom{t+\ell}{\ell+1} = \binom{t+\ell}{t-1}$. So, we will use them interchangeably. Using Corollary 5.38, take the injective function

$$\sigma_t^\ell : \binom{t+\ell}{\ell+1} \to \{f \in \hat{P}_t ; \deg(f) < t\}.$$

Consider the function

$$\tau_t^\ell(x) = \sigma_t^\ell(x) \bmod h, p.$$

We have to show that

$$\text{if} \quad x \neq y \quad \text{then} \quad \tau_t^\ell(x) \not\equiv \tau_t^\ell(y) \pmod{h, p}.$$

For the sake of contradiction, suppose $x \neq y$ but $\tau_t^\ell(x) \equiv \tau_t^\ell(y) \pmod{h, p}$. Denote $\tau_t^\ell(x) = f(\mathcal{X})$ and $\tau_t^\ell(y) = g(\mathcal{X})$. Let $m \in G_r$, i.e., there are $0 \leq i, j \leq r$ such that

$$m \equiv (\frac{n}{p})^i \cdot p^j \pmod{r}.$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Thus,

$$\big(f(\mathcal{X})\big)^m \equiv \big(g(\mathcal{X})\big)^m \pmod{h, p}.$$

By Lemmas 5.28 and 5.29, m is introspective for both f and g. Therefore,

$$\big(f(\mathcal{X})\big)^m \equiv f(\mathcal{X}^m) \pmod{\mathcal{X}^r - 1, p} \quad \big(g(\mathcal{X})\big)^m \equiv g(\mathcal{X}^m) \pmod{\mathcal{X}^r - 1, p}.$$

Since $h(\mathcal{X})$ divides $\mathcal{X}^r - 1$ we get

$$f(\mathcal{X}^m) \equiv g(\mathcal{X}^m) \pmod{h, p}.$$

Define $Q(\mathcal{Y}) = f(\mathcal{Y}) - g(\mathcal{Y})$. Then, $\mathcal{X}^m$ is a root of $Q(\mathcal{Y})$ for each $m \in G_r$. Moreover, if $\mathcal{X}^m \equiv \mathcal{X}^{m'} \pmod{h, p}$ for each $m, m' \in G_r$, then by Lemma 5.30 we get $m = m'$. Hence, there are $|G_r| = t$ many distinct roots of $Q(\mathcal{Y})$ in the field F. However, the degree of $Q(\mathcal{Y})$ is less than t and we get a contradiction. Thus $\tau_t^\ell(x) \not\equiv \tau_t^\ell(y) \pmod{h, p}$. This argument can be formalized in PV_1 because the polynomials used here have logarithmically bounded degrees. □

5.7. Lemma G

Lemma 5.40 (PV_1). *Let x,y and $1^{(k)}$ be numbers such that for any numbers $a, b \le k$ we have $x^a \neq y^b$. There is a* PV*-symbol $f_{x,y}(i)$ such that* PV_1 *proves*

$$f_{x,y} : \{1, 2, \ldots, (k+1)^2\} \to \{x^i y^j \mid 0 \le i, j \le k\}$$

is an injective function.

Proof. For any $1 \le l \le (k+1)^2$ we can write $l = i(k+1) + j + 1$ where $0 \le i, j \le k$. We can find i and j as follows and define the function $f_{x,y}$ as $f_{x,y}(l) = x^i y^j$ where

$$i = \left\lfloor \frac{l-1}{k+1} \right\rfloor \qquad \text{and} \qquad j = l - 1 \mod (k+1).$$

It is clear that $0 \le i, j \le k$. Now, we prove that $f_{x,y}$ is injective, i.e.,

$$\text{if} \qquad f_{x,y}(l) = f_{x,y}(m) \qquad \text{then} \qquad l = m.$$

Suppose $f_{x,y}(l) = f_{x,y}(m)$ for some $l, m \in \{1, \ldots, (k+1)^2\}$. Therefore, there are $0 \le i, i', j', j' \le k$ such that

$$i = \left\lfloor \frac{l-1}{k+1} \right\rfloor \qquad i' = \left\lfloor \frac{m-1}{k+1} \right\rfloor$$
$$j = l - 1 \mod k+1 \qquad j' = m - 1 \mod k+1$$

and

$$x^i y^j = x^{i'} y^{j'}.$$

There are several cases:

- If $i > i'$ and $j < j'$, then $x^{i-i'} = y^{j'-j}$, which is a contradiction with the assumption that for any numbers a, b we have $x^a \neq y^b$.
- If $i < i'$ and $j > j'$, we have a situation similar to the previous case.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

- If $i > i'$ and $j > j'$, then $x^{i-i'}y^{j-j'} = 1$. This only happens when $x = y = 1$, which is again a contradiction with the assumption.
- If $i < i'$ and $j < j'$, we have a situation similar to the previous case.

