The AKS primality test explained

Kuba Perlin

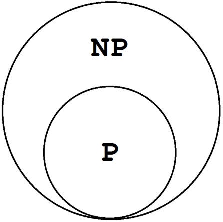
Churchill College

23rd January 2019

The decision problem

PRIMES: Is n prime?

- 1975, Vaughan Pratt: PRIMES $\in$ NP
- 2012, Agrawal, Kayal, Saxena: PRIMES $\in$ P



The original paper

This talk is based on the 2002 paper

PRIMES is in P

by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena.

Also thanks to Dominick Reinhold for his answer

`math.stackexchange.com/a/284467`.

Defining complexity

```
def is_prime(n):
    for i := 2, ..., ⌊√n⌋:
      if i|n:
        return false
    return true
```

Complexity: $\Theta(\sqrt{n})$.

Defining complexity

```
def is_prime(n):
    for i := 2, ..., ⌊√n⌋:
      if i|n:
        return false
    return true
```

Complexity: $\Theta(\sqrt{n})$.

The size of an input n is the number of bits it takes up: $\log n$.

$\Theta(\sqrt{n})$ is $\Theta(e^{\frac{1}{2}\log n})$, which is **exponential** in $\log n$.

Modular algebra refresher

Modulo a number

$$a \equiv b \pmod{n} \iff a = b + kn \iff n | a - b$$

Examples:

- $12 \ = \ 2 \cdot 5 + 2 \ \equiv 2 \pmod{5}$
- $-17 \ = \ -2 \cdot 10 + 3 \ \equiv 3 \pmod{10}$

Polynomials over fields

$\mathbb{Z}_7[X]$ – polynomials of one variable over $\mathbb{Z}_7 = \{0, 1, \ldots, 6\} \pmod 7$

$$
\begin{aligned}
f(X) &= 6X^2 + X + 3 \\
g(X) &= 4X^2 + X + 4 \\
\hline
f(X) + g(X) &= 3X^2 + 2X
\end{aligned}
$$

Modulo a polynomial

$$f(X) = g(X) \pmod{h(X)}$$

$$\iff$$

$$f(X) = g(X) + k(X)h(X)$$

$$\iff$$

$$h(X) | f(X) - g(X)$$

Same principle as before but polynomials instead of integers!

Modulo a polynomial

$$f(X) = g(X) \pmod{h(X)}$$

$$\iff$$

$$f(X) = g(X) + k(X)h(X)$$

$$\iff$$

$$h(X) | f(X) - g(X)$$

Same principle as before but polynomials instead of integers!

- $X^2 + 2 \equiv 3 \pmod{X^2 - 1}$
  because $X^2 + 2 = 1(X^2 - 1) + 3$

Modulo a polynomial

$$f(X) = g(X) \pmod{h(X)}$$

$$\iff$$

$$f(X) = g(X) + k(X)h(X)$$

$$\iff$$

$$h(X) | f(X) - g(X)$$

Same principle as before but polynomials instead of integers!

- $X^2 + 2 \equiv 3 \pmod{X^2 - 1}$
  because $X^2 + 2 = 1(X^2 - 1) + 3$
- $X^3 + X + 1 \equiv 2X + 1 \pmod{X^2 - 1}$
  because $X^3 + X + 1 = X(X^2 - 1) + 2X + 1$

The group generated by n mod r

$$\underline{\gcd(n, r) = 1}$$

$$\langle n \rangle := \{1, n, n^2, n^3, \ldots\} \pmod r$$

The group generated by n mod r

$$\underline{\gcd(n, r) = 1}$$

$$\langle n \rangle := \{1, n, n^2, n^3, \ldots\} \pmod{r}$$

- All the elements are coprime with r.

The group generated by n mod r

$$\underline{\gcd(n, r) = 1}$$

$$\langle n \rangle := \{1, n, n^2, n^3, \ldots\} \pmod{r}$$

- All the elements are coprime with r.
- This is a group, meaning every element has an inverse: $a \cdot a^{-1} = 1$.

The group generated by n mod r

$$\underline{\gcd(n, r) = 1}$$

$$\langle n \rangle := \{1, n, n^2, n^3, \ldots\} \pmod{r}$$

- All the elements are coprime with r.
- This is a group, meaning every element has an inverse: $a \cdot a^{-1} = 1$.
- The smallest e such that $n^e \equiv 1 \pmod{r}$ is the *order* of n mod r. Written as $o_r(n)$.

The group generated by n mod r

$$\underline{\gcd(n, r) = 1}$$

$$\langle n \rangle := \{1, n, n^2, n^3, \dots\} \pmod{r}$$

- All the elements are coprime with r.
- This is a group, meaning every element has an inverse: $a \cdot a^{-1} = 1$.
- The smallest e such that $n^e \equiv 1 \pmod{r}$ is the *order* of n mod r. Written as $o_r(n)$.
  - e.g. $o_7(3) = \mathbf{6}$, because:
    $3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad \underline{3^{\mathbf{6}} = 1} \pmod{7}$

The group generated by n mod r

$$\underline{\gcd(n, r) = 1}$$

$$\langle n \rangle := \{1, n, n^2, n^3, \ldots\} \pmod{r}$$

- All the elements are coprime with r.
- This is a group, meaning every element has an inverse: $a \cdot a^{-1} = 1$.
- The smallest e such that $n^e \equiv 1 \pmod{r}$ is the *order* of n mod r. Written as $o_r(n)$.
  - e.g. $o_7(3) = \mathbf{6}$, because:
    $3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad \underline{3^{\mathbf{6}} = 1} \pmod{7}$
  - **Corollary.** The size of $\langle n \rangle$ is $o_r(n)$. (*We loop after reaching* 1.)

The group generated by n mod r

$$\underline{\gcd(n, r) = 1}$$

$$\langle n \rangle := \{1, n, n^2, n^3, \ldots\} \pmod{r}$$

- All the elements are coprime with r.
- This is a group, meaning every element has an inverse: $a \cdot a^{-1} = 1$.
- The smallest e such that $n^e \equiv 1 \pmod{r}$ is the *order* of n mod r. Written as $o_r(n)$.
  - e.g. $o_7(3) = \mathbf{6}$, because:
    $3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad \underline{3^{\mathbf{6}} = 1} \pmod{7}$
  - **Corollary.** The size of $\langle n \rangle$ is $o_r(n)$. (*We loop after reaching* 1.)
- We can have multiple generators: $\langle n, p \rangle = \{n^i \cdot p^j \mid i, j \geq 0\}$.

