PRIMES is in P

Arka Das

November 2022

Prime Numbers

Definition 1

A natural number $n > 1$ is called prime if the only divisors of n are 1 and n. A natural number $n > 1$ that is not a prime number is called composite.

Prime Numbers

Definition 1

A natural number $n > 1$ is called prime if the only divisors of n are 1 and n. A natural number $n > 1$ that is not a prime number is called composite.

For example, 2, 3, 5, 7, 11 are first few prime numbers.

Prime Numbers

Definition 1

A natural number $n > 1$ is called prime if the only divisors of n are 1 and n. A natural number $n > 1$ that is not a prime number is called composite.

For example, 2, 3, 5, 7, 11 are first few prime numbers.
n is a composite number if and only if n has a divisor d such that $1 < d < n$.

Prime Numbers

Definition 1

A natural number $n > 1$ is called prime if the only divisors of n are 1 and n. A natural number $n > 1$ that is not a prime number is called composite.

For example, 2, 3, 5, 7, 11 are first few prime numbers.
n is a composite number if and only if n has a divisor d such that $1 < d < n$.
For example, 4 is a compositive number as $1 < 2 < 4$ and $2|4$.

Prime Numbers

Definition 1

A natural number $n > 1$ is called prime if the only divisors of n are 1 and n. A natural number $n > 1$ that is not a prime number is called composite.

For example, 2, 3, 5, 7, 11 are first few prime numbers.
n is a composite number if and only if n has a divisor d such that $1 < d < n$.
For example, 4 is a compositive number as $1 < 2 < 4$ and $2|4$.

Theorem 1 (Fundamental Theorem of Arithmetic)

Every natural number $n > 1$ is either a prime or a product of prime numbers in a unique way (up to rearrangement).

Let PRIMES $= \{n\colon\ n$ is prime$\}$ be the set of prime numbers.

Checking if $n \in$ PRIMES

We want to check if a natural number n is prime, *ie*, if $n \in$ PRIMES.

Checking if $n \in$ PRIMES

We want to check if a natural number n is prime, *ie*, if $n \in$ PRIMES.

Why can't we just list all the prime numbers and check if n belongs to that list or not?

Checking if $n \in$ PRIMES

We want to check if a natural number n is prime, *ie*, if $n \in$ PRIMES.

Why can't we just list all the prime numbers and check if n belongs to that list or not?

There are infinitely many prime numbers!

Checking if $n \in$ PRIMES

We want to check if a natural number n is prime, *ie*, if $n \in$ PRIMES.
Why can't we just list all the prime numbers and check if n belongs to that list or not?
There are infinitely many prime numbers!

Proof (due to Euclid).

Suppose not. Then there are finitely many primes $p_1, p_2, ..., p_k$. Consider the number $N = p_1 p_2 ... p_k + 1$. It is not divisible by any prime. So, it is a prime number by the Fundamental Theorem of Arithmetic. Now, $N \geqslant p_i + 1$ for any i with $1 \leqslant i \leqslant k$ So, $N \neq p_i$ for $1 \leqslant i \leqslant k$. But according to our assumption, $p_1, p_2, ..., p_k$ are the only primes. Contradiction!

An Inefficient Algorithm to Check Primality

One can try to check primality right from its definition.

An Inefficient Algorithm to Check Primality

One can try to check primality right from its definition. Given a number $n > 2$, check if m divides n for any $2 \leqslant m \leqslant n - 1$.

An Inefficient Algorithm to Check Primality

One can try to check primality right from its definition.
Given a number $n > 2$, check if m divides n for any $2 \leqslant m \leqslant n - 1$.
It is sufficient to check for $m \leqslant \sqrt{n}$ only.

An Inefficient Algorithm to Check Primality

One can try to check primality right from its definition.
Given a number $n > 2$, check if m divides n for any $2 \leqslant m \leqslant n-1$.
It is sufficient to check for $m \leqslant \sqrt{n}$ only.