Thus, $i = i'$, $j = j'$, and $l = m$. Hence, $f_{x,y}$ is injective. □

Lemma 5.41 (PV_1). *Assume $H(n,r)$. There is a* PV*-symbol $\hat{I}_t(y)$ for which* PV_1 *proves*

$$\hat{I}_t(y) \leftrightarrow \exists\, 0 \le i,j \le \lfloor\sqrt{t}\rfloor \quad y = \left(\frac{n}{p}\right)^i \cdot p^j.$$

Proof. Note that $t < r$ by the discussion after Lemma 5.25 and $r < |n|^{10}$ by Lemma 5.19. Therefore, it is easy to see that given a number y, in PV_1 we can check whether there are numbers $0 \le i,j \le \lfloor\sqrt{t}\rfloor$ such that $y = (\frac{n}{p})^i \cdot p^j$. □

Lemma 5.42 (S^1_2+RUB, Lemma G). *Assume $H(n,r)$. If n is not a power of p then there exists a function*

$$\hat{g}_t : \hat{P}_t \to \{1,\dots,n^{\lfloor\sqrt{t}\rfloor}\},$$

which satisfies the condition:

$$\textit{if} \qquad f_1 \not\equiv f_2 \pmod{h,p} \qquad \textit{then} \qquad \hat{g}_t(f_1) \neq \hat{g}_t(f_2).$$

Proof. Assuming n is not a power of p, then by Lemma 5.20, there is a prime divisor p' of n distinct from p. This implies, that $(n/p)^a \neq p^b$ for any numbers $a,b \le \lfloor\sqrt{t}\rfloor$. Thus, we can use Lemma 5.40, to obtain the function $f_{\frac{n}{p},p}$

$$f_{\frac{n}{p},p} : \{1,2,\dots,(\lfloor\sqrt{t}\rfloor+1)^2\} \to \{(\frac{n}{p})^i \cdot p^j \mid 0 \le i,j \le \lfloor\sqrt{t}\rfloor\}$$

or alternatively

$$f_{\frac{n}{p},p} : \{1,2,\dots,(\lfloor\sqrt{t}\rfloor+1)^2\} \to \{y \mid \hat{I}_t(y) = 1\},$$

which is an injective function. This means that the number of distinct numbers y such that $\hat{I}_t(y) = 1$ is at least $(\lfloor\sqrt{t}\rfloor+1)^2 > t$. As $|G_r| = t$, there are two numbers $m_1 > m_2$ such that

$$\hat{I}_t(m_1), \hat{I}_t(m_2) \text{ and } m_1 \equiv m_2 \pmod{r}.$$

It is easy to see that

$$\mathcal{X}^{m_1} \equiv \mathcal{X}^{m_2} \pmod{\mathcal{X}^r - 1}.$$

We want to define the function $\hat{g}_t : \hat{P}_t \to n^{\lfloor\sqrt{t}\rfloor}$ such that

$$\text{if} \qquad \hat{P}_t(f_1),\ \hat{P}_t(f_2),\ f_1 \not\equiv f_2 \pmod{h,p} \qquad \text{then} \qquad \hat{g}_t(f_1) \neq \hat{g}_t(f_2).$$

Let $f_1, f_2 \in \hat{P}_t$ such that $f_1 \not\equiv f_2 \pmod{h,p}$. Thus, for $i \in \{1,2\}$ we get

$$\begin{aligned}\big(f_i(\mathcal{X})\big)^{m_1} &\equiv f_i(\mathcal{X}^{m_1})\\ &\equiv f_i(\mathcal{X}^{m_2})\\ &\equiv \big(f_i(\mathcal{X})\big)^{m_2} \pmod{\mathcal{X}^r - 1, p}\end{aligned}$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Therefore, in the field F, we have $\big(f_i(\mathcal{X})\big)^{m_1} = \big(f_i(\mathcal{X})\big)^{m_2}$. Now, take the sparse polynomial $Q'(\mathcal{Y}) = \mathcal{Y}^{m_1} - \mathcal{Y}^{m_2}$. We have $\deg(Q') = m_1$ and $f_i(\mathcal{X})$ is a root of $Q'(\mathcal{Y})$ in the field F. By the axiom RUB, the function

$$\iota_{F,Q'} : \{\mathcal{Y} \in F; Q'(\mathcal{Y}) = 0\} \to [\deg Q']$$

is injective. Thus, the number of distinct roots of Q' is at least m_1. In addition, we have $m_1 \leq (\frac{n}{p} \cdot p)^{\lfloor\sqrt{t}\rfloor} \leq n^{\lfloor\sqrt{t}\rfloor}$. Take the function $\hat{g}_t(\mathcal{Y})$ as $\iota_{F,Q'}(\mathcal{Y})$. By the above observations we get $\hat{g}_t(f_1) \neq \hat{g}_t(f_2)$ and this finishes the proof. □

5.8. Lemma H

We start with some easy combinatorial facts.

