# Mechanisation of AKS Algorithm: Part 1 – the Main Theorem

Hing-Lun Chan[1] and Michael Norrish[2]

[1] joseph.chan@anu.edu.au
Australian National University
[2] Michael.Norrish@nicta.com.au
Canberra Research Lab., NICTA*;
*also,* Australian National University

**Abstract.** The AKS algorithm (by Agrawal, Kayal and Saxena) is a significant theoretical result proving "PRIMES in P", as well as a brilliant application of ideas from finite fields. This paper describes the first step towards the goal of a full mechanisation of this result: a mechanisation of the AKS Main Theorem, which justifies the correctness (but not the complexity) of the AKS algorithm.

## 1 Introduction

The AKS algorithm is a decision procedure for primality testing. That is, given a number $n$, it returns "true" if $n$ is prime and "false" otherwise. As *per* the title of AKS paper [3],"PRIMES is in P", the significance of their work is that the number of steps for the verification is bounded by some polynomial function of the size of $n$, measured by $\log_2 n$.

There have been several attempts to formalize the AKS Main Theorem (see Section 6), but so far none is complete. In this paper, we describe the first complete mechanization of this result. In subsequent work, we aim to demonstrate that the algorithm built on top of this result does indeed compute its answer in polynomial time.

### 1.1 Overview

A number $n$ is a perfect-power of another number $m$ if there exists an exponent $e$ such that $n = m^e$, and $n$ is power-free if it is a trivial perfect power, *i.e.*, if $n = m^e$ then $e = 1$ and $m = n$. Given a number $n$, the smallest positive exponent $j$ such that $n^j \equiv 1 \pmod{k}$ is denoted by $\mathsf{order}_k(n)$. Computation in $(\bmod\ n,\ \mathsf{X}^k - 1)$ means that all numerical as well as polynomial computational results are reduced to remainders after divisions by $n$ and by $\mathsf{X}^k - 1$. The constant polynomial arising from constant $c$ is denoted by boldface $\boldsymbol{c}$. More notation will be covered in Section 1.2. Here is a peek at our HOL4 result.

**Theorem 1.** *The AKS Main Theorem.*

$$\begin{array}{l}
\vdash \mathsf{prime}\ n \iff \\
\quad 1 < n \land \mathsf{power\_free}\ n \land \\
\quad \exists k. \\
\qquad \mathsf{prime}\ k \land (2\,(\log n + 1))^2 \le \mathsf{order}_k(n) \land \\
\qquad (\forall j.\ 0 < j \land j \le k \land j < n \Rightarrow \mathsf{gcd}(n,j) = 1) \land \\
\qquad (k < n \Rightarrow \\
\qquad\quad \forall c. \\
\qquad\qquad 0 < c \land c \le 2\sqrt{k}\,(\log n + 1) \Rightarrow \\
\qquad\qquad\quad (\mathsf{X} + \boldsymbol{c})^n \equiv (\mathsf{X}^n + \boldsymbol{c}) \pmod{n,\ \mathsf{X}^k - 1})
\end{array}$$

* NICTA is funded by the Australian Government through the Department of Communications and the Australian Research Council through the ICT Centre of Excellence Program.

This theorem then justifies the following algorithm[1] for primality testing:

```
Input: integer $n > 1$.
1. If ($n = b^m$ for some base $b$ with $m > 1$), return COMPOSITE.
2. Search for a prime $k$ satisfying $\mathsf{order}_k(n) \geq (2\,(\log n + 1))^2$.
3. For each ($j = 1$ to $k$) if ($j = n$) break, else if ($\mathsf{gcd}(j, n) \neq 1$), return COMPOSITE.
4. If ($k \geq n$), return PRIME.
5. For each ($c = 1$ to $2\sqrt{k}\,(\log n + 1)$) if $(\mathsf{X} + \boldsymbol{c})^n \not\equiv (\mathsf{X}^n + \boldsymbol{c}) \pmod{n,\ \mathsf{X}^k - 1}$,
   return COMPOSITE.
6. return PRIME.
```

Given a number $n$, this version of the AKS algorithm requires a search for another prime $k$ in Step 2. Step 4 suggests that it is not always true that $k < n$. Nevertheless, the theorem can still be viewed as a well-founded recursive definition because it turns out that $k$ is roughly bounded by $(\log n)^5$ [3]. So, for sufficiently large values of $n$, there will always be a $k < n$. For smaller $n$ (effectively the base cases of recursion), a look-up table might be used.

The rest of this paper is devoted to explaining the mechanised proof of this result. Section 2 covers some necessary background. Sections 3 and 4 describe the proof of the AKS Main Theorem. Section 5 discusses our mechanisation experience. Section 6 compares our work with others. Finally, we conclude in Section 7.

### 1.2 Notation

All statements starting with a turnstile ($\vdash$) are HOL4 theorems, automatically pretty-printed to LaTeX from the relevant theory in the HOL4 development. Generally, our notation allows an appealing combination of quantifiers ($\forall$, $\exists$), set notation ($\in$, $\cup$ and comprehensions such as $\{\,x \mid x < 6\,\}$), and functional programming ($\lambda$ for function abstraction, and juxtaposition for function application).

The cardinality of a set $s$ is written $|s|$; the image of set $s$ under the mapping $f$ is written $f(\!|s|\!)$; we write $f : s \hookrightarrow t$ to mean that function $f$ is injective from set $s$ to set $t$.

*Number-theoretic Notation* With $n$ a natural number, $\sqrt{n}$ is its square-root, and $\log n$ its logarithm to base 2. Both logarithm and square-root are integer functions, being the floor value of the corresponding real functions. We use $\varphi(n)$ to denote the Euler $\varphi$-function of $n$, the count of coprime numbers less than $n$. We write $n \mid m$ when $n$ divides $m$.

For the AKS algorithm, we shall use $n$ for the input number, $p$ for its prime factor, $k$ for the prime (existentially quantified) "parameter" of the Main Theorem, and $\ell = 2\sqrt{k}\,(\log n + 1)$ for a computed parameter (the limit for a range of constants). Note that $\mathsf{order}_k(n)$ is nonzero whenever $\mathsf{gcd}(k, n) = 1$.

*Ring, Field, and Polynomial Notation* A ring $\mathcal{R}$ has carrier set $\mathsf{R}$, with $\mathbf{1}$ and $\mathbf{0}$ its one and zero. The characteristic of a ring $\mathcal{R}$ is written as $\chi(\mathcal{R})$, often abbreviated to $\chi$ for a generic ring. A ring homomorphism from a ring $\mathcal{R}$ to another ring $\mathcal{S}$ *via* a map $f$ is denoted by $f : \mathcal{R} \mapsto_r \mathcal{S}$.

We write $\mathcal{R}[\mathsf{X}]$ to denote the ring of polynomials with coefficients drawn from the underlying ring $\mathcal{R}$. Similarly, the ring $\mathcal{F}[\mathsf{X}]$ has polynomials with coefficients from a field $\mathcal{F}$. Polynomials from those rings are written with the sans-serif font, *e.g.*, $\mathsf{p}$, $\mathsf{q}$, $\mathsf{h}$. The constant polynomial $\boldsymbol{c}$ (in bold) is derived from adding $\mathbf{1}$ repeatedly $c$ times. The degree of $\mathsf{p}$ is written $\mathsf{deg}\ \mathsf{p}$, its leading coefficient is $\mathsf{lead}\ \mathsf{p}$, and

[1] The constants involved in this algorithm are based on [10, Algorithm 8.2.1]. They are slightly different from those in the AKS papers [2, 3], but such variations do not affect the conclusion of "PRIMES is in P".

$\mathsf{monic}\ \mathsf{p}$ means its leading coefficient is $\mathbf{1}$. The polynomial $\mathsf{X}$ is the monomial (monic of degree 1) with zero constant. The polynomial field quotiented by modulus with an irreducible polynomial $\mathsf{h}$ is $\mathcal{F}_{\mathsf{h}}[\mathsf{X}]$, with multiplicative group $\mathcal{F}_{\mathsf{h}}^{*}[\mathsf{X}]$.

Arithmetic (addition, subtraction, multiplication, remainders) on polynomials is written with usual symbols ($+$, $-$, $*$, $\bmod$ *etc.*), *e.g.*, $\mathsf{X}^{k}\ -\ \mathbf{1}$ is the unity polynomial of degree $k$. Here we can see HOL4's overloading facilities at work: constant polynomials one and zero are $\mathbf{1}$ and $\mathbf{0}$, the same as those for a ring. More aggressively, we use overloading to conceal "implicit" parameters such as the underlying ring $\mathcal{R}$ in terms such as $\mathsf{p} * \mathsf{q}$ (polynomial product).

We write $\mathsf{p}[\![\mathsf{q}]\!]$ to denote the substitution of $\mathsf{q}$ for every $\mathsf{X}$ in $\mathsf{p}$. We use $\mathsf{roots}\ \mathsf{p}$ for the set of $\mathsf{p}$'s roots, and $\mathsf{ipoly}\ \mathsf{p}$ to mean that $\mathsf{p}$ is an irreducible polynomial, both with respect to its underlying ring $\mathcal{R}$. The quotient ring formed by $\mathcal{R}[\mathsf{X}]$ and irreducible polynomial $\mathsf{h}$ is denoted by $\mathcal{R}_{\mathsf{h}}[\mathsf{X}]$, which can be shown to be a field. Its multiplicative group is $\mathcal{R}_{\mathsf{h}}^{*}[\mathsf{X}]$. The order of an element in this group, *e.g.*, $\mathsf{X}$, is denoted by $\mathsf{order}_{\mathsf{h}}(\mathsf{X})$.

*HOL4 Sources* All our proof scripts can be found at `http://bitbucket.org/jhlchan/hol/src/aks/theories`.

## 2 Background

A glance at the algorithm in Section 1.1 shows its most prominent feature: polynomial identity tests in modulo $\mathsf{X}^{k}\ -\ \mathbf{1}$. To understand this we need to get a feel for the motivation behind the AKS algorithm.

### 2.1 Finite Fields

The AKS Main Theorem has a setting in finite fields, since the characteristic of a finite field is always prime. A field is also a ring, and a ring with prime characteristic enjoys some wonderful properties.