Proof.

n is composite if and only if it has a divisor d with $1 < d < n$. Then n/d is also a divisor of n with $1 < \frac{n}{d} < n$. Both d and $\frac{n}{d}$ cannot be $> \sqrt{n}$ (otherwise $n = d \cdot \frac{n}{d} > (\sqrt{n})^2 = n$, a contradiction!). So, n is composite if and only if it has a divisor d with $1 < d \leqslant \sqrt{n}$. □

Still not a good test. We want some algorithm that runs in time polynomial in $\log(n)$.

What is a Group?

Definition 2

A group G is a set together with a binary operation $* : G \times G \to G$ such that

What is a Group?

Definition 2

A group G is a set together with a binary operation $* : G \times G \to G$ such that

(i) for $a, b \in G$, $a * b \in G$

What is a Group?

Definition 2

A group G is a set together with a binary operation $* : G \times G \to G$ such that
(i) for $a, b \in G$, $a * b \in G$
(ii) there is an element $e \in G$ such that $a * e = e * a = a$ for any $a \in G$

What is a Group?

Definition 2

A group G is a set together with a binary operation $* : G \times G \to G$ such that
(i) for $a, b \in G$, $a * b \in G$
(ii) there is an element $e \in G$ such that $a * e = e * a = a$ for any $a \in G$
(iii) for any $a \in G$, there is $b \in G$ such that $a * b = b * a = e$.

What is a Group?

Definition 2

A group G is a set together with a binary operation $* : G \times G \to G$ such that
(i) for $a, b \in G$, $a * b \in G$
(ii) there is an element $e \in G$ such that $a * e = e * a = a$ for any $a \in G$
(iii) for any $a \in G$, there is $b \in G$ such that $a * b = b * a = e$.

If in a group G, $a * b = b * a$ for all $a, b \in G$, then G is called abelian.

What is a Group?

Definition 2

A group G is a set together with a binary operation $* : G \times G \to G$ such that
(i) for $a, b \in G$, $a * b \in G$
(ii) there is an element $e \in G$ such that $a * e = e * a = a$ for any $a \in G$
(iii) for any $a \in G$, there is $b \in G$ such that $a * b = b * a = e$.

If in a group G, $a * b = b * a$ for all $a, b \in G$, then G is called abelian.

Examples:
(i) $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{(n-1)}\}$ with addition modulo n ($\overline{a} * \overline{b} := \overline{a + b \mod n}$).

What is a Group?

Definition 2

A group G is a set together with a binary operation $* : G \times G \to G$ such that
(i) for $a, b \in G$, $a * b \in G$
(ii) there is an element $e \in G$ such that $a * e = e * a = a$ for any $a \in G$
(iii) for any $a \in G$, there is $b \in G$ such that $a * b = b * a = e$.

If in a group G, $a * b = b * a$ for all $a, b \in G$, then G is called abelian.

Examples:
(i) $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{(n-1)}\}$ with addition modulo n ($\overline{a} * \overline{b} := \overline{a + b \mod n}$).
(ii) $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{r} : 0 \leqslant r \leqslant n-1, \gcd(r, n) = 1\}$ with multiplication modulo n ($\overline{a} * \overline{b} := \overline{(ab \mod n)}$).

Order of a Group & Order of an Element

Let G be a finite group.

Order of a Group & Order of an Element

Let G be a finite group.
The order of G (denoted by $|G|$) is the no. of elements in G.

Order of a Group & Order of an Element

Let G be a finite group.
The order of G (denoted by $|G|$) is the no. of elements in G.
For $a \in G$, the order of a (denoted by $|a|$) is the smallest natural number n for which $a^n = a * a * ... * a$ (n times) $= e$.

Order of a Group & Order of an Element

Let G be a finite group.
The order of G (denoted by $|G|$) is the no. of elements in G.
For $a \in G$, the order of a (denoted by $|a|$) is the smallest natural number n for which $a^n = a * a * ... * a$ (n times) $= e$.
Note that if $|a| = n$, then $a^m = e$ iff m is a multiple of n.
Examples:
(i) $|\mathbb{Z}/n\mathbb{Z}| = n$. Order of $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ is n.

