An Unconditional, Deterministic Polynomial Time Algorithm for Primarility Testing

Abha Belorkar (A0120126)
Akshay Narayan (A0095686)
Ratul Saha (A0110031)
Pratik Shah (A0107576)
Wang Shengyi (A0120125)
Shweta Shinde (A0109685)
Shruti Tople (A0109720)

Based on

PRIMES is in P

By Manindra Agrawal, Neeraj Kayal and Nitin Saxena

Introduction

Introduction

99654687631365282746 28451

Introduction

9965468763136528274628451

Why are we interested in primes?

Primality Testing

- $\rightarrow$ Input: A positive number n in *binary*
- $\rightarrow$ Prime? Yes or No

Primality Testing

The algorithm we present is

- $\rightarrow$ Unconditional
- $\rightarrow$ Deterministic
- $\rightarrow$ Polynomial Time

Fermat's Little Theorem

For any prime number p, and any number a not divisible by p,

$$a^{p-1} = 1 \pmod{p}$$

- → Efficient to calculate $\ddot\smile$
- → However, many composites n also satisfy this for some a's $\ddot\frown$
- → *Carmichael Numbers*: $561, 1105, 1729, \ldots$

Other Approaches

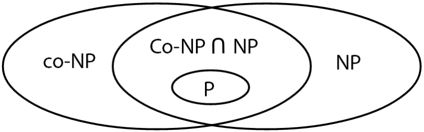
	Uncond	Det	Poly
Miller	×	✓	✓
Miller-Rabin	✓	×	✓
Solovay Strassen	✓	×	✓
APR*	✓	✓	×
Goldwasser & Kilian	×	×	✓

*APR = Adleman, Pomerance & Rumely

Computional Complexity

The problem is in

$$\mathtt{NP} \cap \mathtt{co\text{-}NP}$$



→ Why in $\mathtt{NP}$?

→ Why in $\mathtt{co\text{-}NP}$?

Primes in Times . . .

The New York Times (August 8, 2002) article

→ *Gödel Prize ('06)*

→ *Fulkerson Prize ('06)*

The Idea

The million dollar question

- Is n prime or composite?
- Is there a litmus test? YES!

Child's Binomial Theorem

- $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$ and $gcd(a, n) = 1$
- Then n is prime iff,

$$(x + a)^n = x^n + a \pmod{n}$$

The Litmus Test

Given n and a such that $gcd(a, n) = 1$ should $(x + a)^n = x^n + a \pmod{n}$?

- $\rightarrow$ If n is prime, then yes
- $\rightarrow$ If n is composite, then no

How do we prove it?

- $\rightarrow$ Substitute $(x + a)^n = x^n + \sum_{0<i<n} \binom{n}{i} x^i a^{n-i} + a^n$
- $\rightarrow$ $[(x + a)^n - x^n - a] \pmod{n} = 0$?

The Litmus Test: Proof

$$\rightarrow [x^n + \sum_{0<i<n} \binom{n}{i} x^i a^{n-i} + a^n - x^n - a] \pmod{n}$$

$$\equiv [\sum_{0<i<n} \binom{n}{i} x^i a^{n-i}] \pmod{n} + [a^n - a] \pmod{n}$$

$\rightarrow$ Since $a^n \pmod{n} = a$,

$$\equiv [\sum_{0<i<n} \binom{n}{i} x^i a^{n-i}] \pmod{n}$$

$\Rightarrow$: If n is prime

$$\rightarrow \ [\sum_{0<i<n} \binom{n}{i} x^i a^{n-i}] \pmod{n} = 0$$

$$\equiv \ \forall 0 < i < n, [\tfrac{n!}{i!(n-i)!}] \pmod{n} = 0$$

$\rightarrow$ $n - i < n$ and $i < n$ and n is prime

$\equiv$ No factor of n in denominator

$$\rightarrow \ [\tfrac{(i+1)\dot{(i+2)}\ldots n}{(n-i)!}] \pmod{n}$$

$$\equiv \ [(\tfrac{(i+1)\dot{(i+2)}\ldots(n-1)}{(n-i)!}) * n] \pmod{n}$$

$$\equiv \ 0$$

$\Leftarrow$: If n is composite

- $\rightarrow$ q: prime factor of n
- $\rightarrow$ $\exists k$ such that $q^k \parallel n$