**Theorem 2.** *The Freshman-Fermat Theorem*

$$\vdash \mathsf{Ring}\ \mathcal{R}\ \wedge\ \mathsf{prime}\ \chi\ \Rightarrow\ \forall c.\ \ (\mathsf{X}\ +\ \boldsymbol{c})^{\chi}\ =\ \mathsf{X}^{\chi}\ +\ \boldsymbol{c}$$

*Proof.* This follows directly from two theorems, (a) Freshman's Theorem:

$$\vdash \mathsf{Ring}\ \mathcal{R}\ \wedge\ \mathsf{prime}\ \chi\ \Rightarrow\ \forall \mathsf{p}\ \mathsf{q}.\ \ \mathsf{poly}\ \mathsf{p}\ \wedge\ \mathsf{poly}\ \mathsf{q}\ \Rightarrow\ (\mathsf{p}\ +\ \mathsf{q})^{\chi}\ =\ \mathsf{p}^{\chi}\ +\ \mathsf{q}^{\chi}$$

and (b) Fermat's Little Theorem for polynomials:

$$\vdash \mathsf{Ring}\ \mathcal{R}\ \wedge\ \mathsf{prime}\ \chi\ \Rightarrow\ \forall c.\ \ \boldsymbol{c}^{\chi}\ =\ \boldsymbol{c}$$

Both theorems (a) and (b) have been mechanized in a previous paper by the same authors [6]. □

The converse, suitably formulated, is also true:

**Theorem 3.** *A ring has its characteristic prime iff a Freshman-Fermat identity holds for any constant coprime with the characteristic.*

$$\vdash \mathsf{Ring}\ \mathcal{R}\ \Rightarrow\ \forall c.\ \ \mathsf{gcd}(c,\chi)\ =\ 1\ \Rightarrow\ (\mathsf{prime}\ \chi\ \iff\ 1\ <\ \chi\ \wedge\ (\mathsf{X}\ +\ \boldsymbol{c})^{\chi}\ =\ \mathsf{X}^{\chi}\ +\ \boldsymbol{c})$$

Given a number $n\ >\ 1$, we can identify $\mathcal{R}$ with $\mathbb{Z}_n$, and $\chi(\mathbb{Z}_n)\ =\ n$. Since $\mathsf{gcd}(1,n)\ =\ 1$ always, pick $c\ =\ 1$, then this theorem applies, and whether $n$ is prime is just one check of a Freshman-Fermat polynomial identity in $\mathbb{Z}_n$, *i.e.*, $\pmod{n}$.

Therefore, this theorem amounts to a deterministic primality test. But there is a catch: the left-side, upon expansion, contains $n\ +\ 1$ terms. Thus this is an impractical primality test for large values of $n$.

The AKS idea begins with checking such Freshman-Fermat identities, with two twists:

- Instead of just checking in $\pmod{n}$, perform the computations in $\pmod{n,\ \mathsf{X}^k - \mathbf{1}}$ for a suitably chosen parameter $k$. Since results are always the remainder after division by $\mathsf{X}^k - \mathbf{1}$, the degree of intermediate polynomials (which determines the number of terms) never exceed $k$—presumably $k$ is much smaller than $n$.
- Instead of checking just one coprime value, check for a range of coprime values $c$, for $0 < c \leq \ell$, up to some maximum limit $\ell$—presumably $\ell$ is related to $k$, and small compared to $n$.

Of course, the big question is whether after such modifications there is still a primality test. The AKS team answered this in the affirmative—there exist parameters $k$ and $\ell$, bounded by some polynomial function of the size of input number $n$, *i.e.*, $\log n$, giving a polynomial-time deterministic primality test.

### 2.2 Introspective Relation

Recall from Section 1.1 that AKS computations are done in $\pmod{n,\ \mathsf{X}^k - 1}$. This double modulo notation is clumsy. Let us work in a generic ring $\mathcal{R}$, later to be identified with instances such as $\mathbb{Z}_n$. The first $\pmod{n}$ equivalence becomes equality in the ring $\mathcal{R}$ (*i.e.*, $x \equiv y \pmod{n}$ means $x = y$ in $\mathbb{Z}_n$); leaving the symbol $(\equiv)$ to indicate the polynomial modulo equivalence in $\mathcal{R}[\mathsf{X}]$.

In this context, of a general ring $\mathcal{R}$, the polynomial identity checks in Theorem 1 take the form:

$$(\mathsf{X} + \boldsymbol{c})^{n} \equiv \mathsf{X}^n + \boldsymbol{c} \pmod{\mathsf{X}^k - \mathbf{1}}$$

They look like Freshman-Fermat identities of Theorem 2, only now under modulo by a polynomial. Rewriting with a polynomial substitution, the left and right sides are strikingly similar:

$$(\mathsf{X} + \boldsymbol{c})^{n}[\![\mathsf{X}]\!] \equiv (\mathsf{X} + \boldsymbol{c})[\![\mathsf{X}^n]\!] \pmod{\mathsf{X}^k - \mathbf{1}}$$

The rewrites are trivial, since for any polynomial $\mathsf{p}$, we have $\mathsf{p}[\![\mathsf{X}]\!] = \mathsf{p}$ and $(\mathsf{X} + \boldsymbol{c})[\![\mathsf{p}]\!] = \mathsf{p} + \boldsymbol{c}$. Superficially, the left-hand side is transformed into the right-hand side simply by shifting of the exponent $n$. Following the terminology of AKS team, we say $n$ is *introspective* to polynomial $\mathsf{p}$, denoted by $n \bowtie \mathsf{p}$, when:

$$\vdash n \bowtie \mathsf{p} \iff \mathsf{poly}\ \mathsf{p} \land 0 < k \land \mathsf{p}^n \equiv \mathsf{p}[\![\mathsf{X}^n]\!] \pmod{\mathsf{X}^k - \mathbf{1}}$$

Note that the symbol for introspective relation $(\bowtie)$ hides the polynomial modulus $\mathsf{X}^k - \mathbf{1}$, and the underlying ring $\mathcal{R}$. We shall include a subscript when the underlying ring is of significance, *e.g.*, $\bowtie_{\mathbb{Z}_n}$.

Therefore, the AKS algorithm verifies, for the input number $n$, the identities $n \bowtie \mathsf{X} + \boldsymbol{c}$ in $\mathbb{Z}_n$ for $0 < c \leq \ell$ up to some maximum $\ell$. Moreover, Freshman-Fermat (Theorem 2) can be restated as:

**Theorem 4.** *For a ring with prime characteristic, its characteristic is introspective to any monomial.*

$$\vdash \mathsf{Ring}\ \mathcal{R} \land \mathbf{1} \neq \mathbf{0} \land \mathsf{prime}\ \chi \Rightarrow \forall k.\ 0 < k \Rightarrow \forall c.\ \chi \bowtie \mathsf{X} + \boldsymbol{c}$$

*Proof.* By introspective definition, this is to show: $(\mathsf{X} + \boldsymbol{c})^{\chi} \equiv (\mathsf{X} + \boldsymbol{c})[\![\mathsf{X}^{\chi}]\!] \pmod{\mathsf{X}^k - \mathbf{1}}$. Transforming the right side by substitution, $(\mathsf{X} + \boldsymbol{c})[\![\mathsf{X}^{\chi}]\!] = \mathsf{X}^{\chi} + \boldsymbol{c}$. Then both sides are equal by Freshman-Fermat (Theorem 2), hence they are equivalent under modulo by $\mathsf{X}^k - \mathbf{1}$. □

The fundamental properties of introspective relation are:

**Theorem 5.** *Introspective relation is multiplicative for exponents.*

$$\vdash \mathsf{Ring}\ \mathcal{R} \land \mathbf{1} \neq \mathbf{0} \Rightarrow \forall k\ \mathsf{p}\ n\ m.\ n \bowtie \mathsf{p} \land m \bowtie \mathsf{p} \Rightarrow n\,m \bowtie \mathsf{p}$$

*Proof.* Working in $(\mathrm{mod}\ \mathsf{X}^k - \mathbf{1})$, we have $\mathsf{p}^n \equiv \mathsf{p}[\![\mathsf{X}^n]\!]$ by $n \bowtie \mathsf{p}$, and $\mathsf{p}^m \equiv \mathsf{p}[\![\mathsf{X}^m]\!]$ by $m \bowtie \mathsf{p}$. The latter means $\mathsf{p}[\![\mathsf{X}]\!]^m - \mathsf{p}[\![\mathsf{X}^m]\!]$ is divisible by $\mathsf{X}^k - \mathbf{1}$. Substitute every $\mathsf{X}$ of the previous statement by $\mathsf{X}^n$, and noting $\mathsf{X}^k - \mathbf{1} \mid (\mathsf{X}^n)^k - \mathbf{1}$ by divisibility of unity polynomials, $\mathsf{p}[\![\mathsf{X}^n]\!]^m \equiv \mathsf{p}[\![(\mathsf{X}^n)^m]\!]$. Therefore, $\mathsf{p}^{n\,m} = (\mathsf{p}^n)^m \equiv \mathsf{p}[\![\mathsf{X}^n]\!]^m \equiv \mathsf{p}[\![(\mathsf{X}^n)^m]\!] = \mathsf{p}[\![\mathsf{X}^{n\,m}]\!]$, or $n\,m \bowtie \mathsf{p}$. □

**Theorem 6.** *Introspective relation is multiplicative for polynomials.*

$$\vdash \mathsf{Ring}\ \mathcal{R} \wedge \mathbf{1} \neq \mathbf{0} \Rightarrow \forall k\ \mathsf{p}\ \mathsf{q}\ n.\ n \bowtie \mathsf{p} \wedge n \bowtie \mathsf{q} \Rightarrow n \bowtie \mathsf{p} * \mathsf{q}$$

*Proof.* Working in $(\mathrm{mod}\ \mathsf{X}^k - \mathbf{1})$, we have $\mathsf{p}^n \equiv \mathsf{p}[\![\mathsf{X}^n]\!]$ by $n \bowtie \mathsf{p}$, and $\mathsf{q}^n \equiv \mathsf{q}[\![\mathsf{X}^n]\!]$ by $n \bowtie \mathsf{q}$. Therefore, $(\mathsf{p} * \mathsf{q})^n = \mathsf{p}^n * \mathsf{q}^n \equiv \mathsf{p}[\![\mathsf{X}^n]\!] * \mathsf{q}[\![\mathsf{X}^n]\!] = (\mathsf{p} * \mathsf{q})[\![\mathsf{X}^n]\!]$, or $n \bowtie \mathsf{p} * \mathsf{q}$. □

## 3 Main Theorem

We can now restate the AKS Main Theorem (Theorem 1) in terms of the introspective relation.

**Theorem 7.** *A number is prime iff it satisfies all the AKS checks.*

$$\begin{array}{l}
\vdash \mathsf{prime}\ n \iff \\
\quad 1 < n \wedge \mathsf{power\_free}\ n \wedge \\
\quad \exists k. \\
\qquad \mathsf{prime}\ k \wedge (2\,(\log n + 1))^2 \leq \mathsf{order}_k(n) \wedge \\
\qquad (\forall j.\ 0 < j \wedge j \leq k \wedge j < n \Rightarrow \mathsf{gcd}(n,j) = 1) \wedge \\
\qquad (k < n \Rightarrow \\
\qquad\quad \forall c.\ 0 < c \wedge c \leq 2\sqrt{k}\,(\log n + 1) \Rightarrow n \bowtie_{\mathbb{Z}_n} \mathsf{X} + \boldsymbol{c})
\end{array}$$

Note how the symbol $\bowtie_{\mathbb{Z}_n}$ encapsulates the introspective relation (*i.e.*, $\mathrm{mod}\ \mathsf{X}^k - \mathbf{1}$) within $\mathbb{Z}_n$ (*i.e.*, $\mathrm{mod}\ n$), the double modulo in the AKS computations. We prove this logical equivalence in two parts.

