# Mechanisation of the AKS Algorithm

Hing-Lun Chan

College of Engineering and Computer Science
Australian National University

PhD Review Talk 2014

# Outline

1. Introduction
   - Road Map
   - Current Plan
   - Deterministic Test
2. Deterministic Primality Testing
   - Basic Idea
   - Basic Theorem
   - AKS Theorem

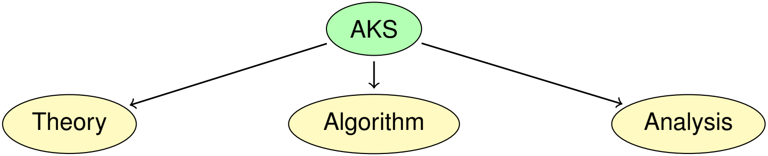
# Mechanisation of AKS Algorithm – Road Map

- Foundation Work:
  - Build Monoid theory in HOL4.
  - Build Group theory from Monoid theory.
  - Build Ring theory using Group and Monoid.
  - Build Field theory using Ring and Group.
  - Build Polynomial theory using Field and Ring.
- Apply to AKS:
  - Code in HOL4: *AKS n* that returns true or false upon input $n$.
  - Prove in HOL4: *AKS n* returns true iff $n$ is prime.
  - Prove in HOL4: number of steps of *AKS n* is bound by $O(\log^k n)$.

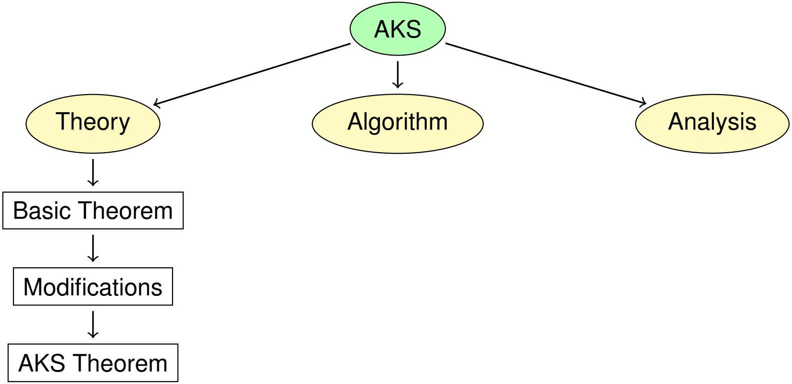
# Mechanisation of AKS Algorithm – Road Map

- Foundation Work:
  - Build Monoid theory in HOL4.($\surd$)
  - Build Group theory from Monoid theory.($\surd$)
  - Build Ring theory using Group and Monoid.($\surd$)
  - Build Field theory using Ring and Group.($\surd$)
  - Build Polynomial theory using Field and Ring.($\surd$)
- Apply to AKS:
  - Code in HOL4: *AKS n* that returns true or false upon input $n$.
  - Prove in HOL4: *AKS n* returns true iff $n$ is prime.
  - Prove in HOL4: number of steps of *AKS n* is bound by $O(\log^k n)$.