Lemma 5.43 (PV_1). *For any numbers $1^{(k)}$, $1^{(l)}$, and $1^{(s)}$ where $k \geq s$ we have $\binom{k+l}{k} \geq \binom{s+l}{s}$.*

Proof. Since $k \geq s$, we have $k + i \geq s + i$ for each $1 \leq i \leq l$. Therefore, $\Pi_{i=1}^{l}(k + i) \geq \Pi_{i=1}^{l}(s + i)$. Hence, $\frac{(k+l)!}{k!l!} \geq \frac{(s+l)!}{s!l!}$, which is $\binom{k+l}{k} \geq \binom{s+l}{s}$. □

Lemma 5.44 (PV_1). *For any number $1^{(k)}$, where $k \geq 6$, we have $\binom{2k+1}{k} > 2^{k+2}$.*

Proof. We have

$$\begin{aligned}\binom{2k+1}{k} &= \frac{(2k+1)(2k)\dots(k+2)}{k!} \\ &= (k+2)\Pi_{i=0}^{k-2}\frac{2(k-i)+(i+1)}{k-i} \\ &> (k+2)2^{k-1}\end{aligned}$$

If $k \geq 6$ then we have $(k + 2)2^{k-1} \geq 2^{k+2}$. Therefore, $\binom{2k+1}{k} > 2^{k+2}$. □

Lemma 5.45 (S_2^1+iWPHP+RUB+GFLT, Lemma H). *Assume $H(n, r)$. If the algorithm returns* PRIME *then n is prime.*

Proof. By Lemma 5.39, there is an injective function from $\binom{t+\ell}{t-1}$ to $\hat{P}_t$. Recall the definition of G_r in Lemma 5.25 and $|G_r| = t$. We have

$$t \geq \mathrm{ord}_r(n) > |n|^2$$

where the rightmost inequality holds by Lemma 5.19 and the leftmost inequality is clear by Lemma 5.25. Hence,

$$\begin{aligned} t &\geq \left\lfloor\sqrt{t}\right\rfloor \cdot \left\lfloor\sqrt{t}\right\rfloor \\ &\geq \left\lfloor\sqrt{t}\right\rfloor \cdot |n| && (t > |n|^2) \\ &> \left\lfloor\sqrt{t}\right\rfloor \cdot \lfloor\log n\rfloor && (|n| = \lceil\log(n+1)\rceil > \lfloor\log n\rfloor)\end{aligned}$$

Consequently, $t - 1 \geq \left\lfloor\sqrt{t}\right\rfloor \cdot \lfloor\log n\rfloor$. In Lemma 5.43 substitute $t - 1$ for k and $\left\lfloor\sqrt{t}\right\rfloor \cdot \lfloor\log n\rfloor$ for s and $\ell + 1$ for l to get

$$\binom{t+\ell}{t-1} \geq \binom{\ell + 1 + \left\lfloor\sqrt{t}\right\rfloor \cdot \lfloor\log n\rfloor}{\left\lfloor\sqrt{t}\right\rfloor \cdot \lfloor\log n\rfloor}.$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

By Lemma 5.26, we have $t \leq \phi(r)$. Hence,

$$\ell = \left\lfloor \sqrt{\phi(r)} \right\rfloor \cdot \lfloor \log n \rfloor \geq \left\lfloor \sqrt{t} \right\rfloor \cdot \lfloor \log n \rfloor.$$

Therefore,

$$\binom{\ell + 1 + \lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor}{\lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor} \geq \binom{2\lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor + 1}{\lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor}.$$

In Lemma 5.44, if we substitute $\lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor$ for k, we get

$$\binom{2\lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor + 1}{\lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor} > 2^{\lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor + 2}$$

for $\lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor \geq 6$, which we can assume to hold as the remaining cases form a true bounded sentence. Moreover, we have $2^{\lfloor \sqrt{t} \rfloor \cdot \lfloor \log n \rfloor + 2} \geq 2n^{\lfloor \sqrt{t} \rfloor}$. This means that there exists an injective function from $2n^{\lfloor \sqrt{t} \rfloor}$ to $\hat{P}_t$. However, by Lemma 5.42, we have if n is not a power of p, then there exists an injective function from $\hat{P}_t$ to $n^{\lfloor \sqrt{t} \rfloor}$. This means that there exists an injective function

$$f : [2n^{\lfloor \sqrt{t} \rfloor}] \to [n^{\lfloor \sqrt{t} \rfloor}]$$

computed by a PV(ι)-term, which is a contradiction with the axiom scheme iWPHP (because what we do is essentially composing ι with PV functions and not iterating ι in some p-time process). Thus, n is a power of p. But, if $n = p^k$ for some $k > 1$ then the algorithm would have returned COMPOSITE in Step 1. Hence $n = p$. □

5.9. The correctness

With the Lemma 5.45 in hand we have everything we need to prove the correctness in S^1_2 + iWPHP + RUB + GFLT.

Theorem 5.46.

$$S^1_2 + \text{iWPHP} + \text{RUB} + \mathit{GFLT} \vdash \mathit{AKSCorrect}$$

Proof. The implication AKSPrime(x) → Prime(x) is proved in Lemma 5.45. The other implication, Prime(x) → AKSPrime(x), is simpler. The AKS algorithm simply checks some properties of the number x and if they are satisfied, the number is proclaimed a prime, so this implication follows from the Lemma 3.1 and the GFLT axiom. □

6. VTC^0_2 proves S^1_2 + iWPHP + RUB + GFLT

In this section, we show that the axioms with which we extended S^1_2 to prove the correctness of the algorithm are actually provable in VTC^0_2. The theory VTC^0_2 includes T_2 by definition. We then show that GFLT can be proved and then that RUB can be proved with ι being replaced by Σ^B_1-definable function. By the Σ^B_0(card) – COMP scheme and the axioms defining counting sequences we obtain that $S^1_2(\iota)$ + iWPHP(ι) + RUB(ι) + GFLT is provable in VTC^0_2 and thus $\text{VTC}^0_2 \vdash$ AKSCorrect.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

6.1. Σ_1^B-definability of algebraic operations

In this section, we will prove the factorial and binomial coefficient functions are Σ_1^B-definable when the inputs are from the number sorts. Similarly, we will show that the function computing the powers of high degree polynomials is Σ_1^B-definable, provided that the exponent is from the number sort. The following two lemmas follow straightforwardly from the provability of the axiom IMUL (see Theorem 2.3).