### 3.1 Easy Part (⇒)

**Theorem 8.** *The if-part of AKS Main Theorem (Theorem 7).*

$$\begin{array}{l}
\vdash \mathsf{prime}\ n \Rightarrow \\
\quad 1 < n \wedge \mathsf{power\_free}\ n \wedge \\
\quad \exists k. \\
\qquad \mathsf{prime}\ k \wedge (2\,(\log n + 1))^2 \leq \mathsf{order}_k(n) \wedge \\
\qquad (\forall j.\ 0 < j \wedge j \leq k \wedge j < n \Rightarrow \mathsf{gcd}(n,j) = 1) \wedge \\
\qquad (k < n \Rightarrow \forall c.\ 0 < c \wedge c \leq 2\sqrt{k}\,(\log n + 1) \Rightarrow n \bowtie_{\mathbb{Z}_n} \mathsf{X} + \boldsymbol{c})
\end{array}$$

*Proof.* The first two goals, $1 < n$ and $\mathsf{power\_free}\ n$, are trivial for a prime $n$. For the third goal, let $m = (2\,(\log n + 1))^2$, then parameter $k$ exists by Theorem 25 in Section 4.6:

$$\vdash 1 < n \wedge 0 < m \Rightarrow \exists k.\ \mathsf{prime}\ k \wedge \mathsf{gcd}(k,n) = 1 \wedge m \leq \mathsf{order}_k(n)$$

If $k \geq n$, the coprime checks are subsumed by $\forall j.\ 0 < j \wedge j < n \Rightarrow \mathsf{gcd}(n,j) = 1$. Otherwise $k < n$, and the coprime checks are subsumed by $\forall j.\ 0 < j \wedge j \leq k \Rightarrow \mathsf{gcd}(n,j) = 1$. Either way this is true since a prime $n$ is coprime with all values less than itself. When $k < n$, the last check is established by Theorem 4, since a prime $n$ gives a field $\mathbb{Z}_n$, with $\chi(\mathbb{Z}_n) = n$. □

A close equivalent of this Theorem 8 was mechanised by de Moura and Tadeu [9] in Coq, and by Campos *et al* [5] in ACL2.

### 3.2 Hard Part ($\Leftarrow$)

**Theorem 9.** *The only-if part of AKS Main Theorem (Theorem 7).*

$$\begin{array}{l}
\vdash 1 < n \land \mathsf{power\_free}\ n \land \\
\quad (\exists k. \\
\qquad \mathsf{prime}\ k \land (2\ (\log n + 1))^2 \le \mathsf{order}_k(n) \land \\
\qquad (\forall j.\ 0 < j \land j \le k \land j < n \Rightarrow \mathsf{gcd}(n,j) = 1) \land \\
\qquad (k < n \Rightarrow \forall c.\ 0 < c \land c \le 2\sqrt{k}\ (\log n + 1) \Rightarrow n \bowtie_{\mathbb{Z}_n} \mathsf{X} + \boldsymbol{c})) \Rightarrow \\
\quad \mathsf{prime}\ n
\end{array}$$

*Proof.* Based on the given parameter $k$, let $\ell = 2\sqrt{k}\ (\log n + 1)$. If $k \ge n$ the coprime checks will verify $\forall j.\ 0 < j \land j < n \Rightarrow \mathsf{gcd}(n,j) = 1$, thus $n$ will be prime since it has no proper factor. Otherwise $k < n$, the coprime checks are $\forall j.\ 0 < j \land j \le k \Rightarrow \mathsf{gcd}(n,j) = 1$. In Section 3.3 we shall establish:

**Theorem 10.** *The AKS Main Theorem in $\mathbb{Z}_n$.*

$$\begin{array}{l}
\vdash 1 < n \Rightarrow \\
\quad \forall k\ \ell. \\
\qquad \mathsf{prime}\ k \land (2\ (\log n + 1))^2 \le \mathsf{order}_k(n) \land \ell = 2\sqrt{k}\ (\log n + 1) \land \\
\qquad (\forall j.\ 0 < j \land j \le k \Rightarrow \mathsf{gcd}(n,j) = 1) \land \\
\qquad (\forall c.\ 0 < c \land c \le \ell \Rightarrow n \bowtie_{\mathbb{Z}_n} \mathsf{X} + \boldsymbol{c}) \Rightarrow \\
\qquad\quad \exists p.\ \mathsf{prime}\ p \land \mathsf{perfect\_power}\ n\ p
\end{array}$$

Applying this theorem, $n = p^e$ for some prime $p$ and exponent $e$ by definition of a perfect power. But $n$ is assumed power-free, so $e = 1$ and $n = p$, making $n$ a prime. □

### 3.3 Shifting Playgrounds

The AKS verifications take polynomials with coefficients from $\mathbb{Z}_n$, a ring for general $n$. Polynomials with coefficients from a ring can have more roots than their degree, due to the possible existence of zero divisors in a ring.[2] A field has no zero divisors, and polynomials with coefficients from a field have this nice property:

$$\vdash \mathsf{Field}\ \mathcal{F} \Rightarrow \forall \mathsf{p}.\ \mathsf{poly}\ \mathsf{p} \land \mathsf{p} \ne \mathbf{0} \Rightarrow |\mathsf{roots}\ \mathsf{p}| \le \mathsf{deg}\ \mathsf{p}$$

As we shall see (Sections 4.3 and 4.4), there will be two important injective maps involved in the AKS proof. To establish the injective property, this restriction on the number of polynomial roots by its degree is of utmost importance.

But where to find a field $\mathcal{F}$ to work with, given that we start in the ring $\mathbb{Z}_n$?

When the number $n$ is not 1, it must have a prime factor $p$. This leads to the field $\mathbb{Z}_p$. If relationships between monomials $\mathsf{X} + \boldsymbol{c}$ are carried over unaffected from $\mathbb{Z}_n[\mathsf{X}]$ to $\mathbb{Z}_p[\mathsf{X}]$, we are in a better place to investigate the nature of $n$. This shifting of playgrounds is essential in the proof of Theorem 10:

*Proof (of Theorem 10).*
If $n$ is prime, take $p = n$. Otherwise, $n$ has a proper prime factor $p$ such that $p < n$ and $p \mid n$. Introduce two rings, $\mathbb{Z}_n$ and $\mathbb{Z}_p$. The latter ring $\mathbb{Z}_p$ is also a field, in fact a finite field. This is because all nonzero elements are coprime to the prime modulus $p$, hence they have inverses.

There is a homomorphism between these two rings due to that fact that $p$ divides $n$:

[2] For example, in $\mathbb{Z}_6$, $2 \times 3 = 0$, hence $(X - 2)(X - 3) = X^2 - 5X = X(X - 5)$, which shows a polynomial of degree 2 can have more than 2 roots.

$$\vdash\ 0 < n \wedge 0 < p \wedge p \mid n \Rightarrow (\lambda x.\ x \bmod p) : \mathbb{Z}_n \mapsto_r \mathbb{Z}_p$$

This ring homomorphism will preserve monomials $\mathsf{X} + \boldsymbol{c}$ if a condition on limit $\ell$ is met:

$$\begin{array}{l}\vdash\ 0 < n \wedge 1 < p \wedge \ell < p \Rightarrow \\ \qquad \forall c.\ 0 < c \wedge c \le \ell \Rightarrow \forall f.\ f : \mathbb{Z}_n \mapsto_r \mathbb{Z}_p \Rightarrow f(\mathsf{X} + \boldsymbol{c}) = \mathsf{X} + \boldsymbol{c}\end{array}$$

Here $f(\mathsf{p})$ denotes applying the ring homomorphism $f$ to each coefficient of a polynomial $\mathsf{p}$. We shall show in Section 4.6 that $\ell \le k$ (Theorem 27). To meet the condition $\ell < p$, we need only to show $k < p$. Note that the given coprime checks on $k$ are (from the statement of Theorem 10):

$$\forall j.\ 0 < j \wedge j \le k \Rightarrow \mathsf{gcd}(n,j) = 1$$

Taking $j = k$, we conclude $\mathsf{gcd}(n,k) = 1$. This will be useful later. Apply the following theorems:

$$\begin{array}{l}\vdash\ 1 < n \wedge \mathsf{prime}\ p \wedge p \mid n \Rightarrow \forall j.\ \mathsf{gcd}(n,j) = 1 \Rightarrow \mathsf{gcd}(p,j) = 1 \\ \vdash\ 1 < p \Rightarrow \forall k.\ (\forall j.\ 0 < j \wedge j \le k \Rightarrow \mathsf{gcd}(p,j) = 1) \Rightarrow k < p\end{array}$$

Tracing the transformation of gcd's gives $k < p$, hence $\ell < p$.

Therefore the monomials are preserved by homomorphism, together with the introspective relation:

$$\begin{array}{l}\vdash\ 0 < n \wedge 1 < p \wedge p \mid n \wedge 0 < k \wedge \ell < p \Rightarrow \\ \qquad \forall m\ c.\ 0 < c \wedge c \le \ell \wedge m \bowtie_{\mathbb{Z}_n} \mathsf{X} + \boldsymbol{c} \Rightarrow m \bowtie_{\mathbb{Z}_p} \mathsf{X} + \boldsymbol{c}\end{array}$$

Thus the AKS checks in $\mathbb{Z}_n$ are equivalent to checks in $\mathbb{Z}_p$, a finite field, where $p$ is a prime factor of $n$. Generalising to arbitrary finite fields, in Section 4.5 we will prove:

**Theorem 11.** *AKS Main Theorem in finite fields.*

$$\begin{array}{l}\vdash\ \mathsf{FiniteField}\ \mathcal{F} \wedge \mathsf{prime}\ k \wedge k < \chi \Rightarrow \\ \qquad \forall n. \\ \qquad\quad 1 < n \wedge \chi \mid n \wedge \mathsf{gcd}(n,k) = 1 \wedge (2\ (\log n + 1))^2 \le \mathsf{order}_k(n) \wedge \\ \qquad\quad \ell = 2\sqrt{k}\ (\log n + 1) \wedge (\forall c.\ 0 < c \wedge c \le \ell \Rightarrow n \bowtie \mathsf{X} + \boldsymbol{c}) \Rightarrow \\ \qquad\qquad \mathsf{perfect\_power}\ n\ \chi\end{array}$$

We then identify $\mathcal{F}$ with $\mathbb{Z}_p$, noting $\chi(\mathbb{Z}_p) = p$, with $k < p$. Knowing $\mathsf{gcd}(n,k) = 1$ from the gcd checks above, we conclude that $n$ must be a perfect power of its prime factor $p$, as required. □

## 4 Introspective Game

There are two useful facts when working in the context of a finite field $\mathcal{F}$, where $\chi$ is necessarily prime:

- We get, for free in $\mathcal{F}[\mathsf{X}]$, the result: $\chi \bowtie \mathsf{X} + \boldsymbol{c}$, by Theorem 4, since a field is a non-trivial ring.
- The modulus polynomial $\mathsf{X}^k - \mathbf{1}$, now in $\mathcal{F}[\mathsf{X}]$, will have a monic irreducible factor $\mathsf{h} \neq \mathsf{X} - \mathbf{1}$.