Preliminaries

Another inefficient primality test

For any $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$:

$$X^n + a \equiv (X + a)^n \pmod{n} \iff n \text{ is prime}$$

$X^n + a \equiv (X + a)^n$ *is an equality of* **polynomials**, *not numbers!*

Another inefficient primality test – proof sketch

$$X^n + a \equiv X^n + \binom{n}{1} X^{n-1} a^1 + \ldots + \binom{n}{n-1} X^1 a^{n-1} + a^n \pmod{n}$$

Another inefficient primality test – proof sketch

$$X^n + a \equiv X^n + \binom{n}{1} X^{n-1} a^1 + \ldots + \binom{n}{n-1} X^1 a^{n-1} + a^n \pmod{n}$$

If n is prime:

- $a \equiv a^n$ by Fermat's Little Theorem.
- All the $\binom{n}{k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1}$ are 0.

Another inefficient primality test – proof sketch

$$X^n + a \equiv X^n + \binom{n}{1} X^{n-1} a^1 + \ldots + \binom{n}{n-1} X^1 a^{n-1} + a^n \pmod{n}$$

If n is prime:

- $a \equiv a^n$ by Fermat's Little Theorem.
- All the $\binom{n}{k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1}$ are 0.

Otherwise:

- Pick any prime $q | n$. Say that q appears in n 'z-many' times.

Another inefficient primality test – proof sketch

$$X^n + a \equiv X^n + \binom{n}{1} X^{n-1} a^1 + \ldots + \binom{n}{n-1} X^1 a^{n-1} + a^n \pmod{n}$$

If n is prime:

- $a \equiv a^n$ by Fermat's Little Theorem.
- All the $\binom{n}{k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1}$ are 0.

Otherwise:

- Pick any prime $q|n$. Say that q appears in n 'z-many' times.
- $\binom{n}{q} a^q \not\equiv 0$ because $\binom{n}{q}$ contains q '$(z-1)$-many' times and a^q has no qs because of $\gcd(a, n) = 1$.

The idea of AKS

Consider the polynomials modulo $X^r - 1$.

$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, n} \overset{?}{\iff} n \text{ is prime}$$

If r is small, the polynomial equality can be checked quickly!

The idea of AKS

Consider the polynomials modulo $X^r - 1$.

$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, n} \Longleftarrow n \text{ is prime}$$

If r is small, the polynomial equality can be checked quickly!

The idea of AKS

Consider the polynomials modulo $X^r - 1$.

$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, n} \Longleftarrow n \text{ is prime}$$

Careful! If n is composite, the two polynomials would be different, but might give the same residue modulo $X^r - 1$.

If r is small, the polynomial equality can be checked quickly!

The idea of AKS

Consider the polynomials modulo $X^r - 1$.

$$\left.\begin{array}{l} X^n + a_1 \equiv (X + a_1)^n \pmod{X^r - 1, n} \\ X^n + a_2 \equiv (X + a_2)^n \pmod{X^r - 1, n} \\ \dots \\ X^n + a_\ell \equiv (X + a_\ell)^n \pmod{X^r - 1, n} \end{array}\right\} \iff n \text{ is prime}$$

The idea of AKS

Consider the polynomials modulo $X^r - 1$.

$$\left.\begin{array}{l} X^n + a_1 \equiv (X + a_1)^n \pmod{X^r - 1, n} \\ X^n + a_2 \equiv (X + a_2)^n \pmod{X^r - 1, n} \\ \dots \\ X^n + a_\ell \equiv (X + a_\ell)^n \pmod{X^r - 1, n} \end{array}\right\} \iff n \text{ is prime}$$

A *small* number (ℓ) of equations with *low* degree (r) polynomials.

The algorithm

The **efficient** primality test

```
def AKS(n):
```

1. if ($n = a^b$ for $a, b \in \mathbb{N}$ and $b \geq 2$), return COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If some $a \leq r$ is not coprime with n, return COMPOSITE.
4. If $r \geq n$, return PRIME.
5. For $a = 1$ to $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$ do:
   if $X^n + a \not\equiv (X + a)^n \pmod{X^r - 1, n}$, return COMPOSITE.
6. Return PRIME.

Sketching the proof of correctness

def AKS(n):

1. if ($n = a^b$ for $a, b \in \mathbb{N}$ and $b \geq 2$), return COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If some $a \leq r$ is not coprime with n, return COMPOSITE.
4. If $r \geq n$, return PRIME.
5. For $a = 1$ to $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$ do:
   if $X^n + a \not\equiv (X + a)^n \pmod{X^r - 1, n}$, return COMPOSITE.
6. Return PRIME.

Main challenge: show that if Line 6. is reached, then n must be prime.

Sketching the proof of time complexity

```
def AKS(n):
```

1. `if` ($n = a^b$ `for` $a, b \in \mathbb{N}$ `and` $b \geq 2$)`, return COMPOSITE.`
2. `Find the smallest` r `such that` $o_r(n) > \log^2 n$`.`
3. `If some` $a \leq r$ `is not coprime with` n`, return COMPOSITE.`
4. `If` $r \geq n$`, return PRIME.`
5. `For` $a = 1$ `to` $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$ `do:`
   `if` $X^n + a \not\equiv (X + a)^n \pmod{X^r - 1, n}$`, return COMPOSITE.`
6. `Return PRIME.`

Lemma 1. r chosen in `line 2.` satisfies $r \leq \lceil \log^5 n \rceil$.
Corollary. This means that $r \in \text{poly}(\log n)$ and thus the running time of AKS is polynomial in the input size.

Proving $r \leq \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \leq \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \leq B = \lceil \log^5 n \rceil$.