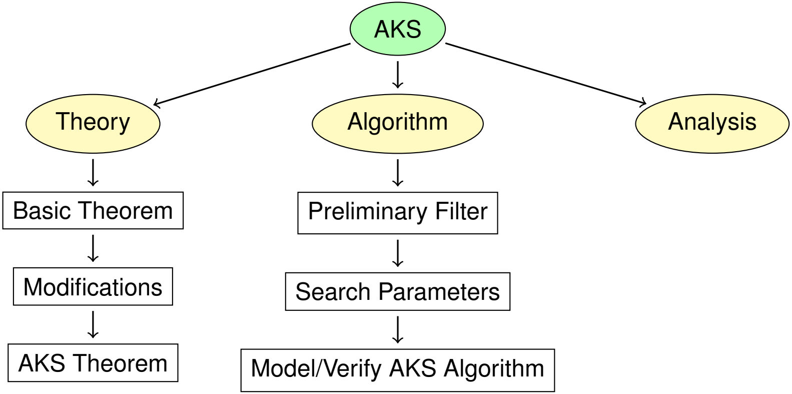
# Current Plan



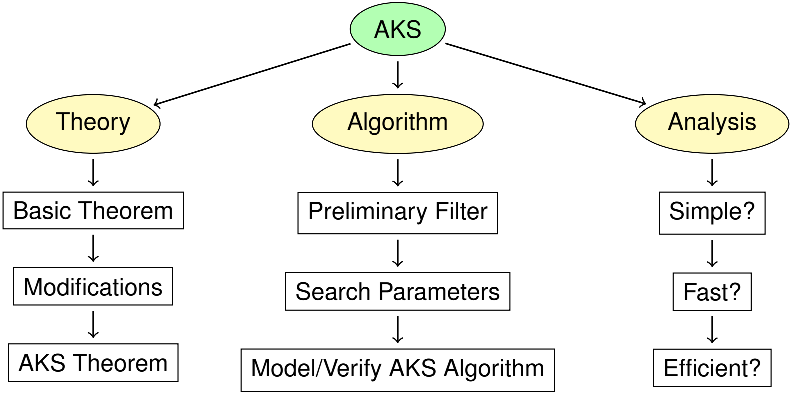
# Current Plan



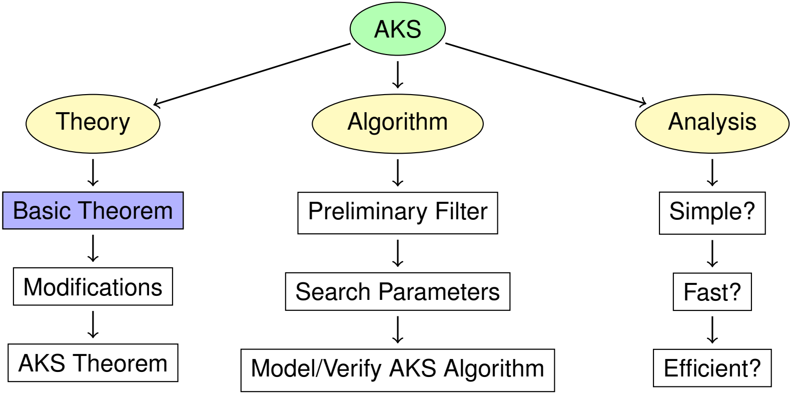
# Current Plan



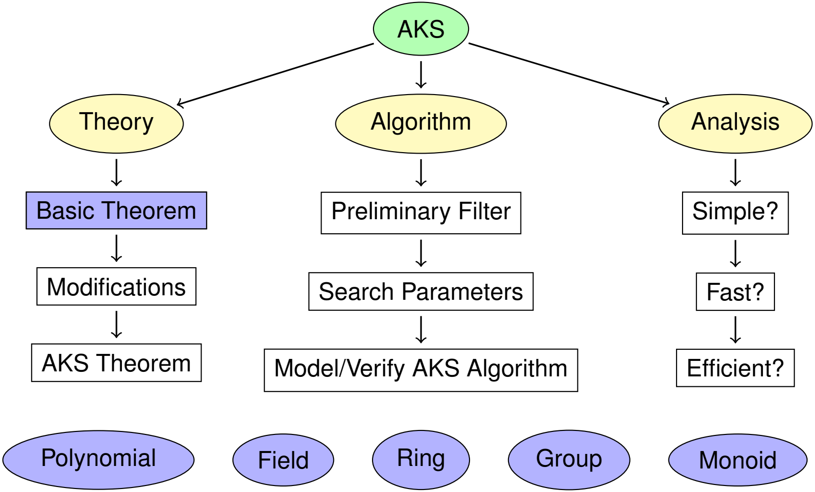
# Current Plan



# Current Plan



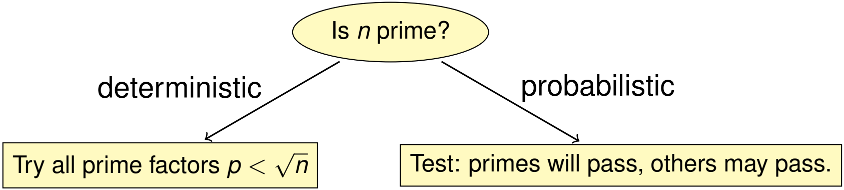
# Current Plan



# Primality Testing

Is $n$ prime?

# Primality Testing



# Primality Testing

Is $n$ prime?

deterministic

Try all prime factors $p < \sqrt{n}$

$\downarrow$

Try 1st prime $\longrightarrow$ no

$\downarrow$

probabilistic

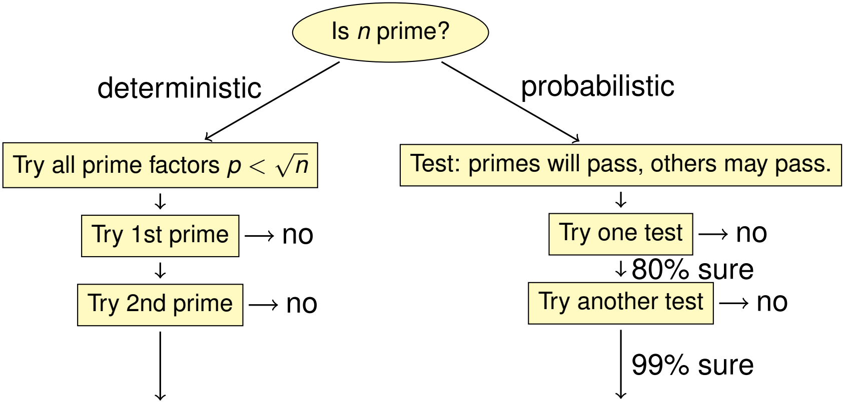
Test: primes will pass, others may pass.