$\Leftarrow$: If n is composite

- q: prime factor of n
- $\exists k$ such that $q^k \parallel n$

- Coefficient of $x^{n-q}a^q$ in $(x+a)^n$

$$\equiv \left[\left(\frac{n!}{(n-q)! \cdot q!}\right) x^{n-q} a^q\right] \pmod{n}$$

$$\equiv \left[\left(\frac{(n-q+1)\ldots(n)}{q!}\right) x^{n-q} a^q\right] \pmod{n}$$

$\Leftarrow$: If n is composite

$$[(\frac{(n-q+1)\dots(n)}{q!})] \pmod{n}$$

- $\rightarrow$ $[(\frac{(n-q+1)\dots(n)}{q!})] \pmod{n} \neq 0$
- $\rightarrow$ The only term q divides in the numerator is n
- $\rightarrow$ The only term q divides in the denominator is q
- $\rightarrow$ q^{k-1} is the highest power of q that divides $\binom{n}{q}$
- $\rightarrow$ $\therefore q^k \nmid \binom{n}{q} \Rightarrow n \nmid \binom{n}{q}$

$\Leftarrow$: If n is composite

$a^q \pmod{n}$

$\rightarrow \ gcd(a, n) = 1$

$\rightarrow \ gcd(a, q^k) = 1$

$\rightarrow \ gcd(a^q, q^k) = 1$

Outline

- → Given n, a and $gcd(a, n) = 1$
- → Calculate $f(x) := (x + a)^n - (x^n + a)$
- → As $f(x) \pmod{n} = 0$
- → $\sum_{0<i<n} \binom{n}{i} X^i a^{n-i}$ - each term should be zero
- → Computation of n coefficients
- → $\Omega(n)$: horribly inefficient!

AKS: The Idea

→ Can we reduce the number of coefficients to be calculated?

$$x^n + \sum_{0<i<n} \binom{n}{i} x^i a^{n-i} + a^n \pmod{n}$$

$$\Downarrow$$

$$x^r + \sum_{0<i<r} \binom{r}{i} x^i a^{n-i} + a^n \pmod{n}$$

AKS: The Idea

- → The algorithm finishes in polynomial time
- → Only r number of calculations
- → For a small r, check if

$$(x+a)^n = x^n + a \pmod{x^r - 1, n}$$

(we refer to this as the AKS Equation)

- → Necessary and Sufficient!

Preliminaries

Group

Integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ under addition forms a *group*, denoted $(\mathbb{Z}, +)$.

- $\rightarrow$ Closure: $a + b \in \mathbb{Z}$
- $\rightarrow$ Associativity: $(a + b) + c = a + (b + c)$
- $\rightarrow$ Identity element: $z + 0 = z$
- $\rightarrow$ Inverse element: $n + (-n) = 0$

$(\mathbb{Z}, +)$ is also an *abelian group* since it satisfies:

- $\rightarrow$ Commutativity: $a + b = b + a$

More Group Examples

For any $n \in \mathbb{N}^+$

- $\rightarrow$ Integers modulo n forms a group under addition modulo n
- $\rightarrow$ Identity element is 0
- $\rightarrow$ Inverse element of x is $(n - x)$ mod n

For $n = 6$, the *abelian* group is $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$$\bar{1} + \bar{2} = \bar{3}$$
$$\bar{3} + \bar{4} = \bar{1}$$
$$\bar{5} + \bar{1} = \bar{0}$$
$$\cdots$$

More Group Examples

For any prime p,

- Integers modulo p is a multiplicative group
- Elements: integers 1 to $p - 1$
- Group operation: multiplication modulo p
- It's an abelian group, too

For example, if $p = 5$, group elements are $1, 2, 3, 4$

More Group Examples

When $p = 5$, the table of inverse elements:

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

It is a cyclic group since the whole group can be generated by 2:

$$2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1$$

Ring

Integers modulo n form a *ring* under modular *add* and *mult*, denoted $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