Lemma 6.1 (VTC^0). *There is a Σ_1^B-definition of a function $x \mapsto x!$, whose values are objects of the set sort, for which VTC_2^0 can prove the inductive properties:*

$$0! = 1$$
$$(x+1)! = (x+1) \cdot x!$$

Lemma 6.2 (VTC^0). *There is a Σ_1^B-definition of a function $\binom{x}{y}$, whose values are objects of the set sort, which for $y \leq x$ satisfies:*

$$\binom{x}{y} = \left\lfloor \frac{x!}{y!(x-y)!} \right\rfloor,$$

and otherwise $\binom{x}{y} = 0$.

The main principle behind the proof of the following Lemma is still the axiom IMUL.

Lemma 6.3 (VTC^0). *There is a Σ_1^B-definable function, which to each high degree polynomial P and each number x assigns a high degree polynomial P^x such that VTC_2^0 proves for every x and P:*

$$P^0 = 1$$
$$P^{x+1} = P \cdot P^x.$$

Proof. For $P = \sum_{i=0}^{d} A_i \mathcal{X}^i$ we define P^x to be $\sum_{i=0}^{xd} B_i \mathcal{X}^i$ such that for any $0 \leq i \leq xd$: $B_i = \left(\sum_{j_1+\cdots+j_x=i} \prod_{k=1}^{x} A_{j_k}\right)$, where $0 \leq j_k \leq n$. This is Σ_1^B-definable as both iterated multiplication and iterated addition are.

We shall prove the recursive properties of this function by induction. For $x = 0$, the statement is clear. Assume the statement holds for x, then

$$\begin{aligned}
P \cdot P^x &= P \cdot \sum_{i=0}^{xd} \left(\sum_{j_1+\cdots+j_x=i} \prod_{l=1}^{x} A_{j_l} \right) \mathcal{X}^i \\
&= \sum_{i=0}^{(x+1)d} \left(\sum_{j+k=i} A_i \cdot \left(\sum_{j_1+\cdots+j_x=j} \prod_{l=1}^{x} A_{j_l} \right) \right) \mathcal{X}^i \\
&= \sum_{i=0}^{(x+1)d} \left(\sum_{j_1+\cdots+j_x+k=i} A_k \prod_{l=1}^{x} A_{j_l} \right) \mathcal{X}^i \\
&= \sum_{i=0}^{(x+1)d} \left(\sum_{j_1+\cdots+j_x+j_{x+1}=i} \prod_{l=1}^{x+1} A_{j_l} \right) \mathcal{X}^i \\
&= P^{x+1}.
\end{aligned}$$

□

6.2. The binomial theorem and provability of GFLT

With the factorial and binomial coefficient functions Σ_1^B-defined, we will prove the binomial theorem, which then serves as a lemma to prove the GFLT axiom.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Lemma 6.4 (VTC^0, Pascal's triangle). *Let* $1 \leq x$ *and* $y \leq x$, *then*

$$\binom{x}{y} = \binom{x-1}{y} + \binom{x-1}{y-1}$$

and

$$\binom{x}{y} y!(x-y)! = x!$$

Proof. By induction on x. If $x = 1$, we can check that both equations hold. Assume the statement holds for x. Regarding the first equation, we have

$$\begin{aligned}\binom{x}{y} + \binom{x}{y-1} &= \left\lfloor \frac{x!}{y!(x-y)!} \right\rfloor + \left\lfloor \frac{x!}{(y-1)!(x-y+1)!} \right\rfloor \\ &= \left\lfloor \frac{x!(x-y+1)}{y!(x-y+1)!} \right\rfloor + \left\lfloor \frac{x! \cdot y}{y!(x-y+1)!} \right\rfloor\end{aligned}$$

by the second equation in the induction hypothesis, both of the denominators divide the numerators and thus

$$\left\lfloor \frac{x!(x-y+1)}{y!(x-y+1)!} \right\rfloor + \left\lfloor \frac{x! \cdot y}{y!(x-y+1)!} \right\rfloor = \left\lfloor \frac{x! \cdot (x+1)}{y!(x+1-y)!} \right\rfloor = \binom{x+1}{y}.$$

To prove the second equation, we start with

$$\binom{x+1}{y} = \binom{x}{y} + \binom{x}{y-1}$$

which we multiply by $y!(x+1-y)!$ to obtain

$$\binom{x+1}{y} y!(x+1-y)! = \binom{x}{y} y!(x+1-y)! + \binom{x}{y-1} y!(x+1-y)!$$

which by the application of the induction hypothesis becomes:

$$\binom{x+1}{y} y!(x+1-y)! = x!(x+1-y) + x!y = x!(x+1) = (x+1)!$$

□

Theorem 6.5 (VTC^0). *For any numbers a and b:*

$$(\mathcal{X} + a)^b = \sum_{i=0}^{b} \binom{b}{i} \mathcal{X}^i a^{b-i}$$

Proof. By induction on b. If $b = 0$, then both sides evaluate to 1.