Both will play significant roles in the proof of Theorem 11. Here are the highlights:

- The finite field $\mathcal{F}$ will enrich the introspective relation, through the interplay between prime $\chi$ and $n$.
- This will give rise to some interesting sets, among them are two finite sets $\widehat{\mathcal{N}}$ and $\mathcal{M}$ (Section 4.2).
- The conditions on parameters $k$ and $\ell$ will establish an injective map from $\widehat{\mathcal{N}}$ to $\mathcal{M}$.
- If $n$ were not a perfect power of $\chi$, then we would have $|\widehat{\mathcal{N}}| > |\mathcal{M}|$, contradicting the Pigeonhole Principle.

### Summary of the AKS proof (Theorem 11)

Our strategy for the AKS proof can be described as a game between two players (see Figure 1). The introspective relations of $n$ and $p$, a prime factor of $n$, give rise to two sets $\mathcal{N}$ and $\mathcal{P}$ (Section 4.1). Taking modulo by $k$ (an AKS parameter) and by $\mathsf{h}$ (an irreducible factor of $\mathsf{X}^k - \mathbf{1}$), the sets $\mathcal{N}$ and $\mathcal{P}$ map (straight arrows), respectively, to two finite sets $\mathcal{M}$ and $\mathcal{Q}_{\mathsf{h}}$ (Section 4.2). Two finite subsets of $\mathcal{N}$ and $\mathcal{P}$, shown as $\widehat{\mathcal{N}}$ and $\widehat{\mathcal{P}}$, can be crafted in such a way that injective maps (curve arrows) between the finite sets can be constructed, if $k$ and $\ell$ (another AKS parameter) are suitably chosen to satisfy the "if" conditions (Section 4.3 and Section 4.4). The construction of injective maps involves interactions (dashed arrows) between the two players, based on properties of the introspective relation and polynomials in $\mathcal{F}_{\mathsf{h}}[\mathsf{X}]$. Once these are all in place, if $n$ were not a perfect power of $p$, the grey set $\widehat{\mathcal{N}}$ will have more than $|\mathcal{M}|$ elements, where $\mathcal{M}$ is the target of the left injective map. This contradicts the Pigeonhole Principle (Section 4.5). Hence $n$ must be a perfect power of its prime factor $p$.

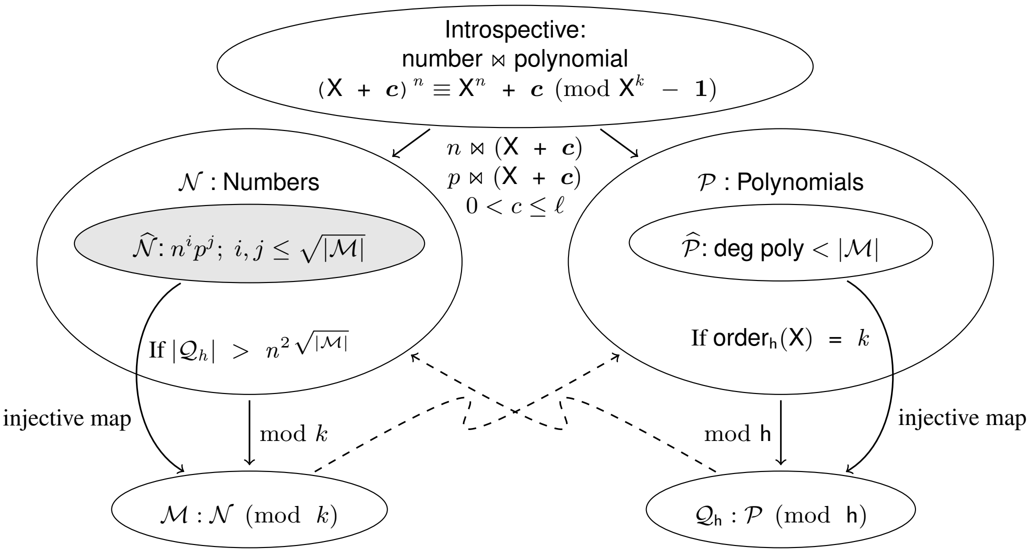
Introspective:
number $\bowtie$ polynomial
$(\mathsf{X} + \boldsymbol{c})^n \equiv \mathsf{X}^n + \boldsymbol{c} \pmod{\mathsf{X}^k - \mathbf{1}}$
$n \bowtie (\mathsf{X} + \boldsymbol{c})$
$p \bowtie (\mathsf{X} + \boldsymbol{c})$
$0 < c \le \ell$
$\mathcal{N}$ : Numbers
$\widehat{\mathcal{N}}$: $n^i p^j;\ i, j \le \sqrt{|\mathcal{M}|}$
If $|\mathcal{Q}_h| > n^{2\sqrt{|\mathcal{M}|}}$
injective map
mod $k$
$\mathcal{M} : \mathcal{N} \pmod{k}$
$\mathcal{P}$ : Polynomials
$\widehat{\mathcal{P}}$: deg poly $< |\mathcal{M}|$
If $\mathsf{order}_{\mathsf{h}}(\mathsf{X}) = k$
mod $\mathsf{h}$
injective map
$\mathcal{Q}_{\mathsf{h}} : \mathcal{P} \pmod{\mathsf{h}}$

**Fig. 1.** The AKS proof as a game between numbers and polynomials *via* introspective relation. Refer to summary above for an explanation.

### 4.1 Introspective Sets

As noted above, after shifting to a finite field $\mathcal{F}$ where $p = \chi$ is prime, for the constants $0 < c \le \ell$, besides the given $n \bowtie \mathsf{X} + \boldsymbol{c}$, we also have $p \bowtie \mathsf{X} + \boldsymbol{c}$ by Theorem 4.

In view of this, we define the following two sets:

$\vdash \mathcal{N} = \{m \mid \mathsf{gcd}(m, k) = 1 \land \forall c.\ 0 < c \land c \le \ell \Rightarrow m \bowtie \mathsf{X} + \boldsymbol{c}\}$
$\vdash \mathcal{P} = \{\mathsf{p} \mid \mathsf{poly}\ \mathsf{p} \land \forall m.\ m \in \mathcal{N} \Rightarrow m \bowtie \mathsf{p}\}$

The set $\mathcal{N}$ captures the introspective exponents. Observe that $n \in \mathcal{N}$, $p \in \mathcal{N}$, and trivially, $1 \in \mathcal{N}$. They are all coprime to $k$, since the coprime checks in Section 3.3 give $\mathsf{gcd}(n, k) = 1$ and $k < p$. For a prime $p$, $k < p$ gives $\mathsf{gcd}(p, k) = 1$.

The set $\mathcal{P}$ captures the introspective polynomials, those with introspective exponents in $\mathcal{N}$. Certainly $\forall c.\ 0 < c \land c \le \ell \Rightarrow \mathsf{X} + \boldsymbol{c} \in \mathcal{P}$, and trivially, $\mathbf{1} \in \mathcal{P}$.

Recall the fundamental properties of introspective relation: there will be multiplicative exponents for $\mathcal{N}$ (Theorem 5) and multiplicative polynomials for $\mathcal{P}$ (Theorem 6). Together they imply that the sets $\mathcal{N}$ and $\mathcal{P}$ will be infinitely large. Our contradiction from the Pigeonhole Principle comes when we have derived some related, and finite sets.

### 4.2 Modulo Sets

One way to get a finite counterpart from an infinite set is by looking at remainders after division, or image of the set under some modulus. For the exponents set $\mathcal{N}$, the parameter $k$ provides a modulus:

$$\vdash \mathcal{M} = (\lambda m.\ m \bmod k)\,(\!|\mathcal{N}|\!)$$

It is easy to estimate the cardinality of $\mathcal{M}$:

**Theorem 12.** *The cardinality of set $\mathcal{M}$ is bounded by $k$ and $\mathsf{order}_k(n)$.*

$$\vdash \mathsf{Ring}\ \mathcal{R} \land \mathbf{1} \ne \mathbf{0} \land 1 < k \Rightarrow \forall n.\ n \in \mathcal{N} \Rightarrow \mathsf{order}_k(n) \le |\mathcal{M}| \land |\mathcal{M}| < k$$

*Proof.* Since there are $k$ remainders under modulo $k$, $|\mathcal{M}| \le k$. But multiples of $k$ (those $n$ with $n \bmod k = 0$) are not in $\mathcal{N}$, as all elements of $\mathcal{N}$ are coprime to $k$ and $k \ne 1$. Therefore $0 \notin \mathcal{M}$, making $|\mathcal{M}| < k$. Given $n \in \mathcal{N}$, so are all its powers: $\forall j.\ n^j \in \mathcal{N}$ by Theorem 5. Hence all the remainders $n^j \bmod k$ are in $\mathcal{M}$. Since $\mathsf{order}_k(n)$ is the minimal exponent $j$ before such remainders wrap around to 1, there are at least $\mathsf{order}_k(n)$ distinct remainders. Thus $\mathsf{order}_k(n) \le |\mathcal{M}|$. □

For the polynomials set $\mathcal{P}$, the irreducible factor $\mathsf{h}$ of $\mathsf{X}^k - \mathbf{1}$ provides a modulus:

$$\vdash \mathcal{Q}_{\mathsf{h}} = (\lambda \mathsf{p}.\ \mathsf{p} \bmod \mathsf{h})\,(\!|\mathcal{P}|\!)$$

For the cardinality of $\mathcal{Q}_h$, estimation requires more work, due to the change of modulus to $\mathsf{h}$. Let $\mathsf{z} = \mathsf{X}^k - \mathbf{1}$, then $\mathsf{monic}\ \mathsf{z}$ and $\mathsf{deg}\ \mathsf{z} = k$. Note that $\mathsf{z} \equiv \mathbf{0} \pmod{\mathsf{h}}$, since $\mathsf{h}$ divides $\mathsf{z}$ by being a factor. These facts ensure that polynomial equivalences in $(\mathrm{mod}\ \mathsf{z})$ are preserved to $(\mathrm{mod}\ \mathsf{h})$:

**Theorem 13.** *Polynomial modulo equivalence holds for modulus factor.*

$$\vdash \mathsf{Ring}\ \mathcal{R} \land \mathsf{monic}\ \mathsf{z} \land 0 < \mathsf{deg}\ \mathsf{z} \land \mathsf{monic}\ \mathsf{h} \land 0 < \mathsf{deg}\ \mathsf{h} \land \mathsf{z} \equiv \mathbf{0} \pmod{\mathsf{h}} \Rightarrow$$
$$\forall \mathsf{p}\ \mathsf{q}.\ \mathsf{poly}\ \mathsf{p} \land \mathsf{poly}\ \mathsf{q} \land \mathsf{p} \equiv \mathsf{q} \pmod{\mathsf{z}} \Rightarrow \mathsf{p} \equiv \mathsf{q} \pmod{\mathsf{h}}$$

*Proof.* When $(\mathsf{p} - \mathsf{q})$ is divisible by $\mathsf{z}$ (due to $\mathsf{p} \equiv \mathsf{q} \pmod{\mathsf{z}}$), and $\mathsf{z}$ is divisible by $\mathsf{h}$ (due to $\mathsf{z} \equiv \mathbf{0} \pmod{\mathsf{h}}$), the difference $(\mathsf{p} - \mathsf{q})$ is also divisible by $\mathsf{h}$ due to transitivity of division. □

An irreducible polynomial $\mathsf{h}$ gives a polynomial modulo field $\mathcal{F}_{\mathsf{h}}[\mathsf{X}]$, and nonzero elements of a field form a multiplicative group. Since $\mathsf{X} \ne \mathbf{0}$, it has a nonzero $\mathsf{order}_{\mathsf{h}}(\mathsf{X})$, with the following feature.