- $\rightarrow$ Abelian Additive Group: $\mathbb{Z}_n$ is an abelian group under modular addition
- $\rightarrow$ Mult. Closure: $x \cdot y \in \mathbb{Z}_n$
- $\rightarrow$ Mult. Associativity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\rightarrow$ Mult. Identity: $x \cdot \bar{1} = x$
- $\rightarrow$ Distributivity: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

Ring Example: Polynomial Ring

The polynomial ring, $K[x]$, in x over a ring K is the set of polynomials in x, of the form

$$c_m x^m + c_{m-1} x^{m-1} + \cdots + c_2 x^2 + c_1 x + c_0$$

where $c_i \in K$ and $x, x^2, \ldots$ are formal symbols

- $+$: Polynomial addition
- $\times$: Polynomial multiplication

Concretely, all polynomials over ring $\mathbb{Z}_n$ (denoted $\mathbb{Z}_n[x]$) form a polynomial ring

Field

- Intuitively, a field F is a generalization of concept of $\mathbb{R}$:

$$\text{We can do } +, -, \times, \div \text{ in } F$$

- Formally, a field is a ring whose nonzero elements form an abelian group under $\times$
- $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields

Field Example: Prime Field

For any prime p, integers modulo p form a field called *prime field*, denoted F_p

Addition in F_5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication in F_5

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Irreducible Polynomial

- $x^2 - 1$ is reducible over $\mathbb{Z}$ since $x^2 - 1 = (x-1)(x+1)$
- $x^2 - 5$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$ since $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$
- $x^2 + 1$ is irreducible over $\mathbb{Q}$ but reducible over F_2
- In $F_2[x]$, $(x+1)^2 = x^2 + 2x + 1 = x^2 + 1$

Irreducible Polynomial

- $\rightarrow$ If p is prime and $h(x)$ is a polynomial of degree d and irreducible over F_p, then $F_p[x]/(h(x))$ is a finite field of order p^d
- $\rightarrow$ Two fields of order 8 are $F_2[x]/(x^3+x+1)$ and $F_2[x]/(x^3+x^2+1)$

Modular Operations on Polynomials

→ We can calculate $P(x)$ mod $Q(x)$ using polynomial long division:

$$
\begin{array}{rrrrrr}
 & & x^5 + x^3 & & + x & \\
\cline{2-5}
x^2 - 1 \big) & x^7 & & & + 6x & - 7 \\
 & -x^7 + x^5 & & & & \\
\cline{2-3}
 & x^5 & & & & \\
 & -x^5 + x^3 & & & & \\
\cline{2-4}
 & & x^3 & & + 6x & \\
 & & -x^3 & & + x & \\
\cline{3-5}
 & & & & 7x &
\end{array}
$$

Modular Operations on Polynomials

→ So $x^7 + 6x - 7 = 7x - 7 \pmod{x^2 - 1}$

→ $f(x) = g(x) \pmod{h(x), n}$ means
$f(x) = g(x)$ in $\mathbb{Z}_n[x]/(h(x))$

Cyclotomic Polynomial

- → A n^{th} cyclotomic polynomial $\Phi_n(x)$ is the unique irreducible polynomial with integer coefficients
- → Divisor of $x^n - 1$, not a divisor of $x^k - 1$ for any $k < n$

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(x - e^{2i\pi\frac{k}{n}}\right)$$

Cyclotomic Polynomial: Examples

- $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$
- $\Phi_{11}(x) =$
  $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

Order of a modulo r

- Given $\gcd(a, r) = 1$, the order of a modulo r is the smallest number k such that $a^k = 1 \pmod{r}$
- It is denoted as $o_r(a)$

Order of a modulo r

- $\rightarrow$ Why does k exist?
- $\rightarrow$ For a given r, $\{a \mid (a, r) = 1 \land a < r\}$ forms a finite abelian group under multiplication modulo r
- $\rightarrow$ For a specific a, $\exists k_1 < k_2$, such that $a^{k_2} = a^{k_1} \pmod{r}$.
  So, $a^{k_2 - k_1} = 1 \pmod{r}$

Order of a modulo r: Example

$\rightarrow$ For $r = 20$, $a = 7$, $o_{20}(7) = 4$ since

$$
\begin{aligned}
7^2 &= 49 = 9 \pmod{20} \\
7^3 &= 343 = 3 \pmod{20} \\
7^4 &= 2401 = 1 \pmod{20}
\end{aligned}
$$

