Mechanisation of the AKS Algorithm

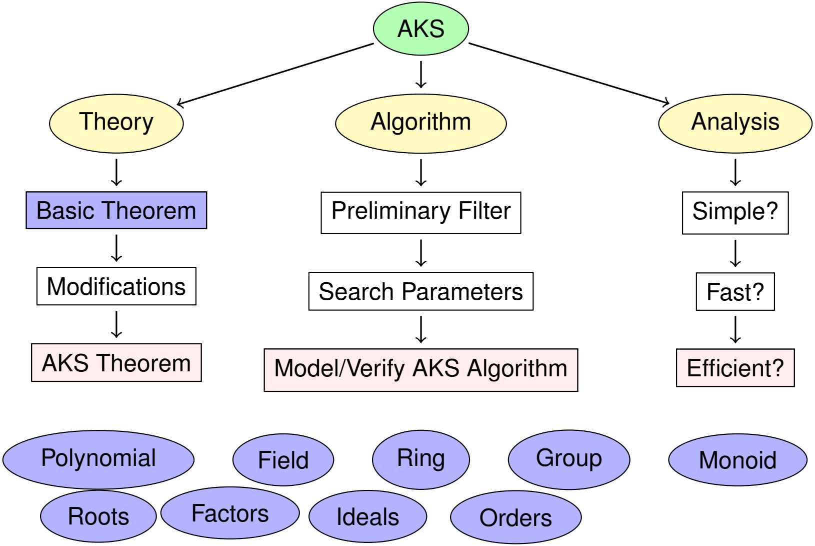
Hing-Lun Chan

College of Engineering and Computer Science
Australian National University

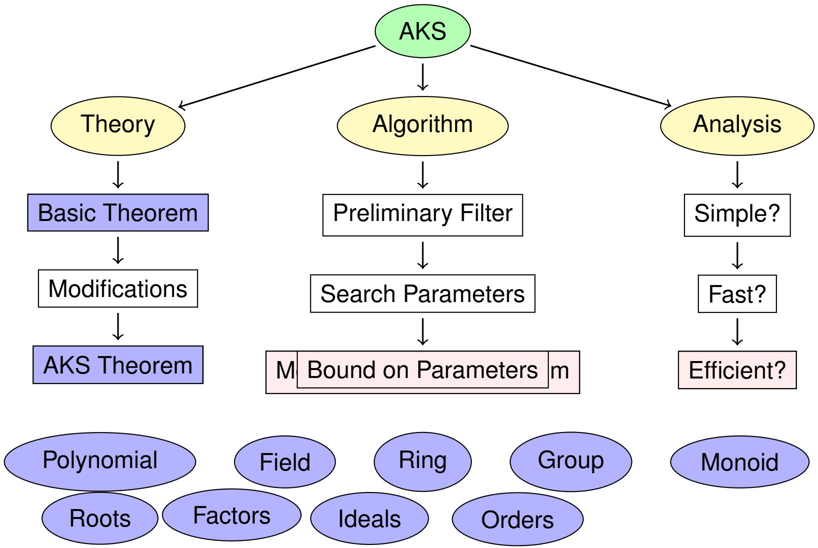
PhD Review Talk 2015

Outline

Mechanisation of AKS Algorithm – Road Map



Mechanisation of AKS Algorithm – Road Map



Basic Theorem for Primality Test

Theorem (Primality condition for the characteristic of a ring.)

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

Basic Theorem for Primality Test

Theorem (Primality condition for the characteristic of a ring.)

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

Given a number $n > 1$,

- Identify $\mathcal{R}$ as $\mathbb{Z}_n$, with $\chi(\mathbb{Z}_n) = n$.
- Always $\gcd(1, n) = 1$. Pick $c = 1$, then this theorem applies.
- Is n prime? Perfrom one Freshman-Fermat identity check in $\mathbb{Z}_n$, *i.e.*, prime $n \iff (\boldsymbol{X} + \boldsymbol{1})^n \equiv \boldsymbol{X}^n + \boldsymbol{1} \pmod{n}$.

Basic Theorem for Primality Test

Theorem (Primality condition for the characteristic of a ring.)