Proving $r \leq \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \leq \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \leq B = \lceil \log^5 n \rceil$. *Proof:*

$$n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1) < n^{\lfloor \log B \rfloor + \frac{1}{2} \log^2 n \cdot (\log^2 n + 1)} \leq n^{\log^4 n} = 2^{\log^5 n} \leq 2^B$$

Proving $r \le \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \le \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \le B = \lceil \log^5 n \rceil$. *Proof:*

$$n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1) < n^{\lfloor \log B \rfloor + \frac{1}{2} \log^2 n \cdot (\log^2 n + 1)} \le n^{\log^4 n} = 2^{\log^5 n} \le 2^B$$

$$L < 2^B \le \operatorname{lcm}\{1, 2, \ldots, B\} \implies L \text{ is not a c.m. of } \{1, 2, \ldots, B\}$$
$$\implies \text{ one of } \{1, 2, \ldots, B\} \text{ does not divide } L$$

Proving $r \leq \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \leq \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \leq B = \lceil \log^5 n \rceil$.
Lemma B. $\gcd(r, n) = 1$ *Proof:*

-
-
-
-

Proving $r \leq \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \leq \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \leq B = \lceil \log^5 n \rceil$.
Lemma B. $\gcd(r, n) = 1$. *Proof:*

- Take all primes p_i that divide both r and n.
  Let $r = \underbrace{\prod p_i^{e_i}}_{a} \cdot \underbrace{\prod q_i^{f_i}}_{b} := ab$.
-
-
-

Proving $r \leq \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \leq \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \leq B = \lceil \log^5 n \rceil$.
Lemma B. $\gcd(r, n) = 1$. *Proof:*

- Take all primes p_i that divide both r and n.
  Let $r = \underbrace{\prod p_i^{e_i}}_{a} \cdot \underbrace{\prod q_i^{f_i}}_{b} := ab$.
- Then $a | n^{\lfloor \log B \rfloor}$ because every $e_i \leq \lfloor \log B \rfloor$.
-
-

Proving $r \leq \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \leq \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \leq B = \lceil \log^5 n \rceil$.
Lemma B. $\gcd(r, n) = 1$. *Proof:*

- Take all primes p_i that divide both r and n.
  Let $r = \underbrace{\prod p_i^{e_i}}_{a} \cdot \underbrace{\prod q_i^{f_i}}_{b} := ab$.
- Then $a | n^{\lfloor \log B \rfloor}$ because every $e_i \leq \lfloor \log B \rfloor$.
- Therefore $b \not| \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$, but b is coprime with $n^{\lfloor \log B \rfloor}$, so $b \not| L$.
-

Proving $r \leq \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \leq \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \leq B = \lceil \log^5 n \rceil$.
Lemma B. $\gcd(r, n) = 1$. *Proof:*

- Take all primes p_i that divide both r and n.
  Let $r = \underbrace{\prod p_i^{e_i}}_{a} \cdot \underbrace{\prod q_i^{f_i}}_{b} := ab$.
- Then $a | n^{\lfloor \log B \rfloor}$ because every $e_i \leq \lfloor \log B \rfloor$.
- Therefore $b \not| \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$, but b is coprime with $n^{\lfloor \log B \rfloor}$, so $b \not| L$.
- Because of minimality of r, we get $b = r$ and so $\gcd(r, n) = \gcd(b, n) = 1$.

Proving $r \leq \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \leq \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \leq B = \lceil \log^5 n \rceil$.
Lemma B. $\gcd(r, n) = 1$.
Lemma C. $o_r(n) > \log^2 n$. *Proof by contradiction:*

Proving $r \leq \lceil \log^5 n \rceil$

Claim. Let r be the smallest number that **does not divide** L (defined below). Then $r \leq \lceil \log^5 n \rceil$ and $o_r(n) > \log^2 n$.

$$\text{Define:} \qquad B := \lceil \log^5 n \rceil, \qquad L := n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Lemma A. $r \leq B = \lceil \log^5 n \rceil$.
Lemma B. $\gcd(r, n) = 1$.
Lemma C. $o_r(n) > \log^2 n$. *Proof by contradiction:*

If $o_r(n) \leq \log^2 n$, then $r \mid n^{o_r(n)} - 1 \mid L$, contradiction.

Proof of correctness

What we're working with

```
def AKS(n):
```

1. `if` ($n = a^b$ `for` $a, b \in \mathbb{N}$ `and` $b \geq 2$), `return COMPOSITE.`
2. `Find the smallest` r `such that` $o_r(n) > \log^2 n$.
3. `If some` $a \leq r$ `is not coprime with` n, `return COMPOSITE.`
4. `If` $r \geq n$, `return PRIME.`

- Our r is coprime with n.

5. `For` $a = 1$ `to` $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$ `do:`
   `if` $X^n + a \not\equiv (X + a)^n \pmod{X^r - 1, n}$, `return COMPOSITE.`

- Our n passed all the ℓ checks above.
- Let's fix a prime divisor p of n, with $p > r$.

6. `Return PRIME.`

What we're going to do now

1. Define a group $\mathcal{G}$ of polynomials.
2.
3.
4.
5.

What we're going to do now

1. Define a group $\mathcal{G}$ of polynomials.
2. Prove that $|\mathcal{G}| \geq \texttt{LowerBound}$.
3.
4.
5.

What we're going to do now

1. Define a group $\mathcal{G}$ of polynomials.
2. Prove that $|\mathcal{G}| \geq$ `LowerBound`.
3. Prove that if $n \neq p^k$, then $|\mathcal{G}| <$ `LowerBound`.
4.
5.

What we're going to do now

1. Define a group $\mathcal{G}$ of polynomials.
2. Prove that $|\mathcal{G}| \geq \texttt{LowerBound}$.
3. Prove that if $n \neq p^k$, then $|\mathcal{G}| < \texttt{LowerBound}$.
4. Deduce that $n = p^k$ for some k.

5.

What we're going to do now

1. Define a group $\mathcal{G}$ of polynomials.
2. Prove that $|\mathcal{G}| \geq$ `LowerBound`.
3. Prove that if $n \neq p^k$, then $|\mathcal{G}| <$ `LowerBound`.
4. Deduce that $n = p^k$ for some k.

But recall `Line 1.` of `AKS`:

`1.  if (`$n = a^b$ `for` $a, b \in \mathbb{N}$ `and` $b \geq 2$`), return COMPOSITE.`

5.