$\downarrow$

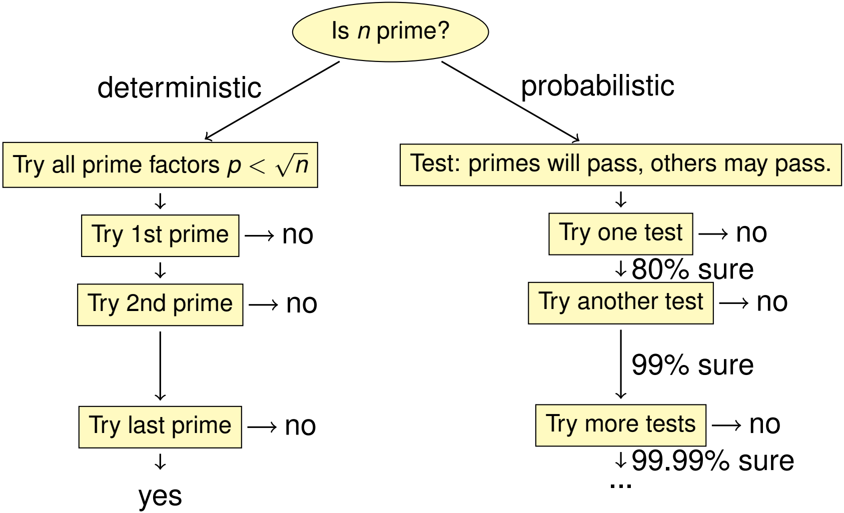
Try one test $\longrightarrow$ no

$\downarrow$ 80% sure

# Primality Testing



# Primality Testing



# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(x+1)^1$ | 1 | 1 | | | | | | |
| $(x+1)^2$ | 1 | 2 | 1 | | | | | |
| $(x+1)^3$ | 1 | 3 | 3 | 1 | | | | |
| $(x+1)^4$ | 1 | 4 | 6 | 4 | 1 | | | |
| $(x+1)^5$ | 1 | 5 | 10 | 10 | 5 | 1 | | |
| $(x+1)^6$ | 1 | 6 | 15 | 20 | 15 | 6 | 1 | |
| $(x+1)^7$ | 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 |

# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

| | |
|---|---|
| $(x+1)^1$ | 1 1 |
| $(x+1)^2$ | 1 2 1 |
| $(x+1)^3$ | 1 3 3 1 |
| $(x+1)^4$ | 1 4 6 4 1 |
| $(x+1)^5$ | 1 5 10 10 5 1 |
| $(x+1)^6$ | 1 6 15 20 15 6 1 |
| $(x+1)^7$ | 1 7 21 35 35 21 7 1 |

- Famous Pascal's triangle, with binomial coefficients $\binom{n}{k}$.

# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(x+1)^1$ | 1 | 1 | | | | | | |
| $(x+1)^2$ | 1 | 2 | 1 | | | | | |
| $(x+1)^3$ | 1 | 3 | 3 | 1 | | | | |
| $(x+1)^4$ | 1 | 4 | 6 | 4 | 1 | | | |
| $(x+1)^5$ | 1 | 5 | 10 | 10 | 5 | 1 | | |
| $(x+1)^6$ | 1 | 6 | 15 | 20 | 15 | 6 | 1 | |
| $(x+1)^7$ | 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 |

- Construction: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \binom{n}{0} = \binom{n}{n} = 1.$

# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(x+1)^1$ | 1 | 1 | | | | | | |
| mod 2 | 1 | 0 | 1 | | | | | |
| $(x+1)^3$ | 1 | 3 | 3 | 1 | | | | |
| $(x+1)^4$ | 1 | 4 | 6 | 4 | 1 | | | |
| $(x+1)^5$ | 1 | 5 | 10 | 10 | 5 | 1 | | |
| $(x+1)^6$ | 1 | 6 | 15 | 20 | 15 | 6 | 1 | |
| $(x+1)^7$ | 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 |

- Construction: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, $\binom{n}{0} = \binom{n}{n} = 1$.

# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(x+1)^1$ | 1 | 1 | | | | | | |
| mod 2 | 1 | 0 | 1 | | | | | |
| mod 3 | 1 | 0 | 0 | 1 | | | | |
| $(x+1)^4$ | 1 | 4 | 6 | 4 | 1 | | | |
| $(x+1)^5$ | 1 | 5 | 10 | 10 | 5 | 1 | | |
| $(x+1)^6$ | 1 | 6 | 15 | 20 | 15 | 6 | 1 | |
| $(x+1)^7$ | 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 |

- Construction: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, $\binom{n}{0} = \binom{n}{n} = 1$.

# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(x+1)^1$ | 1 | 1 | | | | | | |
| mod 2 | 1 | 0 | 1 | | | | | |
| mod 3 | 1 | 0 | 0 | 1 | | | | |
| mod 4 | 1 | 0 | 2 | 0 | 1 | | | |
| mod 5 | 1 | 0 | 0 | 0 | 0 | 1 | | |
| $(x+1)^6$ | 1 | 6 | 15 | 20 | 15 | 6 | 1 | |
| $(x+1)^7$ | 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 |

- Construction: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, $\binom{n}{0} = \binom{n}{n} = 1$.

# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(x+1)^1$ | 1 | 1 | | | | | | |
| mod 2 | 1 | 0 | 1 | | | | | |
| mod 3 | 1 | 0 | 0 | 1 | | | | |
| mod 4 | 1 | 0 | 2 | 0 | 1 | | | |
| mod 5 | 1 | 0 | 0 | 0 | 0 | 1 | | |
| mod 6 | 1 | 0 | 3 | 2 | 3 | 0 | 1 | |
| mod 7 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

- Construction: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \binom{n}{0} = \binom{n}{n} = 1.$

# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(x+1)^1$ | 1 | 1 | | | | | | |
| mod 2 | 1 | 0 | 1 | | | | | |
| mod 3 | 1 | 0 | 0 | 1 | | | | |
| mod 4 | 1 | 0 | 2 | 0 | 1 | | | |
| mod 5 | 1 | 0 | 0 | 0 | 0 | 1 | | |
| mod 6 | 1 | 0 | 3 | 2 | 3 | 0 | 1 | |
| mod 7 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

- Solution: $\binom{n}{k} = \dfrac{n!}{k!\,(n-k)!} = \dfrac{n(n-1)(n-2)\ldots(n-k+1)}{k!}$.

# Primes and Binomial Coefficients

- Prime $n \iff n > 1$ and $n$ divides all its non-unit Binomials.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(x+1)^1$ | 1 | 1 | | | | | | |
| mod 2 | 1 | 0 | 1 | | | | | |
| mod 3 | 1 | 0 | 0 | 1 | | | | |
| mod 4 | 1 | 0 | 2 | 0 | 1 | | | |
| mod 5 | 1 | 0 | 0 | 0 | 0 | 1 | | |
| mod 6 | 1 | 0 | 3 | 2 | 3 | 0 | 1 | |
| mod 7 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

- Theorem: prime $n \Leftrightarrow n > 1$ and $(x+1)^n \equiv x^n + 1 \pmod{n}$.

# Polynomial Identity for Primes

**Theorem**

*Given a number $n$, let $c$ be coprime with $n$; i.e. $gcd(c, n) = 1$.*
*Then prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$.*

# Polynomial Identity for Primes

## Theorem

*Given a number $n$, let $c$ be coprime with $n$; i.e. $gcd(c, n) = 1$.*
*Then prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$.*

If part ($\Rightarrow$):

# Polynomial Identity for Primes

**Theorem**

*Given a number $n$, let $c$ be coprime with $n$; i.e. $gcd(c, n) = 1$.*
*Then prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$.*

If part ($\Rightarrow$):

- "Key" idea: prime $n \Rightarrow n > 1$ and $(x + c)^n \equiv x^n + c^n \mod n$.

# Polynomial Identity for Primes

**Theorem**

*Given a number $n$, let $c$ be coprime with $n$; i.e. $gcd(c, n) = 1$.*
*Then prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$.*

If part ($\Rightarrow$):

- "Key" idea: prime $n \Rightarrow n > 1$ and $(x + c)^n \equiv x^n + c^n \mod n$.
- Fermat's Little Theorem: for any $c$, prime $p \Rightarrow c^p \equiv c \mod p$.

# Polynomial Identity for Primes

## Theorem

*Given a number $n$, let $c$ be coprime with $n$; i.e. $gcd(c, n) = 1$.*
*Then prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$.*

If part ($\Rightarrow$):

- "Key" idea: prime $n \Rightarrow n > 1$ and $(x + c)^n \equiv x^n + c^n \mod n$.
- Fermat's Little Theorem: for any $c$, prime $p \Rightarrow c^p \equiv c \mod p$.

Only-if part ($\Leftarrow$):

# Polynomial Identity for Primes

**Theorem**

*Given a number $n$, let $c$ be coprime with $n$; i.e. $gcd(c, n) = 1$.*
*Then prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \pmod n$.*

If part ($\Rightarrow$):

- "Key" idea: prime $n \Rightarrow n > 1$ and $(x + c)^n \equiv x^n + c^n \pmod n$.
- Fermat's Little Theorem: for any $c$, prime $p \Rightarrow c^p \equiv c \pmod p$.