Assume the statement holds for b. Then

$$\begin{aligned}(\mathcal{X} + a)^{b+1} &= (\mathcal{X} + a)(\mathcal{X} + a)^b \\ &= (\mathcal{X} + a) \sum_{i=0}^{b} \binom{b}{i} \mathcal{X}^i a^{b-i}\end{aligned}$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

$$= \left(\sum_{i=0}^{b} \binom{b}{i} \mathcal{X}^{i+1} a^{b-i}\right) + \left(\sum_{i=0}^{b} \binom{b}{i} \mathcal{X}^{i} a^{b+1-i}\right)$$
$$= \left(\sum_{i=1}^{b+1} \binom{b}{i-1} \mathcal{X}^{i} a^{b+1-i}\right) + \left(\sum_{i=0}^{b} \binom{b}{i} \mathcal{X}^{i} a^{b+1-i}\right)$$
$$= \mathcal{X}^{b+1} + a^{b+1} + \sum_{i=1}^{b} \left(\binom{b}{i} + \binom{b}{i-1}\right) \mathcal{X}^{i} a^{b+1-i},$$

which by Lemma 6.4 equals

$$\sum_{i=0}^{b+1} \binom{b+1}{i} \mathcal{X}^{i} a^{b+1-i}. \qquad \square$$

Lemma 6.6 (VTC^0_2). *Let p be a prime, and let X code a sequence of m elements of the number sort. If for each $i \leq m : p \nmid X^{[i]}$, then $p \nmid \prod_{i=1}^{m} X^{[i]}$.*

Proof. By induction on m. For $m \leq 1$ this is clear. Assume the statement holds for m and let $\tilde{X} = \prod_{i=1}^{m} X^{[i]}$ and $x = X^{(m+1)}$ and assume for contradiction that $p \mid \tilde{X}x$. By Lemma 2.1 there is $\mathrm{xgcd}(x, p) = (1, u, v)$ such that $ux + vp = 1$. Multiplying by $\tilde{X}$ we get

$$ux\tilde{X} + v\tilde{X}p = \tilde{X}.$$

As both summands on the left hand side are divisible by p, so is $\tilde{X}$, which is a contradiction. $\square$

Lemma 6.7 (VTC^0_2). *Let p be a prime, then for every $0 < m < p$ we have $p \mid \binom{p}{m}$.*

Proof. All numbers less than p are not divisible by p, thus by Lemma 6.6 we have that $p \nmid m!(p-m)!$, and thus $m!(p-m)! \not\equiv 0 \pmod{p}$. On the other hand by Lemma 6.4 we have that $m!(p-m)! \mid m!$, therefore the following are equivalent

$$\binom{p}{m} \equiv 0 \pmod{p}$$
$$\binom{p}{m} m!(p-m)! \equiv 0 \pmod{p}.$$

By the second part of Lemma 6.4 we have that

$$\binom{p}{m} m!(p-m)! = p! \equiv 0 \pmod{p}. \qquad \square$$

Lemma 6.8 (The theory VTC^0_2 proves GFLT.). *Let p be a prime, $a \leq p$ a number and $1^{(r)}$ be a number such that $r < p$. Then*

$$(\mathcal{X} + a)^p \equiv \mathcal{X}^p + a \pmod{p, \mathcal{X}^r - 1},$$

where the exponentiation is computed using a PV*-symbol for exponentiation by squaring modulo $\mathcal{X}^r - 1$.*

Proof. By Theorem 6.5 we have

$$(\mathcal{X} + a)^p = \sum_{i=0}^{p} \binom{p}{i} \mathcal{X}^{i} a^{p-i},$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

by Lemma 6.7 we get

$$(\mathcal{X} + a)^p \equiv \mathcal{X}^p + a \pmod{p}.$$

To obtain the final congruence, we take both sides modulo $\mathcal{X}^r - 1$. By Lemma 4.20 and Lemma 6.3 it follows by $\Sigma_0^B(\mathrm{card})$-induction that exponentiation by squaring is equivalent to first taking true exponentiation and then compute the remainder modulo $\mathcal{X}^r - 1$. □

6.3. Division of high degree polynomials and provability of RUB

In this section, we will show that the division of high degree polynomials over a bounded field is total in VTC^0_2, and thus we can formalize the usual proof of the RUB axiom. It is straightforward to find a $\Sigma_0^B(\mathrm{card})$-formula defining a predicate $P \in F[\mathcal{X}]$ formalizing that P is a high degree polynomial over the bounded field F.