Order of a Group & Order of an Element

Let G be a finite group.
The order of G (denoted by $|G|$) is the no. of elements in G.
For $a \in G$, the order of a (denoted by $|a|$) is the smallest natural number n for which $a^n = a * a * ... * a$ (n times) $= e$.
Note that if $|a| = n$, then $a^m = e$ iff m is a multiple of n.
Examples:
(i) $|\mathbb{Z}/n\mathbb{Z}| = n$. Order of $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ is n.
(ii) $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$, where ϕ is the Euler's totient function ($\phi(n)$ is the number of natural numbers $\leqslant n$, that are co-prime to n). Order of $\overline{n-1} \in (\mathbb{Z}/n\mathbb{Z})^*$ is 1, if $n = 2$ and 2, otherwise.

Order of a Group & Order of an Element

Let G be a finite group.
The order of G (denoted by $|G|$) is the no. of elements in G.
For $a \in G$, the order of a (denoted by $|a|$) is the smallest natural number n for which $a^n = a * a * ... * a$ (n times) $= e$.
Note that if $|a| = n$, then $a^m = e$ iff m is a multiple of n.
Examples:
(i) $|\mathbb{Z}/n\mathbb{Z}| = n$. Order of $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ is n.
(ii) $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$, where ϕ is the Euler's totient function ($\phi(n)$ is the number of natural numbers $\leqslant n$, that are co-prime to n). Order of $\overline{n-1} \in (\mathbb{Z}/n\mathbb{Z})^*$ is 1, if $n = 2$ and 2, otherwise.

Theorem 2 (Corollary to Lagrange's Theorem)

If G is a finite group and $a \in G$, then $|a|$ divides $|G|$.

Fermat's Little Theorem

Theorem 3

If n and a are co-prime natural numbers, $a^{\phi(n)} = 1$ (mod n)).

Fermat's Little Theorem

Theorem 3

If n and a are co-prime natural numbers, $a^{\phi(n)} = 1$ (mod n)).

Proof.

As $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, $|\overline{a}|$ divides $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$. □

Fermat's Little Theorem

Theorem 3

If n and a are co-prime natural numbers, $a^{\phi(n)} = 1$ (mod n)).

Proof.

As $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, $|\overline{a}|$ divides $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$. □

Corollary 1 (Fermat's Little Theorem)

If p is prime and $a \in \mathbb{N}$ is not divisible by p, then $a^{p-1} = 1$ (mod p).

Fermat's Little Theorem

Theorem 3

If n and a are co-prime natural numbers, $a^{\phi(n)} = 1$ (mod n)).

Proof.

As $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, $|\overline{a}|$ divides $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$. □

Corollary 1 (Fermat's Little Theorem)

If p is prime and $a \in \mathbb{N}$ is not divisible by p, then $a^{p-1} = 1$ (mod p).

Proof.

If p is prime, $\phi(p) = p - 1$. □

Converse of Fermat's Little Theorem

One might be tempted to think of an efficient test of primality based on Fermat's Little Theorem: Given a number n, choose $a \in \mathbb{N}$ co-prime to n and verify if $a^{n-1} = 1 \pmod{n}$.

Converse of Fermat's Little Theorem

One might be tempted to think of an efficient test of primality based on Fermat's Little Theorem: Given a number n, choose $a \in \mathbb{N}$ co-prime to n and verify if $a^{n-1} = 1 \pmod{n}$.
However, this test doesn't work!

Converse of Fermat's Little Theorem

One might be tempted to think of an efficient test of primality based on Fermat's Little Theorem: Given a number n, choose $a \in \mathbb{N}$ co-prime to n and verify if $a^{n-1} = 1 \pmod{n}$.
However, this test doesn't work!
The converse of the Fermat's Little Theorem is not true.

Converse of Fermat's Little Theorem

One might be tempted to think of an efficient test of primality based on Fermat's Little Theorem: Given a number n, choose $a \in \mathbb{N}$ co-prime to n and verify if $a^{n-1} = 1 \pmod{n}$.
However, this test doesn't work!
The converse of the Fermat's Little Theorem is not true.
For example, $a = 5$ and $n = 4$ are co-prime and $a^{n-1} = 125 = 1 \pmod{4}$ but 4 is not co-prime.