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

Given a number $n > 1$,

- Identify $\mathcal{R}$ as $\mathbb{Z}_n$, with $\chi(\mathbb{Z}_n) = n$.
- Always $\gcd(1, n) = 1$. Pick $c = 1$, then this theorem applies.
- Is n prime? Perfrom one Freshman-Fermat identity check in $\mathbb{Z}_n$, *i.e.*, prime $n \iff (\mathbf{X} + \mathbf{1})^{n} \equiv \mathbf{X}^{n} + \mathbf{1} \pmod{n}$.

Therefore,

- This theorem gives a deterministic primality test.
- Alas: the left-side, upon expansion, contains $(n + 1)$ terms.
- Impractical primality test for large values of n.

AKS twists

The AKS team modifies the Freshman-Fermat identities checks:

- Perform the polynomial identity checks in $\pmod{n,\ \boldsymbol{X}^k - \mathbf{1}}$ for some suitably chosen k.
- Check a range of coprime values c, for $0 < c \leq \ell$, up to some maximum limit ℓ.

AKS twists

The AKS team modifies the Freshman-Fermat identities checks:

- Perform the polynomial identity checks in $\pmod{n,\ \boldsymbol{X}^k - \mathbf{1}}$ for some suitably chosen k. Remainder has only up to k terms.
- Check a range of coprime values c, for $0 < c \leq \ell$, up to some maximum limit ℓ. Provide more ways to weed out composites.

AKS twists

The AKS team modifies the Freshman-Fermat identities checks:

- Perform the polynomial identity checks in $(\bmod\ n,\ \boldsymbol{X}^k - \mathbf{1})$ for some suitably chosen k. Remainder has only up to k terms.
- Check a range of coprime values c, for $0 < c \leq \ell$, up to some maximum limit ℓ. Provide more ways to weed out composites.

The AKS choice of parameters k and ℓ:

- $\text{order}_k(n) \geq (2(\log n + 1))^2$
- $\ell = 2\sqrt{k}(\log n + 1)$

AKS twists

The AKS team modifies the Freshman-Fermat identities checks:

- Perform the polynomial identity checks in $\pmod{n,\ \boldsymbol{X}^k - \mathbf{1}}$ for some suitably chosen k. Remainder has only up to k terms.
- Check a range of coprime values c, for $0 < c \leq \ell$, up to some maximum limit ℓ. Provide more ways to weed out composites.

The AKS choice of parameters k and ℓ:

- $\text{order}_k(n) \geq (2(\log n + 1))^2$, *i.e.*, search for k given n.
- $\ell = 2\sqrt{k}(\log n + 1)$, *i.e.*, compute ℓ from k and n.

AKS twists

The AKS team modifies the Freshman-Fermat identities checks:

- Perform the polynomial identity checks in $(\bmod\ n,\ \boldsymbol{X}^k - \mathbf{1})$ for some suitably chosen k. Remainder has only up to k terms.
- Check a range of coprime values c, for $0 < c \leq \ell$, up to some maximum limit ℓ. Provide more ways to weed out composites.

The AKS choice of parameters k and ℓ:

- $\text{order}_k(n) \geq (2(\log n + 1))^2$,*i.e.*, search for k given n.
- $\ell = 2\sqrt{k}(\log n + 1)$,*i.e.*, compute ℓ from k and n.

The AKS result:

- With k and ℓ chosen, if all modified identity checks are satisfied, then n must be a perfect power of its prime factor p.
- That is, $n = p^e$ where prime $p \mid n$ for some exponent e.
- Include a power check: if n is power free, then n must be prime.

AKS Main Theorem

Theorem (The AKS Main Theorem.)

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

AKS Main Theorem

Theorem (The AKS Main Theorem.)

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

- The details involve more checks: simple coprime checks.
- This version requires that the parameter k is prime.
- Modified identity checks are needed only when $k < n$.

Introspective Relation

AKS polynomial identity checks involve double moduli:

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

Introspective Relation

AKS polynomial identity checks involve double moduli:

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

In the context of $\mathbb{Z}_n$, which is a ring for a general n:

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

Introspective Relation

AKS polynomial identity checks involve double moduli:

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

In the context of $\mathbb{Z}_n$, which is a ring for a general n:

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

Rewriting with polynomial substitution, for a general ring $\mathcal{R}$:

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

Introspective Relation

AKS polynomial identity checks involve double moduli:

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

In the context of $\mathbb{Z}_n$, which is a ring for a general n:

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

Rewriting with polynomial substitution, for a general ring $\mathcal{R}$:

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

Define n is *introspective* to polynomial p, denoted by $n \bowtie \mathrm{p}$, when:

$$\vdash n \bowtie \mathrm{p} \iff \mathrm{poly}\ \mathrm{p} \wedge 0 < k \wedge \mathrm{p}^n \equiv \mathrm{p}[\boldsymbol{X}^n] \pmod{\boldsymbol{X}^k - \mathbf{1}}$$

Freshman-Fermat

Theorem (Prime characteristic is introspective to any monomial.)