What we're going to do now

1. Define a group $\mathcal{G}$ of polynomials.

2. Prove that $|\mathcal{G}| \geq$ `LowerBound`.

3. Prove that if $n \neq p^k$, then $|\mathcal{G}| <$ `LowerBound`.

4. Deduce that $n = p^k$ for some k.

But recall `Line 1.` of `AKS`:

`1.  if (`$n = a^b$ `for` $a, b \in \mathbb{N}$ `and` $b \geq 2$`), return COMPOSITE.`

5. Therefore $k = 1$... and we get that $n = p^1$ is prime. $\square$

What we're going to do now

1. **Define a group $\mathcal{G}$ of polynomials.**
2. Prove that $|\mathcal{G}| \geq$ `LowerBound`.
3. Prove that if $n \neq p^k$, then $|\mathcal{G}| <$ `LowerBound`.
4. Deduce that $n = p^k$ for some k.

But recall `Line 1.` of `AKS`:

`1.  if (`$n = a^b$ `for` $a, b \in \mathbb{N}$ `and` $b \geq 2$`), return COMPOSITE.`

5. Therefore $k = 1$... and we get that $n = p^1$ is prime. $\square$

Introspective numbers – definition

Because our n got past `line 5.` of `AKS`, we know that:

`For` $a = 1$ `to` $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$:

$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, n}$$

Introspective numbers – definition

Because our n got past `line 5.` of `AKS`, we know that:

`For` $a = 1$ `to` $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$:

$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, n}, \texttt{ so also:}$$
$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, p}$$

Introspective numbers – definition

Because our n got past `line 5.` of `AKS`, we know that:

`For` $a = 1$ `to` $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$:

$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, n}, \text{ so also:}$$
$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, p}$$

Because p is prime, we know that (by the 'inefficient primality test'):

`For` $a = 1$ `to` ℓ:

$$X^p + a \equiv (X + a)^p \pmod{X^r - 1, p}.$$

Introspective numbers – definition

Because our n got past `line 5.` of `AKS`, we know that:

`For` $a = 1$ `to` $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$:

$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, n}, \text{ so also:}$$
$$X^n + a \equiv (X + a)^n \pmod{X^r - 1, p}$$

Because p is prime, we know that (by the 'inefficient primality test'):

`For` $a = 1$ `to` ℓ:

$$X^p + a \equiv (X + a)^p \pmod{X^r - 1, p}.$$

Definition. $m \in \mathbb{N}$ is *introspective* for $f(X) \iff$

$$f(X^m) \equiv [f(X)]^m \pmod{X^r - 1, p}$$

Introspective numbers – definition

Because our n got past `line 5.` of `AKS`, we know that:

`For` $a = 1$ `to` $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$:

$$X^n + a \equiv (X+a)^n \pmod{X^r - 1, n}, \texttt{ so also:}$$
$$X^n + a \equiv (X+a)^n \pmod{X^r - 1, p}$$

Because p is prime, we know that (by the 'inefficient primality test'):

`For` $a = 1$ `to` ℓ:

$$X^p + a \equiv (X+a)^p \pmod{X^r - 1, p}.$$

Definition. $m \in \mathbb{N}$ is *introspective* for $f(X) \iff$

$$f(X^m) \equiv [f(X)]^m \pmod{X^r - 1, p}$$

Corollary. n and p are introspective for $X + a$ (for all $a \in \{0, 1, \ldots, \ell\}$).

Introspective numbers – properties

Recall. $m \in \mathbb{N}$ is introspective for $f(X) \iff$

$$f(X^m) \equiv [f(X)]^m \pmod{X^r - 1, p}$$

Corollary. n and p are introspective for $X + a$ (for all $a \in \{0, 1, \ldots, \ell\}$).

Introspective numbers – properties

Recall. $m \in \mathbb{N}$ is introspective for $f(X) \iff$

$$f(X^m) \equiv [f(X)]^m \pmod{X^r - 1, p}$$

Corollary. n and p are introspective for $X + a$ (for all $a \in \{0, 1, \ldots, \ell\}$).

Property 1. If m and m' are introspective for $f(X)$, then so is $m \cdot m'$.

Introspective numbers – properties

Recall. $m \in \mathbb{N}$ is introspective for $f(X) \iff$

$$f(X^m) \equiv [f(X)]^m \pmod{X^r - 1, p}$$

Corollary. n and p are introspective for $X + a$ (for all $a \in \{0, 1, \ldots, \ell\}$).

Property 1. If m and m' are introspective for $f(X)$, then so is $m \cdot m'$.

Property 2. If m is introspective for $f(X)$ and $g(X)$, then so it is for $f(X) \cdot g(X)$.

The group G_1

Recall. $m \in \mathbb{N}$ is introspective for $f(X) \iff$

$$f(X^m) \equiv [f(X)]^m \pmod{X^r - 1, p}$$

Corollary. n and p are introspective for $X + a$ (for all $a \in \{0, 1, \ldots, \ell\}$).

Property 1. If m and m' are introspective for $f(X)$, then so is $m \cdot m'$.

Property 2. If m is introspective for $f(X)$ and $g(X)$, then so it is for $f(X) \cdot g(X)$.

Definition.

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$ *(a group generated by n and p)*
  All elements of G_1 are introspective for $X + a$ ($a \in \{0, 1, \ldots, \ell\}$).

The group $\mathcal{G}$

Recall.

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$ *(the group generated by n and p)*

Definition.

- $\mathcal{G} := \{\prod_{a=0}^{l} (X + a)^{e_a} \mid e_a \geq 0\} \pmod{\underline{h(X)}, p}$
  (the group generated by $X, X+1, \ldots, X+\ell$)

The group $\mathcal{G}$

Recall.

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$ *(the group generated by n and p)*

Definition.

- $\mathcal{G} := \{ \prod_{a=0}^{l} (X + a)^{e_a} \mid e_a \geq 0\} \pmod{\underline{h(X)}, p}$
  (the group generated by $X, X+1, \ldots, X+\ell$)

Corollary. Every element of G_1 is introspective for every element of $\mathcal{G}$.

The group $\mathcal{G}$

Recall.

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$ *(the group generated by n and p)*

Definition.

- $\mathcal{G} := \{ \prod_{a=0}^{l} (X+a)^{e_a} \mid e_a \geq 0\} \pmod{h(X), p}$
  (the group generated by $X, X+1, \ldots, X+\ell$)

Corollary. Every element of G_1 is introspective for every element of $\mathcal{G}$.