Lemma 6.9 (VTC^0_2). *Let F be a bounded field, then there is a Σ_1^B-definable function which to each high degree polynomial $P \in F[\mathcal{X}]$ and a number x assigns a high degree polynomial P^x and VTC^0_2 proves for every x and every high degree polynomial $P \in F[\mathcal{X}]$:*

$$P^0 = 1$$
$$P^{x+1} = P \cdot P^x$$

Proof. This can be proved analogously to Lemma 6.3. □

Lemma 6.10 (VTC^0_2, adapted from [9]). *For every bounded field F and every $P, S \in F[\mathcal{X}]$ there are $Q, R \in F[\mathcal{X}]$ such that*

$$\deg(R) < \deg(S) \text{ and } P = S \cdot Q + R.$$

Proof. Without loss of generality, we can assume P and S to be monic. Further let $\deg P = n$, $\deg S = m$, $P = \sum_{i=0}^n a_i \mathcal{X}^i$ and $S = \sum_{i=0}^m b_i \mathcal{X}^i$. Define $S_{\mathrm{R}} = \sum_{i=0}^n a_{n-i} \mathcal{X}^i$ and $S_{\mathrm{R}} = \sum_{i=0}^m b_{m-i} \mathcal{X}^i$. By Lemma 6.3 and the totality of iterated addition we can define $\tilde{S}_{\mathrm{R}} = \sum_{i=0}^{n-m} (1 - S_{\mathrm{R}})^i$.

Then put $H = P_{\mathrm{R}} \tilde{S}_{\mathrm{R}}$, assume $H = \sum_{i=0}^{2n+m} c_i \mathcal{X}^i$. Finally, define the polynomials $Q = \sum_{i=0}^{n-m} c_{n-m-i} \mathcal{X}^i$ and $R = f - g \cdot q$.

Now it just remains to show that $\deg R < m$. First notice that

$$\begin{aligned}
\tilde{S}_{\mathrm{R}} S_{\mathrm{R}} &= \tilde{S}_{\mathrm{R}}(1 - (1 - S_{\mathrm{R}})) \\
&= \tilde{S}_{\mathrm{R}} - \tilde{S}_{\mathrm{R}}(1 - S_{\mathrm{R}}) \\
&= \left(\sum_{i=0}^{n-m} (1 - g_R)^i \right) - \left(\sum_{i=0}^{n-m} (1 - g_R)^{i+1} \right) \\
&= 1 - (1 - S_{\mathrm{R}})^{n-m+1}.
\end{aligned}$$

Since S is monic, $1 - S_{\mathrm{R}}$ has no constant term and so $(1 - S_R)^{n-m+1}$ has its lowest $n - m + 1$ coefficients with value 0, in other words there exists $T \in F[\mathcal{X}]$ such that $(1 - S_{\mathrm{R}})^{n-m+1} = \mathcal{X}^{n-m+1} T$. Let $d = \deg R$, assume for contradiction, that $d \geq m$. Define $Q_{\mathrm{R}} = \mathcal{X}^{n-m} Q(1/\mathcal{X})$, $R_{\mathrm{R}} = \mathcal{X}^d R(1/\mathcal{X})$. Then

$$\begin{aligned}
P &= S \cdot Q + R \\
P(1/\mathcal{X}) &= S(1/\mathcal{X}) \cdot Q(1/\mathcal{X}) + R(1/\mathcal{X}) \\
\mathcal{X}^n P(1/\mathcal{X}) &= (\mathcal{X}^m S(1/\mathcal{X})) \cdot (\mathcal{X}^{n-m} Q(1/\mathcal{X})) + \mathcal{X}^{n-d} (\mathcal{X}^d R(1/\mathcal{X})) \\
P_{\mathrm{R}} &= S_{\mathrm{R}} \cdot Q_{\mathrm{R}} + x^{n-d} R_{\mathrm{R}}.
\end{aligned}$$

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

Now since $H = P_R\tilde{S}_R = (S_R \cdot Q_R + x^{n-d}R_R)\tilde{S}_R = Q_R(1-(1-S_R)^{n-m+1}) + \mathcal{X}^{n-d}\tilde{S}_R R_R$ then $H = Q_R - \mathcal{X}^{n-m+1}T + \mathcal{X}^{n-d}\tilde{S}_R R_R$. But from the fact that $n-d < n-m+1$ and $\tilde{S}_R$ and R_R have their constant coefficients equal to 1 we obtain that $\mathcal{X}^{n-d}\tilde{S}_R R_R$ has the coefficient of the monomial $\mathcal{X}^{n-d}$ nonzero and thus Q_R is not equal to the lowest $n-m+1$ coefficients of H, a contradiction. □

The following theorem shows provability of RUB in VTC^0_2. In the original formulation of RUB, sparse polynomial are used but every such polynomial determines a high degree polynomial, so the statement we give is actually at least as strong as the original one.

Theorem 6.11 (The theory VTC^0_2 proves RUB.). *There is a Σ^B_1-definable function $I_{F,G}(x)$ such that VTC^0_2 proves:*

For every bounded field F and a high degree polynomial $G \in k[\mathcal{X}]$ the function

$$I_{F,G}(x) : \{a \in F; G(a) = 0\} \to \{1, \dots, \deg G\},$$

is injective.

Proof. There is a Σ^B_1-definable function $D(F,G,x)$ such that for any bounded field F with bound b on its universe and a high degree polynomial $G \in F[\mathcal{X}]$ we have for all $m \le b$: $D_{F,G}(x)(m) = \prod_{i\in\{0,\dots,m-1\},G(i)=0}(\mathcal{X}-i)$.