The Algorithm

The Main Algorithm

Input: integer $n > 1$

(1) Preliminary test

(2) Find a suitable r

(3) Search for non co-prime elements

(4) `if` $n \leq r$, `return` PRIME

(5) `for` $a = 1, 2, \ldots, \lceil \sqrt{r} \log n \rceil$ `do`

(6) `if` $(X - a)^n \neq X^n - a \pmod{X^r - 1, p}$ `then`

`return` COMPOSITE

(7) `return` PRIME

The Process

(1) Preliminary test

If n is perfect power

$\rightarrow$ Given n, if $n = a^b (b > 1)$, n is composite

$\rightarrow$ $b < \log n + 1$

Then for every b, we can find such a using binary search

The Process

(2) Find suitable r

Find the smallest r such that $o_r(n) > (\log n)^2$

$\rightarrow$ Recall, order $o_r(n)$ is smallest j such that $n^j = 1 \pmod r$

`for` $q = 1, 2, \cdots, \lceil (\log n)^5 \rceil$ `do`
 `if` $n^j \neq 1 \pmod q$ `for` $j = 1, 2, \ldots, \lceil (\log n)^2 \rceil$
  $r = q$

(Why $r \leq \lceil (\log n)^5 \rceil$? We shall see later!)

The Process

(3) Search for non co-prime elements

If $\gcd(a, n) > 1$ for some $a \leq r$, COMPOSITE

Use Euclidean algorithm for each a to check if $\gcd(a, n) > 1$
If such an a exists, then n is composite

The Process

(5--6) Main loop

$$
\begin{array}{l}
\texttt{for } a = 1 \texttt{ to } \lceil \sqrt{r} \log n \rceil \texttt{ do} \\
\quad \text{if } (X+a)^n \neq X^n + a \pmod{X^r - 1, n} \texttt{ then} \\
\quad\quad \texttt{return } \text{COMPOSITE}
\end{array}
$$

Use standard mod calculation with fast exponentiation

Putting it all together

Input: integer $n > 1$

(1) `if` $n = a^b$, for $a, b \geq 2$ && $b < \log n + 1$ `then`
 `return` COMPOSITE

(2) choose smallest r such that $o_r(n) > (\log n)^2$

(3) `if` $\exists \, \gcd(a, n) < n$ for some $a < r$
 `return` COMPOSITE

(4) `if` $n \leq r$, `return` PRIME

(5) `for` $a = 1, 2, \ldots, \lceil \sqrt{r} \log n \rceil$ `do`

(6) `if` $(X + a)^n \neq X^n + a \pmod{X^r - 1, p}$ `then`
 `return` COMPOSITE

(7) `return` PRIME

Time Complexity Analysis

Shruti Tople

Arithmetic Computation & $\widetilde{O}$

- $\rightarrow$ If a and b are two positive integers, each with no more than m digits in binary
- $\rightarrow$ $+$ and $-$ take $O(m)$ bit operations
- $\rightarrow$ $\times$ takes $O(m(\log m)^{O(1)})$

We define $\widetilde{O}(m) = O(m(\log m)^{O(1)})$

- $\rightarrow$ For two d degree polynomials with m bit coefficients, multiplication takes $\widetilde{O}(d \cdot m)$

Complexity Analysis

(1) Given n, if $n = a^b (b > 1)$, n is composite

$\rightarrow$ Bound on b: $b < \log n + 1 \Rightarrow O(\log n)$

$\rightarrow$ For every b, find a using binary search $\Rightarrow O(\log n)$

$\rightarrow$ To compute $a^b \Rightarrow \widetilde{O}(\log n)$

Complexity of Step 1: $\widetilde{O}((\log n)^3)$ bit operations

Complexity Analysis

(2) Find the smallest r such that $o_r(n) > (\log n)^2$

$\texttt{for}\ q = 1, 2, \cdots, \lceil (\log n)^5 \rceil\ \texttt{do}$

$\quad \texttt{if}\ n^j \neq 1 \pmod{q}\ \texttt{for}\ j = 1, 2, \cdots, \lceil (\log n)^2 \rceil$