Claim. There exists[1] an irreducible polynomial $h(X)$ that divides $X^r - 1$, does not divide any $X^q - 1$ for $q < r$, and has degree $\deg h > 1$.
For details, see cyclotomic polynomials.

[1]The r^{th} cyclotomic polynomial Q_r over F_p divides $X^r - 1$ and factors into irreducible polynomials of degree $o_r(p)$. A $p|n$ with $o_r(p) > 1$ exists and we assume we have chosen that one. We let $h(X)$ to be any irreducible factor of Q_r.

What we're going to do now

1. Define a group $\mathcal{G}$ of polynomials.
2. **Prove that $|\mathcal{G}| \geq$ `LowerBound`.**
3. Prove that if $n \neq p^k$, then $|\mathcal{G}| <$ `LowerBound`.
4. Deduce that $n = p^k$ for some k.

But recall `Line 1.` of `AKS`:

`1.  if (`$n = a^b$ `for` $a, b \in \mathbb{N}$ `and` $b \geq 2$`), return COMPOSITE.`

5. Therefore $k = 1$... and we get that $n = p^1$ is prime. $\square$

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{l}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

1.
2.

3.
4.

5.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{l}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$ (i.e. distinct $\pmod{h(X)}$). *Proof by contradiction:*

1.

2.

3.

4.

5.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{l}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$ (i.e. distinct $\pmod{h(X)}$). *Proof by contradiction:*

1. Suppose that $f(X) = g(X) \pmod{h(X)}$ (where $\deg f, \deg g < t$).

2.

3.

4.

5.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{l} (X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$ (i.e. distinct $\pmod{h(X)}$). *Proof by contradiction:*

1. Suppose that $f(X) = g(X) \pmod{h(X)}$ (where $\deg f, \deg g < t$).
2. Pick any $m \in G_1$. Because m is introspective for f and g, we have:
$f(X^m) = [f(X)]^m = [g(X)]^m = g(X^m)$ in $\mathcal{G}$.
3.
4.

5.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{l}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$ (i.e. distinct $\pmod{h(X)}$). *Proof by contradiction:*

1. Suppose that $f(X) = g(X) \pmod{h(X)}$ (where $\deg f, \deg g < t$).

2. Pick any $m \in G_1$. Because m is introspective for f and g, we have: $f(X^m) = [f(X)]^m = [g(X)]^m = g(X^m)$ in $\mathcal{G}$.

3. So X^m is a root of $Q(X) := f(X) - g(X)$, where $\deg Q < t$.

4.

5.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{l}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$ (i.e. distinct $\pmod{h(X)}$). *Proof by contradiction:*

1. Suppose that $f(X) = g(X) \pmod{h(X)}$ (where $\deg f, \deg g < t$).

2. Pick any $m \in G_1$. Because m is introspective for f and g, we have: $f(X^m) = [f(X)]^m = [g(X)]^m = g(X^m)$ in $\mathcal{G}$.

3. So X^m is a root of $Q(X) := f(X) - g(X)$, where $\deg Q < t$.

4. But that holds for all $m \in G_1$ and there are t of them.
So some X^{m_1} must equal X^{m_2} in $\mathcal{G}$ for $m_1 \neq m_2$ in G_1.

5.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{l} (X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$ (i.e. distinct $\pmod{h(X)}$). *Proof by contradiction:*

1. Suppose that $f(X) = g(X) \pmod{h(X)}$ (where $\deg f, \deg g < t$).

2. Pick any $m \in G_1$. Because m is introspective for f and g, we have:
$f(X^m) = [f(X)]^m = [g(X)]^m = g(X^m)$ in $\mathcal{G}$.

3. So X^m is a root of $Q(X) := f(X) - g(X)$, where $\deg Q < t$.

4. But that holds for all $m \in G_1$ and there are t of them.
So some X^{m_1} must equal X^{m_2} in $\mathcal{G}$ for $m_1 \neq m_2$ in G_1.

5. Continued on next slide...

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$, cont'd

From last slide:

4. For some $m_1 \neq m_2$ in G_1 we have $X^{m_1} = X^{m_2} \pmod{h(X), p}$.

Getting the contradiction:

i.

ii.

iii.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$, cont'd

From last slide:

4. For some $m_1 \neq m_2$ in G_1 we have $X^{m_1} = X^{m_2} \pmod{h(X), p}$.

Getting the contradiction:

i. $h(X) | X^{m_1} - X^{m_2} = X^{m_2}(X^{m_1 - m_2} - 1)$.

ii.

iii.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$, cont'd

From last slide:

4. For some $m_1 \neq m_2$ in G_1 we have $X^{m_1} = X^{m_2} \pmod{h(X), p}$.

Getting the contradiction:

i. $h(X)|X^{m_1} - X^{m_2} = X^{m_2}(X^{m_1-m_2} - 1)$.

ii. $h(X)$ is an irreducible factor of $X^r - 1$ and does not divide X^{m_2}.

Therefore $h(X)|X^{m_1-m_2} - 1$, i.e. $X^{m_1-m_2} \equiv 1 \pmod{h(X), p}$.

iii.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$, cont'd

From last slide:

4. For some $m_1 \neq m_2$ in G_1 we have $X^{m_1} = X^{m_2} \pmod{h(X), p}$.

Getting the contradiction:

i. $h(X) | X^{m_1} - X^{m_2} = X^{m_2}(X^{m_1 - m_2} - 1)$.

ii. $h(X)$ is an irreducible factor of $X^r - 1$ and does not divide X^{m_2}.

Therefore $h(X) | X^{m_1 - m_2} - 1$, i.e. $X^{m_1 - m_2} \equiv 1 \pmod{h(X), p}$.

iii. Recall that $h(X)$ doesn't divide any $X^q - 1$ for $q < r$.

Look at $X, X^2, X^3, \ldots \pmod{h(X)}$.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$, cont'd

From last slide:

4. For some $m_1 \neq m_2$ in G_1 we have $X^{m_1} = X^{m_2} \pmod{h(X), p}$.

Getting the contradiction:

i. $h(X) | X^{m_1} - X^{m_2} = X^{m_2}(X^{m_1 - m_2} - 1)$.

ii. $h(X)$ is an irreducible factor of $X^r - 1$ and does not divide X^{m_2}.