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

Freshman-Fermat

Theorem (Prime characteristic is introspective to any monomial.)

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

Proof.

- By introspective definition, we need to show:
  $(\boldsymbol{X} + \boldsymbol{c})^{\chi} \equiv (\boldsymbol{X} + \boldsymbol{c})[\boldsymbol{X}^{\chi}] \pmod{\boldsymbol{X}^{k} - \mathbf{1}}$.
- $(\boldsymbol{X} + \boldsymbol{c})^{\chi} = \boldsymbol{X}^{\chi} + \boldsymbol{c}^{\chi}$ by Freshman Theorem, given prime χ.
- $\boldsymbol{c}^{\chi} = \boldsymbol{c}$ by Fermat's Little Theorem, given prime χ.
- $\boldsymbol{X}^{\chi} + \boldsymbol{c} = (\boldsymbol{X} + \boldsymbol{c})[\boldsymbol{X}^{\chi}]$ by polynomial substitution.
- Both sides equal, hence equivalent under modulo by $\boldsymbol{X}^{k} - \mathbf{1}$.

$\square$

AKS Main Theorem — restated

Theorem (A number is prime iff it satisfies all the AKS checks.)

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

AKS Main Theorem — restated

Theorem (A number is prime iff it satisfies all the AKS checks.)

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

Easy part ($\Longrightarrow$), parameter k can be shown to exist.

If $k \ge n, \forall j.\ 0 < j \land j < n \Rightarrow \gcd(n, j) = 1$?

If $k < n, \forall j.\ 0 < j \land j \le k \Rightarrow \gcd(n, j) = 1$?

$\forall c.\ n \bowtie_{\mathbb{Z}_n} \boldsymbol{X} + \boldsymbol{c}$? $\square$

AKS Main Theorem — restated

Theorem (A number is prime iff it satisfies all the AKS checks.)

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

Easy part ($\Longrightarrow$), parameter k can be shown to exist.

If $k \ge n, \forall j.\ 0 < j \land j < n \Rightarrow \gcd(n, j) = 1$? True for prime n.
If $k < n, \forall j.\ 0 < j \land j \le k \Rightarrow \gcd(n, j) = 1$? Still true for prime n.
$\forall c.\ n \bowtie_{\mathbb{Z}_n} \boldsymbol{X} + \boldsymbol{c}$? By Freshman-Fermat for field $\mathbb{Z}_n$, $\chi(\mathbb{Z}_n) = n$. $\square$

AKS Main Theorem — restated

Hard part ($\Longleftarrow$), parameter k is assumed.

If $k \geq n$, we have $\forall j.\ 0 < j \wedge j < n \Rightarrow \gcd(n, j) = 1$
If $k < n$, we have $\forall j.\ 0 < j \wedge j \leq k \Rightarrow \gcd(n, j) = 1$.

$\square$

Theorem (The AKS Main Theorem in $\mathbb{Z}_n$.)

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

AKS Main Theorem — restated

Hard part ($\Longleftarrow$), parameter k is assumed.

If $k \geq n$, we have $\forall j.\ 0 < j \wedge j < n \Rightarrow \gcd(n, j) = 1 \Rightarrow$ prime n.
If $k < n$, we have $\forall j.\ 0 < j \wedge j \leq k \Rightarrow \gcd(n, j) = 1$.
Apply the following Theorem, then $n = p^e$ for prime p and some e.
Since n is power free, $e = 1$ and $n = p$, giving a prime n. $\square$

Theorem (The AKS Main Theorem in $\mathbb{Z}_n$.)

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

Possible Timeline

Thesis plan:

April, 2015:	AKS Main Theorem ($\surd$)
June, 2016:	Bound on Parameters
June, 2017:	Complexity/Efficiency
December, 2017:	Thesis written (hopefully!)