$\quad\quad r = q$

→ First `for` loop $\Rightarrow O(r)$; worst case $O((\log n)^5)$

→ Second `for` loop $\Rightarrow \widetilde{O}((\log n)^2)$

Complexity of Step 2: $\widetilde{O}(r(\log n)^2) = \widetilde{O}((\log n)^7)$

Complexity Analysis

(3) If $\gcd(a, n) > 1$ for some $a \leq r$, n is COMPOSITE

$\rightarrow$ Euclidean algorithm complexity $\Rightarrow O(\log n)$

$\rightarrow$ As $a \leq r$, in worst case need $O(r)$ computation

This can be done in $O(r(\log n)) = O((\log n)^6)$

Complexity Analysis

(5) $\texttt{for}\ a = 1$ to $\lceil \sqrt{r} \log n \rceil$ $\texttt{do}$

(6) $\quad \texttt{if}\ (X+a)^n \neq X^n + a \pmod{X^r - 1, n}$ $\texttt{then}$

$\quad\quad \texttt{return}$ COMPOSITE

We have, a degree r polynomial with $\log n$ bits

$\rightarrow$ Bitwise multiplication $\Rightarrow \widetilde{O}(r(\log n)^2)$

$\rightarrow$ `for` loop runs from 1 to $\sqrt{r} \log n$

$\rightarrow$ Now, the complexity is: $\widetilde{O}(r(\log n)^2 \cdot \sqrt{r} \log n)$

$$= \widetilde{O}(r^{\frac{3}{2}}(\log n)^3) = \widetilde{O}((\log n)^{\frac{21}{2}})$$

Complexity Analysis

Overall complexity

- $\rightarrow$ Step 1: $\widetilde{O}((\log n)^3)$
- $\rightarrow$ Step 2: $\widetilde{O}(r(\log n)^2)$
- $\rightarrow$ Step 3: $O(r(\log n))$
- $\rightarrow$ Final loop: $\widetilde{O}((\log n)^{\frac{21}{2}})$

Complexity of the final loop dominates all others

Hence, overall complexity: $\widetilde{O}((\log n)^{\frac{21}{2}})$

Proof of Correctness

AKS Theorem

For the smallest r such that $o_r(n) > (\log n)^2$

n is prime iff

- $\rightarrow$ n is not a perfect power,
- $\rightarrow$ n does not have any prime factor $\leq r$,
- $\rightarrow$ $(x+a)^n = x^n + a \mod (n, x^r - 1)$ for each integer a, $1 \leq a \leq A = \lceil \sqrt{r} \log n \rceil$

If n is prime

- → If n is prime, steps (1) and (3) can never return COMPOSITE
- → The `for` loop can not return COMPOSITE either
- → Hence the algorithm will output PRIME

We are only left with the other side of the proof!

If the Algorithm Returns PRIME

Proof by contradiction

- → Let's assume n is composite
- → Thus, there exists a prime p such that $p|n$

We assume

- → n is not a perfect power
- → n does not have any prime factor $\leq r$

If the Algorithm Returns PRIME

The master plan:

- $\rightarrow$ We show that there exists a *suitable* r

- $\rightarrow$ We construct a nice group $\mathbb{G}$ assuming $p|n$
- $\rightarrow$ We prove a contradiction on the size of $\mathbb{G}$
  - $\Rightarrow$ There is no such $\mathbb{G}$
- $\rightarrow$ Hence, n is not composite

We assume $\operatorname{lcm}\{1, \cdots, m\} \geq 2^m$ for $m \geq 7$

Existence of a Suitable r

There exists an $r \leq \max\left(3, \lceil (\log n)^5 \rceil\right)$ such that

$$o_r(n) > (\log n)^2$$

- $\rightarrow$ When $n = 2$, $r = 3$. We assume $n > 2$, thus $\lceil (\log n)^5 \rceil > 10$
- $\rightarrow$ Consider $\{r_1, r_2, \cdots, r_t\}$ such that either $o_r(n) \leq (\log n)^2$ or $r_i | n$
- $\rightarrow$ Thus, every r_i divides

$$n \cdot \prod_{i=1}^{\lceil (\log n)^2 \rceil} (n^i - 1) < n^{(\log n)^4} \leq 2^{(\log n)^5}$$