Therefore $h(X) | X^{m_1 - m_2} - 1$, i.e. $X^{m_1 - m_2} \equiv 1 \pmod{h(X), p}$.

iii. Recall that $h(X)$ doesn't divide any $X^q - 1$ for $q < r$.

Look at $X, X^2, X^3, \dots \pmod{h(X)}$.

The first time we reach 1 is at X^r. The next one is X^{2r}. And so on.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$, cont'd

From last slide:
4. For some $m_1 \neq m_2$ in G_1 we have $X^{m_1} = X^{m_2} \pmod{h(X), p}$.

Getting the contradiction:
i. $h(X)|X^{m_1} - X^{m_2} = X^{m_2}(X^{m_1-m_2} - 1)$.
ii. $h(X)$ is an irreducible factor of $X^r - 1$ and does not divide X^{m_2}.
Therefore $h(X)|X^{m_1-m_2} - 1$, i.e. $X^{m_1-m_2} \equiv 1 \pmod{h(X), p}$.
iii. Recall that $h(X)$ doesn't divide any $X^q - 1$ for $q < r$.
Look at $X, X^2, X^3, \ldots \pmod{h(X)}$.
The first time we reach 1 is at X^r. The next one is X^{2r}. And so on.
Therefore $m_1 - m_2 = kr$ for some $k \in \mathbb{Z}$, i.e. $m_1 \equiv m_2 \pmod{r}$.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$, cont'd

From last slide:

4. For some $m_1 \neq m_2$ in G_1 we have $X^{m_1} = X^{m_2} \pmod{h(X), p}$.

Getting the contradiction:

i. $h(X) | X^{m_1} - X^{m_2} = X^{m_2}(X^{m_1-m_2} - 1)$.

ii. $h(X)$ is an irreducible factor of $X^r - 1$ and does not divide X^{m_2}.

Therefore $h(X) | X^{m_1-m_2} - 1$, i.e. $X^{m_1-m_2} \equiv 1 \pmod{h(X), p}$.

iii. Recall that $h(X)$ doesn't divide any $X^q - 1$ for $q < r$.

Look at $X, X^2, X^3, \ldots \pmod{h(X)}$.

The first time we reach 1 is at X^r. The next one is X^{2r}. And so on.

Therefore $m_1 - m_2 = kr$ for some $k \in \mathbb{Z}$, i.e. $m_1 \equiv m_2 \pmod{r}$.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{\ell}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$.

Claim 2. $X, X+1, \ldots, X+\ell$ are all distinct in $\mathcal{G}$ (i.e. mod p). *Proof:*

1.

2.

3.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{\ell}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$.

Claim 2. $X, X+1, \ldots, X+\ell$ are all distinct in $\mathcal{G}$ (i.e. mod p). *Proof:*
1. We show that $p > \ell$ as follows:
2.
3.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{\ell}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$.

Claim 2. $X, X+1, \ldots, X+\ell$ are all distinct in $\mathcal{G}$ (i.e. mod p). *Proof:*

1. We show that $p > \ell$ as follows:
2. Firstly, $r > o_r(n) > \log^2 n$, so $\sqrt{r} > \log n$. Then:
3.

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{\ell}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$.

Claim 2. $X, X+1, \ldots, X+\ell$ are all distinct in $\mathcal{G}$ (i.e. mod p). *Proof:*

1. We show that $p > \ell$ as follows:
2. Firstly, $r > o_r(n) > \log^2 n$, so $\sqrt{r} > \log n$. Then:
3. $p > r = \sqrt{r}\sqrt{r} > \sqrt{r}\log n > \sqrt{\varphi(r)}\log n \geq \lfloor\sqrt{\varphi(r)}\log n\rfloor = \ell$ $\square$

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{\ell}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$.

Claim 2. $X, X+1, \ldots, X+\ell$ are all distinct in $\mathcal{G}$.

Claim 3. There are $\binom{t+\ell}{t-1} = \binom{(t-1)+(\ell+1)}{t-1}$ different polynomials of degree $< t$ in $\mathcal{G}$. *Proof:*

The lower bound: $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$, where $t := |G_1|$

- $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$
- $\mathcal{G} := \underbrace{\{\prod_{a=0}^{l}(X+a)^{e_a} \mid e_a \geq 0\}}_{P} \pmod{h(X), p}$

Claim 1. Any two polynomials of degree $< t$ in P are distinct in $\mathcal{G}$.

Claim 2. $X, X+1, \ldots, X+\ell$ are all distinct in $\mathcal{G}$.

Claim 3. There are $\binom{t+\ell}{t-1} = \binom{(t-1)+(\ell+1)}{t-1}$ different polynomials of degree $< t$ in $\mathcal{G}$. *Proof:*

$$\circ\,\circ \,|\, \circ \,||\, \circ\,\circ\,\circ$$

"Separate $t-1$ 'degrees' with $\ell+1$ bars, assigning the degrees to polynomials 1, X, $X+1$, $\ldots$, $X+\ell$."

What we're going to do now

1. Define a group $\mathcal{G}$ of polynomials.
2. Prove that $|\mathcal{G}| \geq$ `LowerBound`.
3. **Prove that if $n \neq p^k$, then $|\mathcal{G}| <$ `LowerBound`.**
4. Deduce that $n = p^k$ for some k.

But recall `Line 1.` of `AKS`:

`1.  if (`$n = a^b$` for `$a, b \in \mathbb{N}$` and `$b \geq 2$`), return COMPOSITE.`

5. Therefore $k = 1$... and we get that $n = p^1$ is prime. $\square$

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}}$, where $t := |G_1|$

Recall: $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$

$$\texttt{temp} := \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \right\}$$

1.

2.

3.

4.

5.

6.

7.

8.

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}}$, where $t := |G_1|$

Recall: $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$

$$\texttt{temp} := \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \right\}$$

1. This set has $(\lfloor \sqrt{t} \rfloor + 1)^2 > t = |G_1|$ distinct elements.
2.
3.
4.
5.
6.
7.

8.

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}}$, where $t := |G_1|$

Recall: $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$

$$\texttt{temp} := \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \right\}$$

1. This set has $(\lfloor \sqrt{t} \rfloor + 1)^2 > t = |G_1|$ distinct elements.
2. Consider their remainders mod r. All of them belong in G_1.
3.
4.
5.
6.
7.