**Theorem 14.** *When $\mathsf{X}$ is a root of unity, order of $\mathsf{X}$ equals degree of unity when the degree is prime.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \land \mathsf{monic}\ \mathsf{h} \land \mathsf{ipoly}\ \mathsf{h} \land \mathsf{h} \ne \mathsf{X} - \mathbf{1} \Rightarrow$$
$$\forall k.\ \mathsf{prime}\ k \land \mathsf{X}^k \equiv \mathbf{1} \pmod{\mathsf{h}} \Rightarrow \mathsf{order}_{\mathsf{h}}(\mathsf{X}) = k$$

*Proof.* Let $t = \mathsf{order}_{\mathsf{h}}(\mathsf{X})$. By definition of order, $\mathsf{X}^t \equiv \mathbf{1} \pmod{\mathsf{h}}$, and given $\mathsf{X}^k \equiv \mathbf{1} \pmod{\mathsf{h}}$. Since $t$ is the minimal exponent for powers of $\mathsf{X}$ to wrap back to $\mathbf{1}$, $t$ divides $k$. Note that degree of unity $\mathsf{X}^k - \mathbf{1}$ is $k$. Given prime $k$, $t = 1$ or $t = k$. Only $\mathbf{1}$ has order 1, but $\mathsf{X} \not\equiv \mathbf{1} \pmod{\mathsf{h}}$ by assumption. Therefore $\mathsf{order}_{\mathsf{h}}(\mathsf{X}) = t = k$. □

**Theorem 15.** *In the polynomial field $\mathcal{F}_{\mathsf{h}}[\mathsf{X}]$, powers of* $\mathsf{X}$ *are distinct for exponents less than* $\mathsf{order}_{\mathsf{h}}(\mathsf{X})$.

$$\begin{array}{l}\vdash \mathsf{FiniteField}\ \mathcal{F}\ \wedge\ \mathsf{monic}\ \mathsf{h}\ \wedge\ \mathsf{ipoly}\ \mathsf{h}\ \wedge\ \mathsf{h} \neq \mathsf{X} \Rightarrow \\ \qquad \forall m\ n.\ m < \mathsf{order}_{\mathsf{h}}(\mathsf{X}) \wedge n < \mathsf{order}_{\mathsf{h}}(\mathsf{X}) \Rightarrow (\mathsf{X}^m \equiv \mathsf{X}^n \pmod{\mathsf{h}} \iff m = n)\end{array}$$

*Proof.* Since $\mathcal{F}_{\mathsf{h}}[\mathsf{X}]$ is a finite field, its multiplicative group is a finite group. By the given assumption, $\mathsf{X} \not\equiv \mathbf{0} \pmod{\mathsf{h}}$, thus $\mathsf{X}$ is an element in this group. Its order is the minimal exponent for the powers of $\mathsf{X}$ to wrap around to $\mathbf{1}$. Given the exponents are less than its order, such powers of $\mathsf{X}$ are distinct. □

We shall see how the distinct powers of $\mathsf{X}$ lead to a lower bound for $\mathcal{Q}_{\mathsf{h}}$. This simple result is helpful:

**Theorem 16.** *Powers of* $\mathsf{X}$ *are equivalent in* $\mathsf{X}^k - \mathbf{1}$ *if exponents are equivalent in* $\mathbb{Z}_k$.

$$\vdash \mathsf{Ring}\ \mathcal{R}\ \wedge\ \mathbf{1} \neq \mathbf{0} \Rightarrow \forall k.\ 0 < k \Rightarrow \forall m.\ \mathsf{X}^m \equiv \mathsf{X}^{m \bmod k} \pmod{\mathsf{X}^k - \mathbf{1}}$$

*Proof.* Since $m = (m \operatorname{div} k)k + m \bmod k$ and $\mathsf{X}^k \equiv \mathbf{1} \pmod{\mathsf{X}^k - \mathbf{1}}$, the result follows. □

### 4.3 Reduced Polynomials

Referring to Figure 1, we shall see eventually that the right injective map is essential to give a lower bound for $\mathcal{Q}_h$, and this lower bound is essential to provide the left injective map. These two injective maps are critical in the AKS proof.

To obtain a lower bound for $\mathcal{Q}_h$, we need another way to get something finite from the infinite set $\mathcal{P}$, by taking a reduced subset of $\mathcal{P}$:

$$\vdash \widehat{\mathcal{P}} = \{\mathsf{p} \mid \mathsf{p} \in \mathcal{P} \wedge \mathsf{deg}\ \mathsf{p} < |\mathcal{M}|\}$$

This is a finite subset of $\mathcal{P}$ due to the polynomial degree cut-off. We shall prove that there is an injective map from $\widehat{\mathcal{P}}$ to $\mathcal{Q}_{\mathsf{h}}$, hence a lower bound on $|\widehat{\mathcal{P}}|$ will also be a lower bound for $|\mathcal{Q}_{\mathsf{h}}|$.

First, note an interesting interaction from $\mathcal{M}$ to $\mathcal{P}$, which is relevant to $\widehat{\mathcal{P}}$ since $\widehat{\mathcal{P}} \subseteq \mathcal{P}$. We know that $\mathcal{P}$ has a lot of elements (Section 4.1), but $\mathcal{Q}_h$ is finite, so there are two polynomials $\mathsf{p} \in \mathcal{P}$ and $\mathsf{q} \in \mathcal{P}$ that map together in $\mathcal{Q}_h$. It turns out that introspective relation helps to identify some interesting roots of their difference $(\mathsf{p} - \mathsf{q})$, from the elements of $\mathcal{M}$.

**Theorem 17.** *Each element in $\mathcal{M}$ gives a root for a difference polynomial in* $\mathcal{F}_{\mathsf{h}}[\mathsf{X}]$ *composed of two polynomials from $\mathcal{P}$ with the same image in $\mathcal{Q}_h$.*

$$\begin{array}{l}\vdash \mathsf{Field}\ \mathcal{F}\ \wedge\ \mathsf{monic}\ \mathsf{h}\ \wedge\ 0 < \mathsf{deg}\ \mathsf{h}\ \wedge\ \mathsf{X}^k - \mathbf{1} \equiv \mathbf{0} \pmod{\mathsf{h}} \Rightarrow \\ \qquad \forall \mathsf{p}\ \mathsf{q}. \\ \qquad\quad \mathsf{p} \in \mathcal{P} \wedge \mathsf{q} \in \mathcal{P} \wedge \mathsf{p} \equiv \mathsf{q} \pmod{\mathsf{h}} \Rightarrow \\ \qquad\qquad \forall n.\ n \in \mathcal{M} \Rightarrow (\mathsf{p} - \mathsf{q})[\![\mathsf{X}^n]\!] \equiv \mathbf{0} \pmod{\mathsf{h}}\end{array}$$

*Proof.* Given $n \in \mathcal{M}$, there is $m \in \mathcal{N}$ such that $n = m \bmod k$. Therefore $m \bowtie \mathsf{p}$ and $m \bowtie \mathsf{q}$ by definition of $\mathcal{P}$. Let $\mathsf{z} = \mathsf{X}^k - \mathbf{1}$. Note that $\mathsf{z} \equiv \mathbf{0} \pmod{\mathsf{h}}$ by assumption. We can proceed:

| | | |
|---|---|---|
| | $\mathsf{p}^m \equiv \mathsf{p}[\![\mathsf{X}^m]\!] \pmod{\mathsf{z}}$ | by $m \bowtie \mathsf{p}$ |
| and | $\mathsf{p}[\![\mathsf{X}^m]\!] \equiv \mathsf{p}[\![\mathsf{X}^n]\!] \pmod{\mathsf{z}}$ | by Theorem 16 |
| so | $\mathsf{p}^m \equiv \mathsf{p}[\![\mathsf{X}^n]\!] \pmod{\mathsf{z}}$ | by transitivity |
| or for $\mathsf{p}$ , by $\mathsf{z} \equiv \mathbf{0} \pmod{\mathsf{h}}$ | $\mathsf{p}^m \equiv \mathsf{p}[\![\mathsf{X}^n]\!] \pmod{\mathsf{h}}$ | by Theorem 13—[1] |
| Repeat the same steps for $\mathsf{q}$ | $\mathsf{q}^m \equiv \mathsf{q}[\![\mathsf{X}^n]\!] \pmod{\mathsf{h}}$ | by $m \bowtie \mathsf{q}$ *etc.*—[2] |
| Since | $\mathsf{p}^m \equiv \mathsf{q}^m \pmod{\mathsf{h}}$ | by $\mathsf{p} \equiv \mathsf{q} \pmod{\mathsf{h}}$ given |
| so | $\mathsf{p}[\![\mathsf{X}^n]\!] \equiv \mathsf{q}[\![\mathsf{X}^n]\!] \pmod{\mathsf{h}}$ | by [1] and [2] above |
| or | $(\mathsf{p} - \mathsf{q})[\![\mathsf{X}^n]\!] \equiv \mathbf{0} \pmod{\mathsf{h}}$ | as claimed. |

□

Due to this, an injective map between the two finite sets derived from $\mathcal{P}$ is possible:

**Theorem 18.** *There is an injective map from reduced set of $\mathcal{P}$ to modulo set of $\mathcal{P}$.*

$$\vdash \ \mathsf{FiniteField}\ \mathcal{F} \wedge 0 < k \wedge \mathsf{monic}\ \mathsf{h} \wedge \mathsf{ipoly}\ \mathsf{h} \wedge \mathsf{X}^k - \mathbf{1} \equiv \mathbf{0} \pmod{\mathsf{h}} \wedge$$
$$k = \mathsf{order}_\mathsf{h}(\mathsf{X}) \Rightarrow$$
$$(\lambda \mathtt{p}.\ \mathtt{p} \bmod \mathtt{h}) : \widehat{\mathcal{P}} \hookrightarrow \mathcal{Q}_\mathsf{h}$$

*Proof.* Let $\mathsf{p},\ \mathsf{q} \in \widehat{\mathcal{P}}$, with $\mathsf{p} \equiv \mathsf{q} \pmod{\mathsf{h}}$ in $\mathcal{Q}_\mathsf{h}$. For our map to be injective, we need to show $\mathsf{p} = \mathsf{q}$. Since $\widehat{\mathcal{P}} \subseteq \mathcal{P}$, $\mathsf{p},\ \mathsf{q} \in \mathcal{P}$. Theorem 17 applies: each $n \in \mathcal{M}$ gives a root $\mathsf{X}^n$ for $(\mathsf{p} - \mathsf{q})$. Now $\mathsf{h} \neq \mathsf{X}$ because, by assumption, $\mathsf{h} \mid \mathsf{X}^k - \mathbf{1}$, but $\mathsf{X} \not\mid \mathsf{X}^k - \mathbf{1}$, and $n < k$ since $n \in \mathcal{M}$ means $n$ is a remainder in $\pmod{k}$. By assumption, $k = \mathsf{order}_\mathsf{h}(\mathsf{X})$, hence these roots are distinct by Theorem 15. Thus there are at least $|\mathcal{M}|$ distinct roots for $(\mathsf{p} - \mathsf{q})$.