Existence of a Suitable r

But the lcm of the first $\lceil (\log n)^5 \rceil$ numbers is at least $2^{\lceil (\log n)^5 \rceil}$

Thus, $\exists s \leq \lceil (\log n)^5 \rceil$, such that $s \notin \{r_1, \cdots, r_t\}$

- $\rightarrow$ If $\gcd(s, n) = 1$, then $o_s(n) > (\log n)^2$
- $\rightarrow$ If $\gcd(s, n) > 1$, then since $s \nmid n$ and $(s, n) \in \{r_1, \cdots, r_t\}$, $r = \frac{s}{\gcd(s,n)} \notin \{r_1, \cdots, r_t\}$ and so $o_r(n) > (\log n)^2$

Find a Nice Group $\mathbb{G}$

For each integer a, $1 \leq a \leq A$,

→ We know

$$(x+a)^n = x^n + a \pmod{x^r - 1, n}$$

→ $p|n$, hence

$$(x+a)^n = x^n + a \pmod{x^r - 1, p}$$

→ Let $h(x)$ be an irreducible factor of $\Phi_r(x)$ $\pmod{p}$ (i.e. in $(\mathbb{Z}/p\mathbb{Z})[x]$), then

$$(x+a)^n = x^n + a \pmod{h(x), p}$$

Find a Nice Group $\mathbb{G}$

- Given $\mathbb{F} = \mathbb{Z}[x]/(p, h(x))$, non-zero elements of $\mathbb{F}$ form a cyclic group of order $p^m - 1$
- Let H be the multiplicative group modulo $(x^r - 1, p)$ generated by $x, x+1, x+2, \cdots, x+A$
- Let $\mathbb{G}$ be the (multiplicative) subgroup of $\mathbb{F}$ generated by $x, x+1, x+2, \cdots, x+A$
- All the elements of $\mathbb{G}$ are non-zero

Bounds on $|\mathbb{G}|$

$g(x) = \prod_{0 \le a \le A} (x+a)^{e_a} \in H$, then

$$
\begin{aligned}
g(x)^n &= \prod_a ((x+a)^n)^{e_a} \pmod{x^r - 1, p} \\
&= \prod_a (x^n + a)^{e_a} \pmod{x^r - 1, p} \\
&= g(x^n) \pmod{x^r - 1, p}
\end{aligned}
$$

Bounds on $|\mathbb{G}|$

Define S to be the set of positive integers k for which $g(x^k) = g(x)^k \pmod{x^r - 1, p}$ for all $g \in H$

- $p, n \in S$

A few properties of S:

- If $a, b \in S$, $ab \in S$ (Lemma 1)
- If $a, b \in S$ and $a = b \pmod{r}$, then $a = b \pmod{|\mathbb{G}|}$ (Lemma 2)

Upper Bound on $|\mathbb{G}|$

- Let R be the subgroup of $(\mathbb{Z}/r\mathbb{Z})^*$ generated by n and p
- There exist more than $|R|$ integers of the form $n^i p^j$ with distinct $0 \leq i, j \leq \sqrt{|R|}$
- Two of them must be congruent $\pmod{r}$
- Say, $n^i p^j = n^I p^J \pmod{r}$
- $|\mathbb{G}| \leq |n^i p^j - n^I p^J| \leq (np)^{\sqrt{|R|}-1} \leq n^{2\sqrt{|R|}-1}$
- If $n/p \in S$, $|\mathbb{G}| \leq n^{\sqrt{|R|}-1}$

Lower Bound on $|\mathbb{G}|$

- $\rightarrow$ The products $\prod_{a \in T}(x+a)$ give distinct elements of $\mathbb{G}$ for every proper subset T of $\{0, 1, 2, \cdots, \lceil \sqrt{|R|} \log n \rceil\}$
- $\rightarrow$ $|\mathbb{G}| \geq 2^{\lceil \sqrt{|R|} \log n \rceil + 1} - 1 > n^{\sqrt{|R|}} - 1$