8.

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}}$, where $t := |G_1|$

Recall: $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$

$$\texttt{temp} := \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor\sqrt{t}\rfloor \right\}$$

1. This set has $(\lfloor\sqrt{t}\rfloor + 1)^2 > t = |G_1|$ distinct elements.
2. Consider their remainders mod r. All of them belong in G_1.
3. Therefore some $m_1 > m_2 \in \texttt{temp}$ are equal mod r.
4.
5.
6.
7.

8.

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}}$, where $t := |G_1|$

Recall: $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$

$$\mathtt{temp} := \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \right\}$$

1. This set has $(\lfloor \sqrt{t} \rfloor + 1)^2 > t = |G_1|$ distinct elements.
2. Consider their remainders mod r. All of them belong in G_1.
3. Therefore some $m_1 > m_2 \in \mathtt{temp}$ are equal mod r.
4. Then $X^{m_1} = X^{m_2 + kr} = X^{m_2} \cdot (X^r)^k = X^{m_2} \pmod{X^r - 1}$.
5.
6.
7.
8.

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}}$, where $t := |G_1|$

Recall: $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod{r}$

$$\texttt{temp} := \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor\sqrt{t}\rfloor \right\}$$

1. This set has $(\lfloor\sqrt{t}\rfloor + 1)^2 > t = |G_1|$ distinct elements.
2. Consider their remainders mod r. All of them belong in G_1.
3. Therefore some $m_1 > m_2 \in \texttt{temp}$ are equal mod r.
4. Then $X^{m_1} = X^{m_2+kr} = X^{m_2} \cdot (X^r)^k = X^{m_2} \pmod{X^r - 1}$.
5. Pick an arbitrary $f(X) \in \mathcal{G}$. Recall: m_1, m_2 are introspective for $f(X)$.
6.
7.

8.

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}}$, where $t := |G_1|$

Recall: $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$

$$\texttt{temp} := \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \right\}$$

1. This set has $(\lfloor \sqrt{t} \rfloor + 1)^2 > t = |G_1|$ distinct elements.
2. Consider their remainders mod r. All of them belong in G_1.
3. Therefore some $m_1 > m_2 \in \texttt{temp}$ are equal mod r.
4. Then $X^{m_1} = X^{m_2+kr} = X^{m_2} \cdot (X^r)^k = X^{m_2} \pmod{X^r - 1}$.
5. Pick an arbitrary $f(X) \in \mathcal{G}$. Recall: m_1, m_2 are introspective for $f(X)$.
6. Therefore $[f(X)]^{m_1} = f(X^{m_1}) = f(X^{m_2}) = [f(X)]^{m_2}$.
7.

8.

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}}$, where $t := |G_1|$

Recall: $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$

$$\texttt{temp} := \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \right\}$$

1. This set has $(\lfloor \sqrt{t} \rfloor + 1)^2 > t = |G_1|$ distinct elements.
2. Consider their remainders mod r. All of them belong in G_1.
3. Therefore some $m_1 > m_2 \in \texttt{temp}$ are equal mod r.
4. Then $X^{m_1} = X^{m_2 + kr} = X^{m_2} \cdot (X^r)^k = X^{m_2} \pmod{X^r - 1}$.
5. Pick an arbitrary $f(X) \in \mathcal{G}$. Recall: m_1, m_2 are introspective for $f(X)$.
6. Therefore $[f(X)]^{m_1} = f(X^{m_1}) = f(X^{m_2}) = [f(X)]^{m_2}$.
7. $f(X)$ is a root of $Q(Y) = Y^{m_1} - Y^{m_2}$. But that holds for any $f(X) \in \mathcal{G}$, so $|\mathcal{G}| \leq \deg Q$.

8.

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}}$, where $t := |G_1|$

Recall: $G_1 := \{n^i \cdot p^j \mid i, j \geq 0\} \pmod r$

$$\texttt{temp} := \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \right\}$$

1. This set has $(\lfloor \sqrt{t} \rfloor + 1)^2 > t = |G_1|$ distinct elements.
2. Consider their remainders mod r. All of them belong in G_1.
3. Therefore some $m_1 > m_2 \in \texttt{temp}$ are equal mod r.
4. Then $X^{m_1} = X^{m_2 + kr} = X^{m_2} \cdot (X^r)^k = X^{m_2} \pmod{X^r - 1}$.
5. Pick an arbitrary $f(X) \in \mathcal{G}$. Recall: m_1, m_2 are introspective for $f(X)$.
6. Therefore $[f(X)]^{m_1} = f(X^{m_1}) = f(X^{m_2}) = [f(X)]^{m_2}$.
7. $f(X)$ is a root of $Q(Y) = Y^{m_1} - Y^{m_2}$. But that holds for any $f(X) \in \mathcal{G}$, so $|\mathcal{G}| \leq \deg Q$.
8. $|\mathcal{G}| \leq \deg Q = m_1 \leq \max(\texttt{temp}) = \left(\frac{n}{p}\right)^{\lfloor \sqrt{t} \rfloor} \cdot p^{\lfloor \sqrt{t} \rfloor} = n^{\lfloor \sqrt{t} \rfloor} \leq n^{\sqrt{t}}$.

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}} < \binom{t+\ell}{t-1}$

$$n^{\sqrt{t}} = 2^{\sqrt{t}\log n} \leq 2^{\lfloor \sqrt{t}\log n \rfloor + 1}$$

[*because* $\sqrt{t}\log n \leq \lfloor \sqrt{t}\log n \rfloor + 1$]

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}} < \binom{t+\ell}{t-1}$

$$
\begin{aligned}
n^{\sqrt{t}} = 2^{\sqrt{t}\log n} &\leq 2^{\lfloor \sqrt{t}\log n \rfloor + 1} \\
&< \binom{2\lfloor \sqrt{t}\log n \rfloor + 1}{\lfloor \sqrt{t}\log n \rfloor}
\end{aligned}
$$

[*because* $\binom{2x+1}{x} > 2^{x+1}$ *for* $x > 1$]