Only-if part ($\Leftarrow$):

- Equating coefficients, $\binom{n}{k} c^{(n-k)} \equiv 0 \pmod n$, for $0 < k < n$.

# Polynomial Identity for Primes

### Theorem

*Given a number $n$, let $c$ be coprime with $n$; i.e. $gcd(c, n) = 1$.*
*Then prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$.*

If part ($\Rightarrow$):

- "Key" idea: prime $n \Rightarrow n > 1$ and $(x + c)^n \equiv x^n + c^n \mod n$.
- Fermat's Little Theorem: for any $c$, prime $p \Rightarrow c^p \equiv c \mod p$.

Only-if part ($\Leftarrow$):

- Equating coefficients, $\binom{n}{k} c^{(n-k)} \equiv 0 \mod n$, for $0 < k < n$.
- By coprime with $c$, $n$ cannot divide $c^{(n-k)}$,

# Polynomial Identity for Primes

**Theorem**

*Given a number $n$, let $c$ be coprime with $n$; i.e. $gcd(c, n) = 1$.*
*Then prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$.*

If part ($\Rightarrow$):

- "Key" idea: prime $n \Rightarrow n > 1$ and $(x + c)^n \equiv x^n + c^n \mod n$.
- Fermat's Little Theorem: for any $c$, prime $p \Rightarrow c^p \equiv c \mod p$.

Only-if part ($\Leftarrow$):

- Equating coefficients, $\binom{n}{k} c^{(n-k)} \equiv 0 \mod n$, for $0 < k < n$.
- By coprime with $c$, $n$ cannot divide $c^{(n-k)}$, *i.e.* $c^{(n-k)} \not\equiv 0 \mod n$.

# Polynomial Identity for Primes

**Theorem**

*Given a number $n$, let $c$ be coprime with $n$; i.e. $gcd(c, n) = 1$.*
*Then prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$.*

If part ($\Rightarrow$):

- "Key" idea: prime $n \Rightarrow n > 1$ and $(x + c)^n \equiv x^n + c^n \mod n$.
- Fermat's Little Theorem: for any $c$, prime $p \Rightarrow c^p \equiv c \mod p$.

Only-if part ($\Leftarrow$):

- Equating coefficients, $\binom{n}{k} c^{(n-k)} \equiv 0 \mod n$, for $0 < k < n$.
- By coprime with $c$, $n$ cannot divide $c^{(n-k)}$, *i.e.* $c^{(n-k)} \not\equiv 0 \mod n$.
- Therefore, $\binom{n}{k} \equiv 0 \mod n$, for $0 < k < n$, or prime $n$ by "key". $\square$

# Towards AKS

Basic Theorem:
prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$ for any coprime $c$.

# Towards AKS

Basic Theorem:
prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$ for any coprime $c$.

- Good: need to check only one coprime $c$ (*e.g.* $c = 1$).
- Bad: need to compute with polynomials up to degree $n$.

# Towards AKS

Basic Theorem:
prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$ for any coprime $c$.

- Good: need to check only one coprime $c$ (*e.g.* $c = 1$).
- Bad: need to compute with polynomials up to degree $n$.

Modifications (for a practical algorithm):

- Compute with polynomial remainders after division by $(x^r - 1)$.
- Check a range of coprimes: $1 \leq c \leq s$.

# Towards AKS

Basic Theorem:
prime $n \iff n > 1$ and $(x+c)^n \equiv x^n + c \mod n$ for any coprime $c$.

- Good: need to check only one coprime $c$ (*e.g.* $c = 1$).
- Bad: need to compute with polynomials up to degree $n$.

Modifications (for a practical algorithm):

- Compute with polynomial remainders after division by $(x^r - 1)$.
- Check a range of coprimes: $1 \le c \le s$.

## Theorem

*Theorem is broken:*
*Assume* $n > 1$,
*prime* $n \Rightarrow (x+c)^n \equiv x^n + c \mod (n, x^r - 1)$ *for coprimes:* $1 \le c \le s$.
*prime* $n \not\Leftarrow (x+c)^n \equiv x^n + c \mod (n, x^r - 1)$ *for coprimes:* $1 \le c \le s$.
*(polynomial remainders of degree up to* $r$ *have less number of terms!)*

# Towards AKS

Basic Theorem:
prime $n \iff n > 1$ and $(x + c)^n \equiv x^n + c \mod n$ for any coprime $c$.

- Good: need to check only one coprime $c$ (*e.g.* $c = 1$).
- Bad: need to compute with polynomials up to degree $n$.