The upper and lower bounds conflict, thus making our only assumption wrong

There exists no such $\mathbb{G}$

Hence, n is not composite, completing the proof of correctness

Supplementary Material

Supplementary Material

If $a, b \in S$, $ab \in S$

$\rightarrow$ If $g(x) \in H$, $g(x^b) = g(x)^b \pmod{x^r - 1, p}$

$\rightarrow$ Replacing x by x^a, we get

$g((x^a)^b) = g(x^a)^b \pmod{(x^a)^r - 1, p}$ and

hence $\pmod{x^r - 1, p}$

$\rightarrow$

$$
\begin{aligned}
g(x)^{ab} &= g((x)^a)^b && \ldots (a \in S) \\
&= g((x^a)^b) && \ldots (b \in S) \\
&= g(x^{ab}) \pmod{x^r - 1, p}
\end{aligned}
$$

Supplementary Material

If $a, b \in S$ and $a = b \pmod{r}$, then $a = b \pmod{|\mathbb{G}|}$

$\rightarrow$ $(x^r - 1) | (x^{a-b} - 1)$ and $(x^{a-b} - 1) | (x^a - x^b)$

$\rightarrow$ $(x^a - x^b) | (g(x^a) - g(x^b))$

$\rightarrow$ $(x^r - 1) | (g(x^a) - g(x^b))$

$\rightarrow$ $g(x) \in H$, then $g(x)^a = g(x)^b \pmod{x^r - 1, p}$

$\rightarrow$ If $g(x) \in \mathbb{G}$, $g(x)^{a-b} = 1$ in $\mathbb{F}$

$\rightarrow$ Since $\mathbb{G}$ is cyclic, taking generator g, $|\mathbb{G}|$ divides $a - b$

Statements Not Proved

- $\rightarrow$ $\operatorname{lcm}\{1, \cdots, m\} \geq 2^m$ for $m \geq 7$
- $\rightarrow$ $n/p \in S$
- $\rightarrow$ Two distinct polynomials of the form $\prod_a (x + a)$ of degree $< |R|$ will map to different elements of $\mathbb{G}$

Limitations and Future Work

Usefulness

$$996546876313652827462 8451$$

AKS in SAGE* takes ≈ 70 min for the above number!

*(Software for Algebra and Geometry Experimentation)

Comparison

Practical alternatives

- → APR primality runs in $\widetilde{O}((\log n)^{(\log\log\log n)})$ and yet performs better than AKS
- → Miller-Rabin and other randomized algorithms, which takes average time $\widetilde{O}(\log n)^3$, are used in practice

Agrawal's Conjecture

- → The `for` loop in the algorithm (in step 5) runs $\lceil(\sqrt{r}\log n)\rceil$ times
- → This can be reduced assuming the following conjecture:

If r is a prime number that does not divide n and if $(x+1)^n = x^n + 1 \pmod{x^r - 1, n}$ then either n is prime or $n^2 = 1 \pmod{r}$

Agrawal's Conjecture: Consequences

- $\rightarrow$ We can modify the algorithm to search for an r which does not divide $n^2 - 1$
- $\rightarrow$ Such an r exists in $[2, 4 \log n]$ (product of prime numbers less than x is at least e^x)
- $\rightarrow$ Verifying the congruence takes $\widetilde{O}(r(\log n)^2)$.
- $\rightarrow$ Overall complexity: $\widetilde{O}(\log n)^3$

Agrawal's Conjecture: Progress

- 2003: Lenstra and Pomerance gave a heuristic argument that suggested that the conjecture is false.
- 2005: A group at UT Austin proved that the conjecture is true if $r > n/2$

Other Improvements

Possible improvements in implementation

→ Mapping the polynomial rings onto integer rings

→ Using suitable libraries (NTL better than LiDIA)

Summary

- Efficient to work with Child's Binomial Theorem by reducing its degree by a factor r
- Use this for primality test which runs in polynomial time
- Possible improvements

Take Away

The ground breaking AKS Primality Test is

- $\rightarrow$ unconditional
- $\rightarrow$ deterministic
- $\rightarrow$ polynomial time

References

1. Granville, Andrew. "It is easy to determine whether a given integer is prime." Bulletin of the American Mathematical Society 42.1 (2005): 3-38.
2. Student Talks by S Ramprasad The AKS Primality Test
3. Lang, Serge. Undergraduate algebra. Springer, 2005.

Thank You!
Questions?