But $\mathsf{deg}\ \mathsf{p} < |\mathcal{M}|$ and $\mathsf{deg}\ \mathsf{q} < |\mathcal{M}|$ since $\mathsf{p},\ \mathsf{q} \in \widehat{\mathcal{P}}$, hence $\mathsf{deg}\ (\mathsf{p} - \mathsf{q}) < |\mathcal{M}|$. There are more roots than its degree for the difference $(\mathsf{p} - \mathsf{q})$ with coefficients from a finite field $\mathcal{F}$. This is possible only when the difference is $\mathbf{0}$, *i.e.*, $\mathsf{p} = \mathsf{q}$. □

This injective map leads to a lower bound for the cardinality of $\mathcal{Q}_\mathsf{h}$.

**Theorem 19.** *The modulo set of $\mathcal{P}$ has a nice lower bound.*

$$\vdash \ \mathsf{FiniteField}\ \mathcal{F} \wedge 1 < k \wedge k = \mathsf{order}_\mathsf{h}(\mathsf{X}) \wedge \ell < \chi \wedge \mathsf{monic}\ \mathsf{h} \wedge \mathsf{ipoly}\ \mathsf{h} \wedge$$
$$\mathsf{X}^k - \mathbf{1} \equiv \mathbf{0} \pmod{\mathsf{h}} \Rightarrow$$
$$2^{\mathsf{min}(\ell,|\mathcal{M}|)} \leq |\mathcal{Q}_\mathsf{h}|$$

*Proof.* Applying Theorem 18, there is an injective map from $\widehat{\mathcal{P}}$ to $\mathcal{Q}_\mathsf{h}$. As both sets are finite, $|\widehat{\mathcal{P}}| \leq |\mathcal{Q}_h|$. We shall estimate $|\widehat{\mathcal{P}}|$, by counting how many polynomials $\mathsf{p} \in \mathcal{P}$ have $\mathsf{deg}\ \mathsf{p} < |\mathcal{M}|$.

Note that $1 < |\mathcal{M}|$, since $\mathsf{order}_k(n) \leq |\mathcal{M}|$ by Theorem 12, and $1 < \mathsf{order}_k(n)$ since $n \neq 1$. A simple estimate for $|\widehat{\mathcal{P}}|$ proceeds as follows:

- For $0 < c \leq \ell$, $\mathsf{X} + \boldsymbol{c} \in \widehat{\mathcal{P}}$, since each monomial is in $\mathcal{P}$, and each has a degree equal to 1.
- Given $\ell < \chi$, these monomials are distinct, as $\chi$ is the least additive wrap-around of $\mathbf{1}$ in field $\mathcal{F}$.[3]
- By Theorem 6, any product of these monomials will be in $\widehat{\mathcal{P}}$, if the product has a degree less than $|\mathcal{M}|$.
- If $\ell < |\mathcal{M}|$, there are less than $|\mathcal{M}|$ such monomials. Therefore any product drawn from a subset of $\{\mathsf{X} + \boldsymbol{c} \mid 0 < c \leq \ell\}$ will have a degree less than $|\mathcal{M}|$. There are $2^\ell$ such products.
- If $|\mathcal{M}| \leq \ell$, reduce the constants range to $0 < c \leq |\mathcal{M}|$. Any product drawn from a subset of $\{\mathsf{X} + \boldsymbol{c} \mid 0 < c \leq |\mathcal{M}|\}$ will have a degree less than $|\mathcal{M}|$, almost—the product of all such monomials must be excluded. However, $\mathbf{1} \in \widehat{\mathcal{P}}$, but $\mathbf{1}$ is not a monomial product. There are still $2^{|\mathcal{M}|}$ products.

Considering both cases, we conclude that $2^{\mathsf{min}(\ell,|\mathcal{M}|)} \leq |\mathcal{Q}_h|$. □

### 4.4 Reduced Exponents

It turns out that an injective map to $\mathcal{M}$ is possible based on the following set of reduced exponents:

$$\vdash \ \widehat{\mathcal{N}}\ p\ n\ m = \{p^i\, n^j \mid i \leq m \wedge j \leq m\}$$

This is generated by the two known elements $n, p \in \mathcal{N}$ (Section 4.1), with cut-off $m$ in their exponents. By multiplicative closure of introspective exponents (Theorem 5), $\widehat{\mathcal{N}} \subseteq \mathcal{N}$. Observe the following property:

**Theorem 20.** *Upper bound of an element in $\widehat{\mathcal{N}}\ p\ n\ m$.*

$$\vdash \ 1 < p \wedge p \leq n \Rightarrow \forall e\ m.\ e \in \widehat{\mathcal{N}}\ p\ n\ m \Rightarrow e \leq n^{2\,m}$$

[3] The characteristic $\chi$ of a ring $\mathcal{R}$ is defined as the order of $\mathbf{1}$ in the additive group of $\mathcal{R}$, *i.e.*, $\chi\mathbf{1} = \mathbf{0}$.

*Proof.* Each $e \in \widehat{\mathcal{N}}\ p\ n\ m$ has the form $p^i\, n^j$, where $i, j \le m$. Given $p \le n$, we can deduce $e = p^i\, n^j \le n^i\, n^j \le n^m\, n^m = n^{2\,m}$. □

Note another interesting interaction from $\mathcal{Q}_\mathsf{h}$ to $\mathcal{N}$, which is relevant to $\widehat{\mathcal{N}}$ since $\widehat{\mathcal{N}}\ n\ p\ m \subseteq \mathcal{N}$. Pick two exponents $n \in \mathcal{N}$ and $m \in \mathcal{N}$ that map together in $\mathcal{M}$. Consider the difference polynomial $\mathsf{X}^n - \mathsf{X}^m$. It turns out that the introspective relation helps to identify some interesting roots of this difference polynomial, from the elements of $\mathcal{Q}_\mathsf{h}$.

**Theorem 21.** *Each element in $\mathcal{Q}_\mathsf{h}$ gives a root for a difference polynomial in $\mathcal{F}_\mathsf{h}[\mathsf{X}]$ constructed with two exponents from $\mathcal{N}$ with same image in $\mathcal{M}$.*

$$\begin{array}{l}
\vdash \mathsf{Field}\ \mathcal{F} \land \mathsf{monic}\ \mathsf{h} \land \mathsf{ipoly}\ \mathsf{h} \land \mathsf{X}^k - \mathbf{1} \equiv \mathbf{0} \pmod{\mathsf{h}} \Rightarrow \\
\qquad \forall n\ m. \\
\qquad\quad n \in \mathcal{N} \land m \in \mathcal{N} \land n \equiv m \pmod{k} \Rightarrow \\
\qquad\qquad \forall \mathsf{p}.\ \mathsf{p} \in \mathcal{Q}_\mathsf{h} \Rightarrow (\mathsf{X}^n - \mathsf{X}^m)[\![\mathsf{p}]\!] \equiv \mathbf{0} \pmod{\mathsf{h}}
\end{array}$$

*Proof.* Given $\mathsf{p} \in \mathcal{Q}_\mathsf{h}$, there is $\mathsf{q} \in \mathcal{P}$ such that $\mathsf{p} = \mathsf{q} \bmod \mathsf{h}$. Therefore $n \bowtie \mathsf{q}$ and $m \bowtie \mathsf{q}$ by definition of $\mathcal{P}$. Let $z = \mathsf{X}^k - \mathbf{1}$. Note that $\mathsf{z} \equiv \mathbf{0} \pmod{\mathsf{h}}$ by given. We can proceed:

| | | |
|---|---|---|
| | $\mathsf{q}^n \equiv \mathsf{q}[\![\mathsf{X}^n]\!] \pmod{\mathsf{z}}$ | by $n \bowtie \mathsf{q}$ — [1] |
| | $\mathsf{q}^m \equiv \mathsf{q}[\![\mathsf{X}^m]\!] \pmod{\mathsf{z}}$ | by $m \bowtie \mathsf{q}$ — [2] |
| and | $\mathsf{q}[\![\mathsf{X}^m]\!] \equiv \mathsf{q}[\![\mathsf{X}^n]\!] \pmod{\mathsf{z}}$ | by Theorem 16 |
| so | $\mathsf{q}^n \equiv \mathsf{q}^m \pmod{\mathsf{z}}$ | by [1], [2], transitivity |
| Therefore | $\mathsf{q}^n - \mathsf{q}^m \equiv \mathbf{0} \pmod{\mathsf{z}}$ | by subtraction |
| by $\mathsf{z} \equiv \mathbf{0} \pmod{\mathsf{h}}$ | $\mathsf{q}^n - \mathsf{q}^m \equiv \mathbf{0} \pmod{\mathsf{h}}$ | by Theorem 13—[3] |
| Since | $(\mathsf{X}^n - \mathsf{X}^m)[\![\mathsf{p}]\!] \equiv (\mathsf{X}^n - \mathsf{X}^m)[\![\mathsf{q}]\!] \pmod{\mathsf{h}}$ | by $\mathsf{p} = \mathsf{q} \bmod \mathsf{h}$ —[4] |
| and the right-side | $(\mathsf{X}^n - \mathsf{X}^m)[\![\mathsf{q}]\!] = \mathsf{q}^n - \mathsf{q}^m$ | by substitution of $\mathsf{q}$ —[5] |
| Combine [4],[5],[3] | $(\mathsf{X}^n - \mathsf{X}^m)[\![\mathsf{p}]\!] \equiv \mathbf{0} \pmod{\mathsf{h}}$ | as claimed. |

□

Due to this, an injective map between the two finite sets derived from $\mathcal{N}$ is possible:

**Theorem 22.** *There is an injective map from reduced set of $\mathcal{N}$ to modulo set of $\mathcal{N}$.*

$$\begin{array}{l}
\vdash \mathsf{FiniteField}\ \mathcal{F} \land \mathsf{monic}\ \mathsf{h} \land \mathsf{ipoly}\ \mathsf{h} \land \mathsf{X}^k - \mathbf{1} \equiv \mathbf{0} \pmod{\mathsf{h}} \Rightarrow \\
\qquad \forall n\ p. \\
\qquad\quad 1 < p \land p < n \land n \in \mathcal{N} \land p \in \mathcal{N} \land n^{2\sqrt{|\mathcal{M}|}} < |\mathcal{Q}_\mathsf{h}| \Rightarrow \\
\qquad\qquad (\lambda m.\ m \bmod k) : \widehat{\mathcal{N}}\ p\ n\ \sqrt{|\mathcal{M}|} \hookrightarrow \mathcal{M}
\end{array}$$

*Proof.* Let $i,\ j \in \widehat{\mathcal{N}}\ n\ p\ \sqrt{|\mathcal{M}|}$, with $i \equiv j \pmod{k}$ in $\mathcal{M}$. If the map is to be injective, we need $i = j$. Since $\widehat{\mathcal{N}}\ n\ p\ \sqrt{|\mathcal{M}|} \subseteq \mathcal{N}$, both $i, j \in \mathcal{N}$. Theorem 21 applies: every $\mathsf{p} \in \mathcal{Q}_h$ is a root of $\mathsf{X}^i - \mathsf{X}^j$. Hence there are at least $|\mathcal{Q}_h|$ roots.