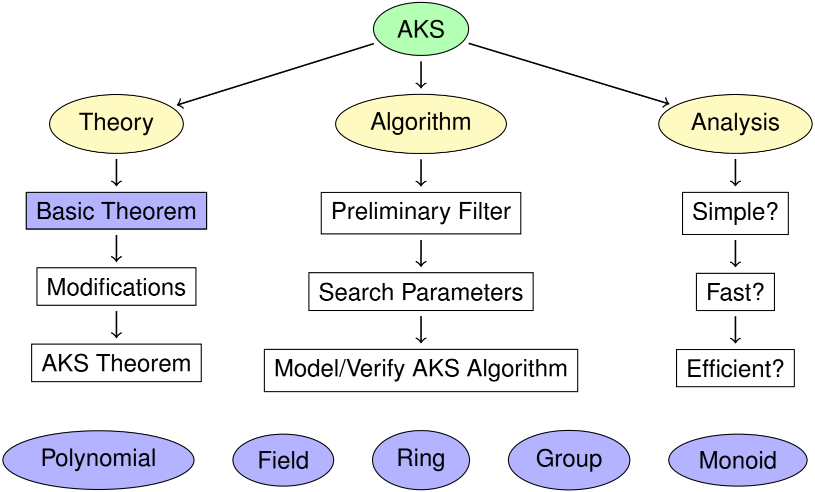
Modifications (for a practical algorithm):

- Compute with polynomial remainders after division by $(x^r - 1)$.
- Check a range of coprimes: $1 \le c \le s$.

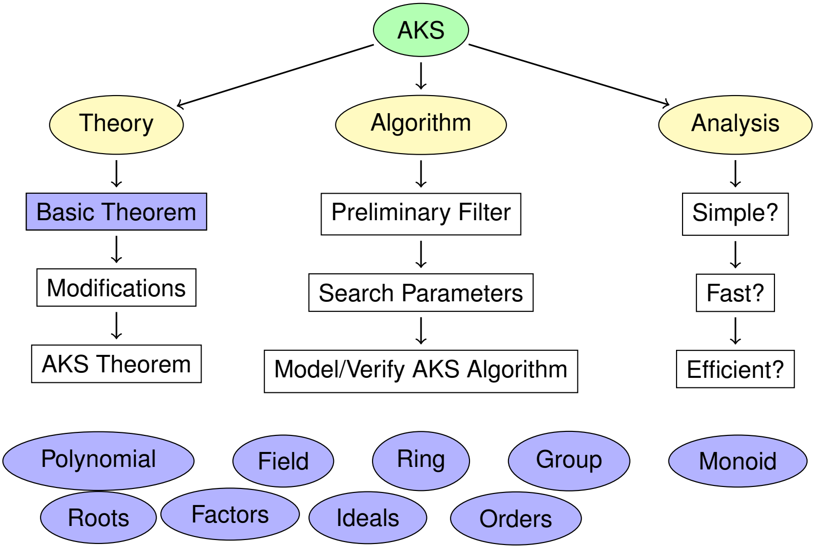
## Theorem

*Theorem found by AKS team:*
*Given* $n > 1$,
*there exists suitable parameters* $r$ *and* $s$ *related to* $n$*, such that:*
$(x + c)^n \equiv x^n + c \mod (n, x^r - 1)$ *for coprimes:* $1 \le c \le s$
$\Rightarrow$ *$n$ is a prime power.*

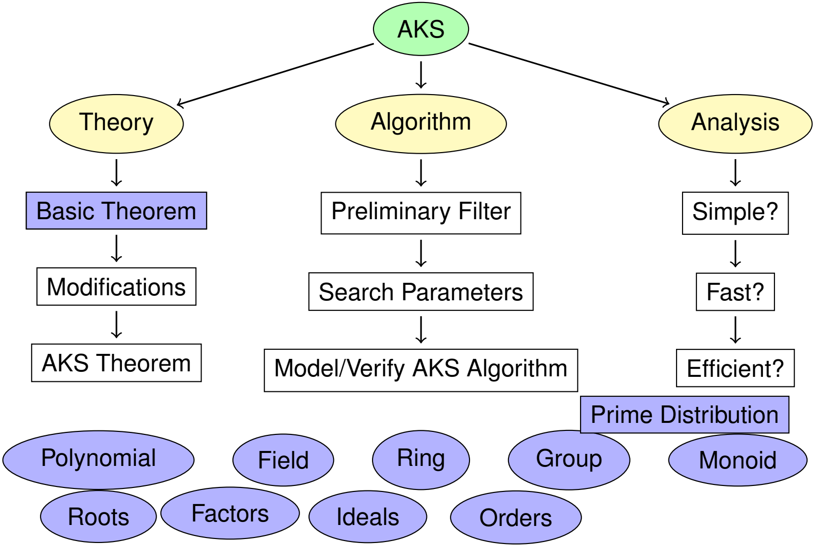
# Road Ahead


AKS
Theory
Algorithm
Analysis
Basic Theorem
Modifications
AKS Theorem
Preliminary Filter
Search Parameters
Model/Verify AKS Algorithm
Simple?
Fast?
Efficient?
Polynomial
Field
Ring
Group
Monoid