Claim. For all $m \le b$: $D_{F,G}(m) \mid G$.

Proof of claim. By induction on m. For $m = 0$, we have $D_{F,G}(0) = 1$ and thus $D_{F,G}(0) \mid G$. Assume the statement holds for m, that is $D_{F,G}(m)$ divides G. If $G(m) \neq 0$, then $D_{F,G}(m+1) = D_{F,G}(k) \mid G$ and we are done. Therefore, we assume that $G(m) = 0$. By the induction hypothesis, there is $H \in k[\mathcal{X}]$ such that $G = D_{F,G}(m) \cdot H$. Hence, $0 = G(m) = D_{F,G}(m) \cdot H(m)$. And since $D_{F,G}(m) = \prod_{i\in\{0,\dots,m-1\},G(i)=0}(m-i)$ is a product of nonzero elements of k, we have that $H(m) = 0$. By Lemma 6.10, there are Q and R such that $H = (\mathcal{X}-m)Q + R$, if $R \neq 0$, then $0 = H(0) = 0 \cdot Q + R \neq 0$. This implies that $R = 0$ and therefore $(\mathcal{X}-m)\cdot Q = H$. Together we get that $D_{F,G}(k+1)Q = D_{F,G}(m)(\mathcal{X}-m)Q = G_k H = G$ and that $D_{F,G}(m+1) \mid G$ which proves the claim.

Finally, we can Σ^B_1-define a function $I_{F,G}(x)$ such that for any bounded field F with bound b on its universe and a high degree polynomial $G \in k[\mathcal{X}]$ we have for all $m \in \{0, \dots, b\}$:

$$I_{F,G}(m) = \begin{cases} 0 & m = 0, \\ I_{F,G}(m-1) + 1 & \text{else if } D_{F,G}(m-1) \neq D_{F,G}(m), \\ I_{F,G}(m-1) & \text{otherwise.} \end{cases}$$

By induction on m we get that for all $m \le b$ we have

$$I_{F,G}(m) = \deg D_{F,G}(m) \le \deg G$$

and that $I_{F,G}(-)$ is nondecreasing. Let $a, b \in k$ such that $G(a) = G(b) = 0$ and $a < b$, then $I_{F,G}(a) < I_{F,G}(b)$, which shows the injectivity of $I_{F,G}(x)$. □

Finally, we have everything needed to finish the proof of correctness in the theory VTC^0_2.

Theorem 6.12. *VTC^0_2 proves the consequences of the theory S^1_2 + iWPHP + RUB + GFLT restricted to the language of* PV*, that is, the consequences without the symbol ι.*

Proof. By Theorem 6.11, the theory VTC^0_2 proves that a Σ^B_1-definition of $I_{F,G}(x)$ satisfies the axiom $\mathrm{RUB}(\iota)$ with ι replaced by the definable function $I_{F,G}(x)$. By the $\Sigma^B_0(\mathrm{card})$-COMP, we can show that it also proves the Σ^b_1-LMIN scheme with the symbol ι being replaced by the definition of $I_{F,G}(x)$.

It is well known that VTC^0 proves the PHP for maps represented by an object of the set sort, by the $\Sigma^B_0(\mathrm{card})$-COMP scheme and the Σ^B_1-definability of $I_{F,G}(x)$ we obtain that it also proves

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

S_2^1 + iWPHP(ι) + RUB with ι replaced by the definable map $I_{F,G}(x)$. The remaining GFLT axiom is provable in VTC_2^0 by Lemma 5.13. □

Using Theorem 6.12 and Theorem 5.46 we obtain the following.

Corollary 6.13. *The theory VTC_2^0, and consequently the theory T_2^{count}, both prove the sentence AKSCorrect.*

7. Concluding remarks

In this work, we proved the correctness of the AKS algorithm as a first order sentence in the language of PV in the theory VTC_2^0. Obtaining such a proof inside T_2 seems to be unlikely as even ordinary Fermat's Little Theorem implies, over T_2, an instance of PHP which is not known to be provable in T_2 [12]. Therefore, we believe it is natural to ask about the following problem.

Problem 7.1. Does $T_2 + \mathrm{PHP}(\Sigma_\infty^b)$ prove the correctness of the AKS algorithm?

We do know, by Jeřábek's work [12], that $T_2 + \mathrm{PHP}$ proves Fermat's Little Theorem. Does this imply anything about GFLT in $T_2 + \mathrm{PHP}$?

Problem 7.2. Does $T_2 + \mathrm{PHP}(\Sigma_\infty^b)$ prove the GFLT axiom?

Showing the unprovability of either of the above statements under some complexity theoretic assumptions is just as interesting. In fact, it is an old problem of Macintyre whether $I\Delta_0$ proves PHP for bounded formulas. It is also tempting to understand the role of the function computed by the polynomial $(\mathcal{X} + a)^p$, or any similar function, in the context of proof complexity generators.

The provability of the implication $\mathrm{Prime}(x) \to \mathrm{AKSPrime}(x)$, which is a Σ_1^b-formula, relates to the complexity of total NP search problems by well known witnessing theorems. The relevant total problem is: For an input number x either verify it is prime using the AKS algorithm or find a proper divisor. We show provability of this implication in the theory $S_2^1 + \mathrm{GFLT}$. Unfortunately, it seems the corresponding witnessing theorem gives only trivial reductions for the factorization problem. It would be interesting to find a provability of this implication in a theory which gives nontrivial witnessing.