By Theorem 20, both $i,\ j$ are bounded by $n^{2\sqrt{|\mathcal{M}|}}$, hence $\mathsf{deg}\ (\mathsf{X}^i - \mathsf{X}^j) \le n^{2\sqrt{|\mathcal{M}|}}$. Given $n^{2\,|\mathcal{M}|} < |\mathcal{Q}_\mathsf{h}|$, there are more roots than its degree for the polynomial $(\mathsf{X}^i - \mathsf{X}^j)$ with coefficients from a finite field $\mathcal{F}$. This is not possible, unless it is $\mathbf{0}$, which means $i = j$. □

## 4.5 Punch Line

Given a prime $p$ that divides $n$, if $n^x = p^y$ for some exponents $x, y$ with $x > 0$, what can we conclude?

**Theorem 23.** *A condition that implies a number is a perfect power of prime.*

$$\vdash\ 0 < n \wedge \textsf{prime}\ p \wedge p \mid n \wedge (\exists x\ y.\ 0 < x \wedge p^x = n^y) \Rightarrow \textsf{perfect\_power}\ n\ p$$

*Proof.* Since $p \mid n$, divide $n$ by $p$ as many times as possible, and express $n = p^m q$ where $m$ is the maximum possible, and $p \nmid q$. The equation $p^x = n^y$ becomes $p^x = (p^m q)^y = p^{my} q^y$. By unique factorisation, with prime $p$ and $p \nmid q$ and $x \neq 0$, it must be that $y \neq 0$, and $q^y = 1$, *i.e.*, $q = 1$. □

When its generators have a special property, the cardinality of $\widehat{\mathcal{N}}\ p\ n\ m$ is simple to express:

**Theorem 24.** *Cardinality of $\widehat{\mathcal{N}}$ when generators $n$ and prime divisor $p$ are not related by perfect power.*

$$\begin{array}{l}
\vdash\ \textsf{Ring}\ \mathcal{R} \wedge \mathbf{1} \neq \mathbf{0} \wedge 1 < k \Rightarrow \\
\quad \forall n\ p\ m. \\
\qquad n \in \mathcal{N} \wedge p \in \mathcal{N} \wedge \textsf{prime}\ p \wedge p \mid n \wedge \neg\textsf{perfect\_power}\ n\ p \Rightarrow \\
\qquad\quad |\widehat{\mathcal{N}}\ p\ n\ m| = (m+1)^2
\end{array}$$

*Proof.* Let $f = (\lambda\ (i,j)\ .\ p^i\, n^j)$, $t = \{j \mid j \leq m\}$. From its definition, it is simple to verify that $\widehat{\mathcal{N}}\ p\ n\ m = \{p^i\, n^j \mid i \leq m \wedge j \leq m\} = f(\!|t \times t|\!)$. More interesting is that the conditions will imply $f : t \times t \hookrightarrow \widehat{\mathcal{N}}\ p\ q\ n$. Once this is proved, being the image of an injective map gives $|\widehat{\mathcal{N}}\ p\ q\ n| = |t \times t| = |t|^2 = (m+1)^2$.

To show that the map is injective, assume $p^i\, n^j = p^u\, n^v$ for some $i, j$ and $u, v$. We need to show $i = u$ and $j = v$. This comes down to analysis by cases.

If $i < u$, only the case $j > v$ is interesting, with $n^{j-v} = p^{u-i}$. As $j - v \neq 0$, Theorem 23 applies, giving $\textsf{perfect\_power}\ n\ p$, which contradicts the assumption. By the symmetric roles of $i, j$ and $u, v$, the case $i > u$ leads to the same contradiction. The only possible case is $i = u$, giving $j = v$. □

This property is crucial in order to complete the proof of AKS Main Theorem (Theorem 11).

*Proof (of Theorem 11).* AKS Main Theorem in finite fields

$$\begin{array}{l}
\vdash\ \textsf{FiniteField}\ \mathcal{F} \wedge \textsf{prime}\ k \wedge k < \chi \Rightarrow \\
\quad \forall n. \\
\qquad 1 < n \wedge \chi \mid n \wedge \textsf{gcd}(n,k) = 1 \wedge (2\ (\log n + 1))^2 \leq \textsf{order}_k(n) \wedge \\
\qquad \ell = 2\sqrt{k}\ (\log n + 1) \wedge (\forall c.\ 0 < c \wedge c \leq \ell \Rightarrow n \bowtie \mathsf{X} + \boldsymbol{c}) \Rightarrow \\
\qquad\quad \textsf{perfect\_power}\ n\ \chi
\end{array}$$

Let $p = \chi$. By assumption, $p \mid n$, so $p \leq n$. The case $p = n$ is trivial, so we shall assume $p < n$.

The finite field $\mathcal{F}$ gives prime $p$, so $p \bowtie \mathsf{X} + \boldsymbol{c}$ (Theorem 4). We have $k < p$, so $\textsf{gcd}(p, k) = 1$. Assuming $\textsf{gcd}(n, k) = 1$ and $n \bowtie \mathsf{X} + \boldsymbol{c}$, we have the ingredients for the introspective sets $\mathcal{N}$ and $\mathcal{P}$ (Section 4.1). Their finite counterparts, the modulo sets $\mathcal{M}$ and $\mathcal{Q}_{\mathsf{h}}$ (Section 4.2), and reduced sets $\widehat{\mathcal{N}}$ and $\widehat{\mathcal{P}}$ (Section 4.3 and Section 4.4) can be set up accordingly.

Recall that the introspective relation is based on modulus $\mathsf{X}^k - \mathbf{1}$. By the second useful fact in Section 4, in a finite field $\mathcal{F}$ it has a monic irreducible factor $\mathsf{h} \neq \mathsf{X} - \mathbf{1}$, *i.e.*, $\mathsf{X}^k - \mathbf{1} \equiv \mathbf{0} \pmod{\mathsf{h}}$. With $\textsf{prime}\ k$, we have $\textsf{order}_{\mathsf{h}}(\mathsf{X}) = k$ (Theorem 14), giving the injective map from $\widehat{\mathcal{P}}$ to $\mathcal{Q}_h$ (Theorem 18), which is essential for the lower bound estimate of $\mathcal{Q}_h$.

In Section 4.6, we shall investigate the parameters $k$ and $\ell$. We shall show that $\ell < k$ (Theorem 27). By assumption, $k < p$, so $\ell < p$. Therefore $2^{\textsf{min}(\ell, |\mathcal{M}|)} \leq |\mathcal{Q}_h|$ (Theorem 19, which invokes Theorem 18). We shall also show that $n^{2\sqrt{|\mathcal{M}|}} < 2^{\textsf{min}(\ell,|\mathcal{M}|)}$ (Theorem 26). Hence $n^{2\sqrt{|\mathcal{M}|}} < |\mathcal{Q}_h|$. With $p < n$, these inequalities establish the injective map from $\widehat{\mathcal{N}}\ n\ p\ \sqrt{|\mathcal{M}|}$ to $\widehat{\mathcal{N}}$ (Theorem 22).

Now, given prime $p$ and $p \mid n$, if $n$ were not a perfect power of $p$, Theorem 24 applies, so that:

$$|\widehat{\mathcal{N}}\ p\ n\ \sqrt{|\mathcal{M}|}| = (\sqrt{|\mathcal{M}|} + 1)^2 = |\mathcal{M}| + (2\sqrt{|\mathcal{M}|}) + 1 > |\mathcal{M}|$$

This means the injective map from $\widehat{\mathcal{N}}\ p\ n\ \sqrt{|\mathcal{M}|}$ to $\mathcal{M}$, both finite sets, would violate the Pigeonhole Principle. Therefore, $n$ must be a perfect power of $p = \chi$. □

### 4.6 Parameters

The AKS Main Theorem contains a parameter $k$ with the property: $\mathsf{order}_k(n) \geq (2\,(\log n + 1)\,)^2$, from which a related parameter $\ell = 2\sqrt{k}\,(\log n + 1)$ is computed.

In the original AKS paper [2], parameter $k$ is a prime (for a different set of conditions) while in the revised version [3] this prime requirement on $k$ is dropped. Only the bound on $k$ affects the conclusion "PRIMES is in P", a general $k$ needs more advanced theory to establish. Our mechanisation effort is based on a prime $k$, following Dietzfelbinger [10]. We use a prime $k$ to show $k = \mathsf{order}_{\mathsf{h}}(\mathsf{X})$ in Theorem 14.

The existence of such a prime $k$ can be established by generalizing the problem: given a number $n$, and a maximum $m$, find a prime modulus $k$ such that $\mathsf{order}_k(n) \geq m$. This is applied in Theorem 8:

**Theorem 25.** *There is always a modulus $k$ giving big enough order for $n$ in $\mathbb{Z}_k$.*

$\vdash 1 < n \wedge 0 < m \Rightarrow \exists k.\ \mathsf{prime}\ k \wedge \mathsf{gcd}(k,n) = 1 \wedge m \leq \mathsf{order}_k(n)$

*Proof.* First, we define a set of candidates:

$\vdash \mathsf{candidates}\ n\ m = \{k \mid \mathsf{prime}\ k \wedge k \nmid n \wedge \forall j.\ 0 < j \wedge j < m \Rightarrow k \nmid n^j - 1\}$

Pick a large prime $z > n^m$, then $z$ cannot divide $n$ or any of the factors $n^j - 1$ for $0 < j < m$, hence $z \in \mathsf{candidates}\ n\ m$.