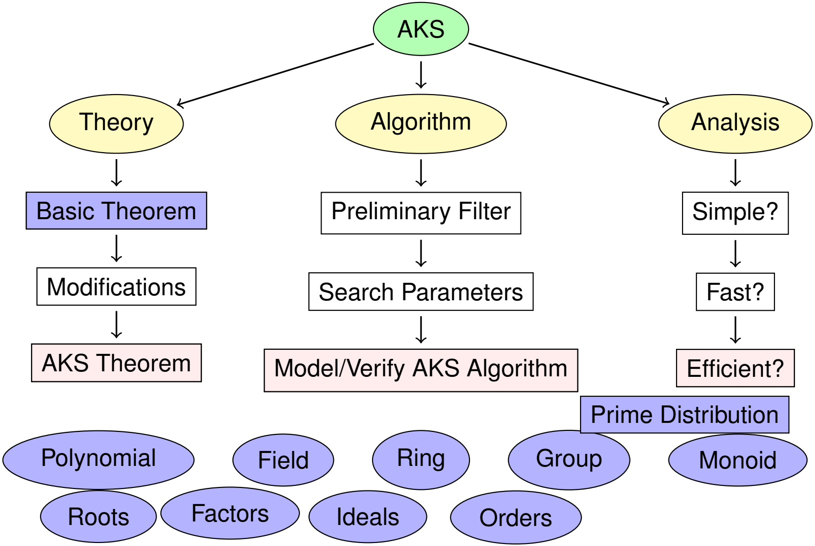
# Road Ahead


AKS
Theory
Algorithm
Analysis
Basic Theorem
Modifications
AKS Theorem
Preliminary Filter
Search Parameters
Model/Verify AKS Algorithm
Simple?
Fast?
Efficient?
Polynomial
Field
Ring
Group
Monoid
Roots
Factors
Ideals
Orders

# Road Ahead


AKS
Theory
Algorithm
Analysis
Basic Theorem
Modifications
AKS Theorem
Preliminary Filter
Search Parameters
Model/Verify AKS Algorithm
Simple?
Fast?
Efficient?
Prime Distribution
Polynomial
Field
Ring
Group
Monoid
Roots
Factors
Ideals
Orders

# Road Ahead


AKS
Theory
Algorithm
Analysis
Basic Theorem
Modifications
AKS Theorem
Preliminary Filter
Search Parameters
Model/Verify AKS Algorithm
Simple?
Fast?
Efficient?
Prime Distribution
Polynomial
Field
Ring
Group
Monoid
Roots
Factors
Ideals
Orders

# Possible Timeline

Thesis plan:

| | |
|---|---|
| **(end of) 2014:** | AKS Theorem |
| **June, 2015:** | Model/Verify AKS Algorithm |
| **June, 2016:** | Complexity/Efficiency |
| **December, 2016:** | Thesis written(!) |

# Possible Timeline

Thesis plan:

| | |
|---|---|
| **(end of) 2014:** | AKS Theorem |
| **June, 2015:** | Model/Verify AKS Algorithm |
| **June, 2016:** | Complexity/Efficiency |
| **December, 2016:** | Thesis written(!) |

My official start-date was 7 April 2012

My latest possible submission date is $\sim$4 years later: 7 March 2016

If necessary, will switch to part-time to extend this deadline

# The Key - Part 1

## Theorem

*Prime n* $\Leftrightarrow n > 1$ *and n divides* $\binom{n}{k}$ *for* $0 < k < n$.

# The Key - Part 1

**Theorem**

*Prime* $n \Leftrightarrow n > 1$ *and* $n$ *divides* $\binom{n}{k}$ *for* $0 < k < n$.

If part ($\Rightarrow$)

# The Key - Part 1

**Theorem**

*Prime $n \Leftrightarrow n > 1$ and $n$ divides $\binom{n}{k}$ for $0 < k < n$.*

If part ($\Rightarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$

# The Key - Part 1

**Theorem**

*Prime n* $\Leftrightarrow n > 1$ *and n divides* $\binom{n}{k}$ *for* $0 < k < n$.

If part ($\Rightarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$
- Let $n = p$ be prime, $p > 1$ is trivial. Replace $n$ by $p$:
  $k!\binom{p}{k} = p(p-1)(p-2)...(p-k+1)$

# The Key - Part 1

## Theorem

*Prime n* $\Leftrightarrow n > 1$ *and n divides* $\binom{n}{k}$ *for* $0 < k < n$.

If part ($\Rightarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$
- Let $n = p$ be prime, $p > 1$ is trivial. Replace $n$ by $p$:
  $$k!\binom{p}{k} = p(p-1)(p-2)...(p-k+1)$$
- Surely, $p$ divides RHS. Thus $p$ also divides LHS.

