Mechanisation of AKS Algorithm

Hing-Lun Chan

College of Engineering and Computer Science
Australian National University

PhD Annual Review Talk 2013

Outline

1. The AKS Algorithm
   - Idea and Theory
   - Algorithm
2. Work Progress
   - Building Theories
   - Achievements
3. Recall
   - AKS Algorithm = a deterministic primality test in polynomial-time

The Idea

- Based on a generalization of Fermat's Little Theorem:

Theorem

If $gcd(a, n) = 1$, $(x + a)^n \equiv x^n + a \mod (n)$ *iff* n *is prime.*

- Put $a = 1$, and compute – but the left side involves n terms, the degree of the polynomial.

The Idea

- Based on a generalization of Fermat's Little Theorem:

Theorem

If $gcd(a, n) = 1$, $(x + a)^n \equiv x^n + a \mod (n)$ *iff* n *is prime.*

- Put $a = 1$, and compute – but the left side involves n terms, the degree of the polynomial.
- To reduce the task to polynomial-time, compute the polynomial remainder of both sides by division of some $x^r - 1$. There would only be r terms, and hopefully degree $r \sim O(log^h n)$ for some h.
- To compensate for lowering of degree, verify more polynomials: $(x + a)^n \equiv x^n + a \mod (x^r - 1, n)$ for $1 \leq a \leq s$, and hopefully limit $s \sim O(log^k n)$ for some k.
- If this works, the overall number of steps is $O(rs \times log^2 n)$.

The Aim

- The AKS team looks for a theorem of this form:

Theorem

Given $n > 1$, there are "suitably chosen" values of r and s such that, if $(x + a)^n \equiv x^n + a \mod (x^r - 1, n)$ for $1 \le a \le s$, then n must be a prime (hopefully).

The Aim

- The AKS team looks for a theorem of this form:

Theorem

Given $n > 1$, there are "suitably chosen" values of r and s such that, if $(x+a)^n \equiv x^n + a \mod (x^r - 1, n)$ for $1 \le a \le s$, then n must be a prime (hopefully).

- Problem: need a prime p to apply the generalized Fermat's Little Theorem, but don't know if n is prime.

The Aim

- The AKS team looks for a theorem of this form:

Theorem

Given $n > 1$, there are "suitably chosen" values of r and s such that, if $(x + a)^n \equiv x^n + a \mod (x^r - 1, n)$ for $1 \leq a \leq s$, then n must be a prime (hopefully).

- Problem: need a prime p to apply the generalized Fermat's Little Theorem, but don't know if n is prime.
- Solution: n must have a prime factor p, so use the prime p to investigate the unknown n.

The Aim

- The AKS team looks for a theorem of this form:

Theorem

Given $n > 1$, there are "suitably chosen" values of r and s such that, if $(x + a)^n \equiv x^n + a \mod (x^r - 1, n)$ for $1 \leq a \leq s$, then n must be a prime (hopefully).

- Problem: need a prime p to apply the generalized Fermat's Little Theorem, but don't know if n is prime.
- Solution: n must have a prime factor p, so use the prime p to investigate the unknown n.
- Bonus: Since p divides n, $x \equiv y \mod n$ implies $x \equiv y \mod p$, the modulo n can be replaced by p during investigation.

The Innovation

- Replacing the modulo n by p:
  $(x+a)^n \equiv x^n + a \mod (x^r - 1, p)$ for $1 \le a \le s$, by given
  $(x+a)^p \equiv x^p + a \mod (x^r - 1, p)$ for $1 \le a \le s$, by prime p
- There is a pattern here, which the AKS team cleverly exploits to squeeze information of n from p:

Theorem

Given $n > 1$, if r and s are chosen wisely, and preliminary checks are done, and $(x+a)^n \equiv x^n + a \mod (x^r - 1, n)$ for $1 \le a \le s$, then $n = p^k$ for some prime p and index k, i.e. n is a prime power.

- Hence if a power check is performed at the start, n must be prime.
- The AKS theory is based on finite fields $\mathbb{F}$, and the ring of polynomials $\mathbb{F}[x]$ with coefficients from such fields.

The Algorithm

```
Input:  integer n > 1.
1.  If (n = a^b for a ∈ N and b > 1), output COMPOSITE.
2.  Find the smallest r such that o_r(n) > log² n.
3.  If 1 < (a,n) < n for some a ≤ r, output COMPOSITE.
4.  If n ≤ r, output PRIME.¹
5.  For a = 1 to ⌊√φ(r) log n⌋ do
          if ((X + a)^n ≠ X^n + a (mod X^r − 1, n)), output COMPOSITE;
6.  Output PRIME;
```

Input: integer $n > 1$.

1. If ($n = a^b$ for $a \in \mathcal{N}$ and $b > 1$), output COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output COMPOSITE.
4. If $n \leq r$, output PRIME.[1]
5. For $a = 1$ to $\lfloor \sqrt{\phi(r)} \log n \rfloor$ do
   if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, output COMPOSITE;
6. Output PRIME;

Algorithm for Primality Testing

- Others have made slight variations of this basic algorithm.
- The only known deteministic polynomial-time primality test.

Road Map

- Foundation Work:
  - ($\surd$) 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.
- 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 $O(\log^k n)$.

Milestones

- ($\surd$) Subgroups and Lagrange Theorem.
- ($\surd$) Units of a Ring form a Group.
- ($\surd$) GF(p) for prime p are indeed Finite Fields.
- ($\surd$) Polynomials $\mathbb{F}[x]$ over a field $\mathbb{F}$ form a Ring.
- ($\surd$) Polynomials $\mathbb{F}[x]$ have no zero divisiors.
- ($\surd$) Polynomials $\mathbb{F}[x]$ have a Division Algorithm.
  i.e. Existence and Uniqueness of quotient and remainder.
- Polynomial Divisibility and Modulo.
- Polynomial Factors and Roots.
- Irreducible Polynomials.
- Polynomial Quotient Ring.

References

- Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, "PRIMES in P" (revised 2005)
- Manindra Agrawal, "Primality Tests Based on Fermat's Little Theorem" (2006)

Questions