Thus $\mathsf{candidates}\ n\ m \neq \emptyset$, and we can pick a candidate $k$, say the least value, from the set. Being an element, $\mathsf{prime}\ k \wedge k \nmid n$. Since a prime is coprime to its non-multiples, $\mathsf{gcd}(k,n) = 1$. Thus $n$ has nonzero order in $\mathbb{Z}_k$. Let $j = \mathsf{order}_k(n)$, then $0 < j$ with $n^j \equiv 1 \pmod{k}$, or $k \mid n^j - 1$. If $j < m$, by the candidates definition $k \nmid n^j - 1$, a contradiction. Hence $\mathsf{order}_k(n) = j \geq m$. □

The parameters $k$ and $\ell$ provide a crucial inequality involving $|\mathcal{M}|$, used in Theorem 11:

**Theorem 26.** *The AKS parameters meet the inequality condition.*

$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge 1 < k \wedge 1 < n \wedge n \in \mathcal{N} \wedge (2\,(\log n + 1)\,)^2 \leq \mathsf{order}_k(n) \wedge$
$\quad \ell = 2\sqrt{k}\,(\log n + 1) \Rightarrow$
$\qquad n^{2\sqrt{|\mathcal{M}|}} < 2^{\mathsf{min}(\ell,|\mathcal{M}|)}$

*Proof.* Let $j = \mathsf{order}_k(n)$, and $m = \log n + 1$, then $2^m > n$ for integer logarithm. By Theorem 12, $j \leq |\mathcal{M}|$ and $|\mathcal{M}| < k$. By the given assumption, $(2\,m)^2 \leq j$. Taking integer square roots, we have $\sqrt{|\mathcal{M}|} \geq \sqrt{j}$, $\sqrt{k} \geq \sqrt{|\mathcal{M}|}$ and $\sqrt{j} \geq 2\,m$. Note also $|\mathcal{M}| \geq \sqrt{|\mathcal{M}|}\,\sqrt{|\mathcal{M}|}$ by integer square root. Therefore:

- $\ell = 2\sqrt{k}\,m \geq m\,(2\sqrt{|\mathcal{M}|})$
- $|\mathcal{M}| \geq \sqrt{j}\,\sqrt{|\mathcal{M}|} \geq m\,(2\sqrt{|\mathcal{M}|})$

Thus $\mathsf{min}(\ell,|\mathcal{M}|) \geq m\,(2\sqrt{|\mathcal{M}|})$, and

$$2^{\mathsf{min}(\ell,|\mathcal{M}|)} \geq 2^{m\,(2\sqrt{|\mathcal{M}|})} = 2^{m 2\sqrt{|\mathcal{M}|}} > n^{2\sqrt{|\mathcal{M}|}}.$$

□

Incidentally, the choice of $k$ and $\ell$ ensures that $\ell \leq k$, used in Theorem 10 and Theorem 11:

**Theorem 27.** *The AKS computed parameter does not exceed the modulus parameter.*

$\vdash 1 < n \wedge 1 < k \wedge \mathsf{gcd}(k,n) = 1 \wedge (2\,(\log n + 1)\,)^2 \leq \mathsf{order}_k(n) \Rightarrow$
$\qquad 2\sqrt{k}\,(\log n + 1) \leq k$

*Proof.* Since $\mathsf{order}_k(n) \mid \varphi(k)$, and $\varphi(k) < k$ when $k > 1$, we have $\mathsf{order}_k(n) < k$. Taking integer square-roots, with the given $\mathsf{order}_k(n)$, deduce

$$k \geq \sqrt{k}\,\sqrt{k} \geq \sqrt{k}\,\sqrt{\mathsf{order}_k(n)} \geq 2\sqrt{k}\,(\log n + 1)\,.$$

□

## 5 Mechanisation and Its Traps

The updated AKS proof [3] is contained within four pages. Mechanisation of such a proof is the process of unwinding the dense mathematics within those pages. It took us about a year to build up the basic libraries, another year to forge the advanced libraries, then about six months to adapt the libraries for the proof of AKS Main Theorem, during which time the missing pieces in the developed libraries were steadily being filled in.

There are always pitfalls during the mechanisation process. One example is the symbol $\mathsf{X}$ in various expositions of the AKS proof, *e.g.*, [10, 7, 8, 4]. Usually $\mathsf{X}$ starts as an indeterminate or a degree one zero constant monomial, then switches to a root of unity, even to a primitive root of unity. While this is common practice, such changes mean that we needed to prove the switchings are valid.

The substitution by $\mathsf{X}$ is fundamental in the introspective relation (Section 2.2). These subtle changes in the role of $\mathsf{X}$ presented some difficulties in our initial effort to formalize the AKS proof. Indeed, we first used an inappropriate definition and got carried along until we found that shifting playgrounds (Section 3.3) is impossible with that definition.

Shifting of playgrounds in the AKS proof is pivotal. Most expositions just point this out without further elaboration.[4] After this shifting, where the playground is now $\mathbb{Z}_p$, the introspective relation is defined in $\mathbb{Z}_p[\mathsf{X}]$, side-stepping the issue. It was in the process of mechanisation that we realized a proper formulation should start by defining the introspective relation in a ring $\mathcal{R}$ (Section 2.2), and then prove that shifting is valid through ring homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_p$ (Section 3.3).

*Lessons Learnt* Rather than attempting a direct transcription of the AKS proof, we came to understand the proof in the context of finite fields, identifying the key concepts involved in the proof, even comparing various expositions. By reformulations of polynomial theorems in number theory into their counterparts in rings and fields, a clear picture of the proof's logic emerged, resulting in this succinct presentation.

*HOL4 and Abstract Algebra* This work demonstrates that HOL4's simple type theory, together with its proof machinery, are sufficient to allow the statement and proof of moderately complicated theorems in abstract algebra. Without dependent types (as in Coq) or locales (as in Isabelle), theorems are slightly more awkward to state, but our experience is that *ad hoc* overloading gets one a long way. Over-annotation of terms so that the parser chooses the "right" meaning of a symbol like + is only necessary occasionally. Exploiting overloading in this way requires a careful understanding of just what the parser is and is not capable of, and one is often on exactly that boundary. Nonetheless, the result gives terms that are not far removed from those that have been pretty-printed in this paper. (Pretty-printing to LaTeX adds niceties such as superscripts and juxtaposition for multiplication; these could not be handled by the parser.)

Nor should we forget that Campos *et al* [5] proved half of the Main Theorem in ACL2, where the underlying logic is even simpler, and provides no static type-checking.

## 6 Related Work

*Other Pen-and-Paper Proofs* The revised proof (2004) of the AKS team [3] takes this approach: use the injective map on $\mathcal{Q}_\mathsf{h}$ to establish a lower bound for $|\mathcal{Q}_h|$; assuming that $n$ is not a power of $p$, use the Pigeonhole Principle to show that a special nonzero polynomial has at least $|\mathcal{Q}_h|$ roots, thus giving an upper bound for $|\mathcal{Q}_h|$; manipulate inequalities to show that the chosen parameters will lead to the lower bound exceeding the upper bound, hence a contradiction.

Other expositions of the AKS Main Theorem [1, 12, 11, 13] take similar approaches, working mainly in $\mathbb{Z}_p[\mathsf{X}]$. Our method is equivalent, but is clean in that we: (*i*) emphasize the important role of shifting

[4] For example, [3] first stated the computational identity in $\mathbb{Z}_n$, then "this implies" the corresponding identity in $\mathbb{Z}_p$. Only [10] proved the shifting from $\mathbb{Z}_n$ to $\mathbb{Z}_p$ as a lemma.

from $\mathbb{Z}_n$ to $\mathbb{Z}_p$ (Section 3.3); (*ii*) reformulate the AKS Main Theorem in the context of finite fields (Theorem 11); (*iii*) clarify that the choice of parameters gives injective maps between reduced sets and modulo sets (Theorem 18 and Theorem 22); (*iv*) bring in the assumption that $n$ is not a power of prime $p$ as late as possible; and (*v*) use the Pigeonhole Principle as a punch line to force $n$ to be a power of prime $p$ (Section 4.5).

*Other Mechanisations* We believe that we are the first to mechanise both directions of the central theorem of AKS algorithm. As noted earlier, two other teams (Campos *et al* [5] in ACL2, and de Moura and Tadeu [9] in Coq) have mechanised the fact that if the number being tested is prime, then the AKS algorithm will indeed report "yes".

We are also aware of preliminary work started by John Harrison, and carried out in HOL Light.[5]

## 7 Conclusion

It is well-known that the cardinality of a finite field must be a prime power, and it is elementary to check whether a number is power-free. In essence, the AKS team showed that primality testing can be reduced to finite field cardinality testing, and demonstrated that the latter can be done in polynomial time.

Through our mechanisation effort, especially in presenting the AKS proof as an introspective game (Section 4), we hope that this elementary proof of the AKS Main Theorem provides further appreciation of the AKS team's brilliant ideas.

*Future Work* While the existence of parameter $k$ in the AKS Main Theorem is assured, to show that it is bounded by a polynomial function of $\log n$ is harder. In future work, we intend to perform the necessary complexity analysis of the AKS algorithm to complete the mechanised proof that PRIMES is indeed in P.

## References

1. Manindra Agrawal. Primality tests based on Fermat's Little Theorem, December 2006. Available from `http://www.cse.iitk.ac.in/users/manindra/presentations/FLTBasedTests.pdf`.
2. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P, August 2002. Original paper.
3. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004.
4. Alberto Bedodi. Primality tests in polynomial time. Master's thesis, Universitá Degli Studi Roma TRE, February 2010.
5. Cynthia Campos, Francois Modave, and Steve Roach. Towards the verification of the AKS primality test in ACL2, November 2004. Fifth International Conference on Intelligent Technologies.
6. Hing-Lun Chan and Michael Norrish. A string of pearls: Proofs of Fermat's Little Theorem. *Journal of Formalized Reasoning*, 6(1):63–87, December 2013.
7. Richard Crandall and Carl Pomerance. *Prime Numbers: A Computational Perspective*. Springer, 2005.
8. Gabriel Daleson. Deterministic primality testing in polynomial time. Master's thesis, Portland State University, December 2006.
9. Flávio L. C. de Moura and Ricardo Tadeu. The correctness of the AKS primality test in Coq, July 2008. Available from `http://www.cic.unb.br/~flavio/AKS.pdf`.
10. Martin Dietzfelbinger. *Primality Testing in Polynomial Time: From Randomized Algorithms to 'PRIMES is in P'*. Lecture Notes in Computer Science. Springer, 2004.
11. Riaal Domingues. A polynomial time algorithm for prime recognition. Master's thesis, University of Pretoria, January 2006.
12. Benjamin Linowitz. An exposition of the AKS polynomial time primality testing. Master's thesis, University of Pennsylvania, March 2006.
13. Carl Pomerance. Primality testing, variations on a theme of Lucas, 2008. Available from `http://cm.bell-labs.com/who/carlp/PS/primalitytalk5.ps`.

[5] John was kind enough to share his approach with us *via* private communication.