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}} < \binom{t+\ell}{t-1}$

$$
\begin{aligned}
n^{\sqrt{t}} = 2^{\sqrt{t}\log n} &\leq 2^{\lfloor \sqrt{t}\log n \rfloor + 1} \\
&< \binom{2\lfloor \sqrt{t}\log n \rfloor + 1}{\lfloor \sqrt{t}\log n \rfloor} \\
&\leq \binom{\ell + \lfloor \sqrt{t}\log n \rfloor + 1}{\ell} \\
&= \binom{\ell + \lfloor \sqrt{t}\log n \rfloor + 1}{\lfloor \sqrt{t}\log n \rfloor}
\end{aligned}
$$

[*because* $\binom{x}{y} \leq \binom{x+a}{y+a}$ *and* $\lfloor \sqrt{t}\log n \rfloor \leq \ell$]

[*which holds because* $\ell = \lfloor \sqrt{\varphi(r)}\log n \rfloor$ *and* $t = |G_1| \leq \varphi(r)$]

The upper bound: $n \neq p^k \implies |\mathcal{G}| \leq n^{\sqrt{t}} < \binom{t+\ell}{t-1}$

$$
\begin{aligned}
n^{\sqrt{t}} = 2^{\sqrt{t}\log n} &\leq 2^{\lfloor \sqrt{t}\log n \rfloor + 1} \\
&< \binom{2\lfloor \sqrt{t}\log n \rfloor + 1}{\lfloor \sqrt{t}\log n \rfloor} \\
&\leq \binom{\ell + \lfloor \sqrt{t}\log n \rfloor + 1}{\ell} \\
&= \binom{\ell + \lfloor \sqrt{t}\log n \rfloor + 1}{\lfloor \sqrt{t}\log n \rfloor} \\
&\leq \binom{\ell + (t-1) + 1}{t-1} = \binom{t+\ell}{t-1}
\end{aligned}
$$

[*because* $\binom{x}{y} \leq \binom{x+a}{y+a}$ *and* $\lfloor \sqrt{t}\log n \rfloor \leq t-1 \iff t > \log^2 n$]
[*which holds because* $t = |G_1| = |\langle n, p\rangle| \geq |\langle n \rangle| = o_r(n) > \log^2 n$]

What we've done now

1. Define a group $\mathcal{G}$ of polynomials.
2. Prove that $|\mathcal{G}| \geq$ `LowerBound`.
3. Prove that if $n \neq p^k$, then $|\mathcal{G}| <$ `LowerBound`.
4. Deduce that $n = p^k$ for some k.

But recall `Line 1.` of `AKS`:

`1.  if (`$n = a^b$` for `$a, b \in \mathbb{N}$` and `$b \geq 2$`), return COMPOSITE.`

5. Therefore $k = 1$... and we get that $n = p^1$ is prime. $\square$

Summary of the proof

1. The inefficient primality test.
2.
3.

Summary of the proof

1. The inefficient primality test.
2. Remove the inefficiency but lose correctness.
3.

Summary of the proof

1. The inefficient primality test.
2. Remove the inefficiency but lose correctness.
3. Restore the correctness by repeating the test ℓ times.
   Prove that only prime numbers pass the repeated test:

Summary of the proof

1. The inefficient primality test.
2. Remove the inefficiency but lose correctness.
3. Restore the correctness by repeating the test ℓ times.
   Prove that only prime numbers pass the repeated test:

...

Summary of the proof

...

4. Identify **the introspective property** of n and p w.r.t. $X + a$ polynomials.

5.

6.

7.

8.

9.

Summary of the proof

...

4. Identify **the introspective property** of n and p w.r.t. $X + a$ polynomials.

5. Prove the **multiplicative-closure properties** of introspectiveness.

6.

7.

8.

9.

Summary of the proof

...

4. Identify **the introspective property** of n and p w.r.t. $X + a$ polynomials.

5. Prove the **multiplicative-closure properties** of introspectiveness.

6. **Define G_1 and $\mathcal{G}$** based directly on step **4**.

7.

8.

9.

Summary of the proof

...

4. Identify **the introspective property** of n and p w.r.t. $X + a$ polynomials.

5. Prove the **multiplicative-closure properties** of introspectiveness.

6. **Define G_1 and $\mathcal{G}$** based directly on step **4**.

7. Prove that $\mathcal{G}$ **must have many elements** by examining polynomials X^m and referring to introspectiveness between G_1 and $\mathcal{G}$.

8.

9.

Summary of the proof

...

4. Identify **the introspective property** of n and p w.r.t. $X + a$ polynomials.

5. Prove the **multiplicative-closure properties** of introspectiveness.

6. **Define** G_1 **and** $\mathcal{G}$ based directly on step **4**.

7. Prove that $\mathcal{G}$ **must have many elements** by examining polynomials X^m and referring to introspectiveness between G_1 and $\mathcal{G}$.

8. Prove that, if $n \neq p^k$, then $\mathcal{G}$ **can't have too many elements** by examining polynomials X^m and referring to introspectiveness between G_1 and $\mathcal{G}$.

9.

Summary of the proof

...

4. Identify **the introspective property** of n and p w.r.t. $X + a$ polynomials.

5. Prove the **multiplicative-closure properties** of introspectiveness.

6. **Define** G_1 **and** $\mathcal{G}$ based directly on step **4**.

7. Prove that $\mathcal{G}$ **must have many elements** by examining polynomials X^m and referring to introspectiveness between G_1 and $\mathcal{G}$.

8. Prove that, if $n \neq p^k$, then $\mathcal{G}$ **can't have too many elements** by examining polynomials X^m and referring to introspectiveness between G_1 and $\mathcal{G}$.

9. The required properties of r and l **emerge from the proof**.

Lessons learned

1.
2.
3.

Lessons learned

1. The *break and repair* pattern.
2.
3.

Lessons learned

1. The *break and repair* pattern.
2. Groundbreaking algorithms can emerge directly from pure mathematics.
3.

Lessons learned

1. The *break and repair* pattern.
2. Groundbreaking algorithms can emerge directly from pure mathematics.
3. Problems that went unsolved for decades can have elementary solutions.

Acknowledgements

Thanks to the mentor of this talk – **Matthew Ireland**,
and all others involved in the organization of this event.

Lessons learned

1. The *break and repair* pattern.
2. Groundbreaking algorithms can emerge directly from pure mathematics.
3. Problems that went unsolved for decades can have elementary solutions.