# The Key - Part 1

## Theorem

*Prime $n \Leftrightarrow n > 1$ and $n$ divides $\binom{n}{k}$ for $0 < k < n$.*

If part ($\Rightarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$
- Let $n = p$ be prime, $p > 1$ is trivial. Replace $n$ by $p$:
  $$k!\binom{p}{k} = p(p-1)(p-2)...(p-k+1)$$
- Surely, $p$ divides RHS. Thus $p$ also divides LHS.
- Since all $k < p$, prime $p$ cannot divide $k!$.

# The Key - Part 1

**Theorem**

*Prime $n \Leftrightarrow n > 1$ and $n$ divides $\binom{n}{k}$ for $0 < k < n$.*

If part ($\Rightarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$
- Let $n = p$ be prime, $p > 1$ is trivial. Replace $n$ by $p$:
  $$k!\binom{p}{k} = p(p-1)(p-2)...(p-k+1)$$
- Surely, $p$ divides RHS. Thus $p$ also divides LHS.
- Since all $k < p$, prime $p$ cannot divide $k!$.
- Therefore, $p$ must divide $\binom{p}{k}$. $\square$

# The Key - Part 2

**Theorem**

*Prime* $n \Leftrightarrow n > 1$ *and* $n$ *divides* $\binom{n}{k}$ *for* $0 < k < n$.

# The Key - Part 2

## Theorem

*Prime* $n \Leftrightarrow n > 1$ *and* $n$ *divides* $\binom{n}{k}$ *for* $0 < k < n$.

Only-if part ($\Leftarrow$)

# The Key - Part 2

## Theorem

*Prime* $n \Leftrightarrow n > 1$ *and* $n$ *divides* $\binom{n}{k}$ *for* $0 < k < n$.

Only-if part ($\Leftarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$

# The Key - Part 2

## Theorem

*Prime n* $\Leftrightarrow n > 1$ *and n divides* $\binom{n}{k}$ *for* $0 < k < n$.

Only-if part ($\Leftarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$
- Assume $n$ is not prime, then it has a prime factor $p$ and $p < n$.
- Let $k = p$, divide by $n$: $\quad p!\frac{\binom{n}{p}}{n} = (n-1)(n-2)...(n-p+1)$

# The Key - Part 2

**Theorem**

*Prime $n \Leftrightarrow n > 1$ and $n$ divides $\binom{n}{k}$ for $0 < k < n$.*

Only-if part ($\Leftarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$
- Assume $n$ is not prime, then it has a prime factor $p$ and $p < n$.
- Let $k = p$, divide by $n$: $\quad p!\frac{\binom{n}{p}}{n} = (n-1)(n-2)...(n-p+1)$
- Note that $\frac{\binom{n}{p}}{n}$ is an integer, since $n$ divides all non-unit binomials.
- Therefore $p$ divides LHS. So $p$ must also divide RHS.

# The Key - Part 2

## Theorem

*Prime $n \Leftrightarrow n > 1$ and $n$ divides $\binom{n}{k}$ for $0 < k < n$.*

Only-if part ($\Leftarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$
- Assume $n$ is not prime, then it has a prime factor $p$ and $p < n$.
- Let $k = p$, divide by $n$: $\quad p!\frac{\binom{n}{p}}{n} = (n-1)(n-2)...(n-p+1)$
- Note that $\frac{\binom{n}{p}}{n}$ is an integer, since $n$ divides all non-unit binomials.
- Therefore $p$ divides LHS. So $p$ must also divide RHS.
- But $n$ is a multiple of $p$; the nearest prior multiple is $(n-p)$.
- Since $p$ is prime, $p$ cannot divide any of $(n-1)$, ..., $(n-p+1)$.

# The Key - Part 2

## Theorem

*Prime n* $\Leftrightarrow n > 1$ *and n divides* $\binom{n}{k}$ *for* $0 < k < n$.

Only-if part ($\Leftarrow$)

- Recall binomial formula: $k!\binom{n}{k} = n(n-1)(n-2)...(n-k+1)$
- Assume $n$ is not prime, then it has a prime factor $p$ and $p < n$.
- Let $k = p$, divide by $n$: $\quad p!\frac{\binom{n}{p}}{n} = (n-1)(n-2)...(n-p+1)$
- Note that $\frac{\binom{n}{p}}{n}$ is an integer, since $n$ divides all non-unit binomials.
- Therefore $p$ divides LHS. So $p$ must also divide RHS.
- But $n$ is a multiple of $p$; the nearest prior multiple is $(n-p)$.
- Since $p$ is prime, $p$ cannot divide any of $(n-1)$, ..., $(n-p+1)$.
- A contradiction — $n$ must be prime! $\square$