The other implication, $\mathrm{AKSPrime}(x) \to \mathrm{Prime}(x)$, is a Π_1^b statement and thus relates to propositional proof complexity by results about propositional translations. Our proof in VTC_2^0 implies a proof in U_2^1 whose corresponding proof system is the quantified sequent calculus G. The theory VTC_2^0 also proves everything T_2 does, which implies that the proof we obtain by propositional translations should be in a system above every G_i, but below G.

Problem 7.3. Describe the propositional proof system corresponding to the Π_1^b-consequences of the theory VTC_2^0 or alternatively to the theory T_2^{count}.

The theory S_2^1 + RUB + iWPHP + GFLT is likely weaker than full T_2^{count}. It could also be interesting to find the propositional proof system corresponding to its Π_1^b-consequences.

Acknowledgment. We are deeply grateful to Emil Jeřábek for his generous and thoughtful feedback on an earlier draft of this work. His comments helped us clarify key arguments, correct important inaccuracies, and his suggestion to consult [9] was especially valuable. We are grateful to Jan Krajíček and Pavel Pudlák for their comments and guidance. We also thank Eitetsu Ken, Erfan Khaniki, Faruk Gölogluu, and Amir Tabatabai for helpful discussions.

Competing interests. The authors have no competing interests to declare.

Financial support. Ondřej Ježil was supported by Charles University Research Center program No. UNCE/24/SCI/022, the project SVV-2025-260837, and by the GA UK project No. 246223.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press

References

[1] M. Agrawal, N. Kayal and N. Saxena, 'PRIMES is in P', *Ann. Math.* **160** (2004), 781–793.

[2] A. Atserias and I. Tzameret, 'Feasibly constructive proof of Schwartz–Zippel lemma and the complexity of finding hitting sets', in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery, 2025), 1096–1107.

[3] S. R. Buss, *Bounded Arithmetic*. PhD thesis, Princeton University, 1985.

[4] L. Chen, J. Li and I. C. Oliveira, 'Reverse mathematics of complexity lower bounds', in *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2024), 505–527.

[5] L. Chen, Z. Lu, I. C. Oliveira, H. Ren and R. Santhanam, 'Polynomial-time pseudodeterministic construction of primes', in *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2023), 1261–1270.

[6] S. Cook and P. Nguyen, *Logical Foundations of Proof Complexity*, volume 11 (Cambridge University Press, Cambridge, 2010).

[7] S. A. Cook, 'Feasibly constructive proofs and the propositional calculus (preliminary version)', in *Proceedings of the Seventh Annual ACM Symposium on Theory of Computing*, STOC '75 (New York, NY, Association for Computing Machinery, 1975), 83–97.

[8] A. Gaysin, 'Proof complexity of universal algebra in a csp dichotomy proof', 2024, arXiv preprint arXiv:2403.06704.

[9] A. Healy and E. Viola, 'Constant-depth circuits for arithmetic in finite fields of characteristic two', in *Annual Symposium on Theoretical Aspects of Computer Science* (Springer, 2006), 672–683.

[10] E. Jeřábek, *Weak pigeonhole principle, and randomized computation*. PhD thesis, Ph. D. thesis, Faculty of Mathematics and Physics, Charles University, Prague, 2005.

[11] E. Jeřábek, 'Abelian groups and quadratic residues in weak arithmetic', *Math. Logic Quarterly* **56**(3) (2010), 262–278.

[12] E. Jeřábek, 'Iterated multiplication in VTC^0', *Arch. Math. Logic* **61**(5) (2022), 705–767.

[13] E. Jeřábek, 'Dual weak pigeonhole principle, boolean complexity, and derandomization', *Ann. Pure Appl. Logic* **129**(1–3) (2004), 1–37.

[14] O. Ježil, Prime Factorization in Models of PV_1, to appear in Logical Methods in Computer Science, 2026.

[15] J. Krajíček, *Bounded Arithmetic, Propositional Logic and Complexity Theory*, volume 60 (Cambridge University Press, Cambridge, 1995).

[16] J. Krajíček, P. Pudlák and G. Takeuti, 'Bounded arithmetic and the polynomial hierarchy', *Ann. Pure Appl. Logic* **52**(1–2) (1991), 143–153.

[17] M. Müller and J. Pich, 'Feasibly constructive proofs of succinct weak circuit lower bounds', *Ann. Pure Appl. Logic* **171**(2) (2020), 102735.

[18] P. Nguyen, *Bounded reverse mathematics*. PhD thesis, University of Toronto, 2008.

[19] I. C. Oliveira, 'Meta-mathematics of computational complexity theory', *ACM SIGACT News*, **56**(1) (2025), 41–68.

[20] J. Pich, 'Logical strength of complexity theory and a formalization of the PCP theorem in bounded arithmetic', *Log. Methods Comput. Sci.* **11** (2015), 1–38.

https://doi.org/10.1017/fms.2026.10194 Published online by Cambridge University Press