Converse of Fermat's Little Theorem

One might be tempted to think of an efficient test of primality based on Fermat's Little Theorem: Given a number n, choose $a \in \mathbb{N}$ co-prime to n and verify if $a^{n-1} = 1 \pmod{n}$.
However, this test doesn't work!
The converse of the Fermat's Little Theorem is not true.
For example, $a = 5$ and $n = 4$ are co-prime and $a^{n-1} = 125 = 1 \pmod{4}$ but 4 is not co-prime.
In fact, there are composite numbers n such that $a^{n-1} = 1 \pmod{n}$ for any $a \in \mathbb{N}$ co-prime to n. Such numbers are called Carmichael numbers and there are infinitely many Carmichael numbers [Alford, Granville & Pomerance, 1994].

Converse of Fermat's Little Theorem

One might be tempted to think of an efficient test of primality based on Fermat's Little Theorem: Given a number n, choose $a \in \mathbb{N}$ co-prime to n and verify if $a^{n-1} = 1 \pmod{n}$.
However, this test doesn't work!
The converse of the Fermat's Little Theorem is not true.
For example, $a = 5$ and $n = 4$ are co-prime and $a^{n-1} = 125 = 1 \pmod{4}$ but 4 is not co-prime.
In fact, there are composite numbers n such that $a^{n-1} = 1 \pmod{n}$ for any $a \in \mathbb{N}$ co-prime to n. Such numbers are called Carmichael numbers and there are infinitely many Carmichael numbers [Alford, Granville & Pomerance, 1994].
$561 = 3 \times 11 \times 17$ is one such Carmichael number.

Converse of Fermat's Little Theorem

One might be tempted to think of an efficient test of primality based on Fermat's Little Theorem: Given a number n, choose $a \in \mathbb{N}$ co-prime to n and verify if $a^{n-1} = 1 \pmod{n}$.
However, this test doesn't work!
The converse of the Fermat's Little Theorem is not true.
For example, $a = 5$ and $n = 4$ are co-prime and $a^{n-1} = 125 = 1 \pmod{4}$ but 4 is not co-prime.
In fact, there are composite numbers n such that $a^{n-1} = 1 \pmod{n}$ for any $a \in \mathbb{N}$ co-prime to n. Such numbers are called Carmichael numbers and there are infinitely many Carmichael numbers [Alford, Granville & Pomerance, 1994].
$561 = 3 \times 11 \times 17$ is one such Carmichael number.
However, there is a partial converse of Fermat's Little Theorem – Lehmer's Theorem.

Lehmer's Theorem

Theorem 4 (Lehmer's Theorem)

If a is an integer co-prime to n such that $a^{n-1} = 1 \pmod{n}$ but $a^r \neq 1 \pmod{n}$ for any $1 \leqslant r < n-1$, then n is prime.

Using Lehmer's theorem and the fact that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic for any prime p, we get the following result:

Proposition 1

A number n is prime if and only if there is a number $a \in \{2, 3, ..., n-1\}$ satisfying
(i) $a^{n-1} = 1 \pmod{n}$ and (ii) for every prime factor r of $n-1$, $a^{\frac{n-1}{r}} \neq 1 \pmod{n}$.

This was precisely the hint given in Q3 of Assignment 1.

PRIMES is in NP $\cap$ co-NP

1. Does PRIMES $\in$ NP?

PRIMES is in NP $\cap$ co-NP

1. Does PRIMES $\in$ NP?
   Yes, we saw in Question 3 of Assignment 1 that PRIMES is in NP. The certificate of primality constructed using the hint given in that question is called Pratt certificate [Pratt, 1975].

PRIMES is in NP $\cap$ co-NP

1. Does PRIMES $\in$ NP?
   Yes, we saw in Question 3 of Assignment 1 that PRIMES is in NP. The certificate of primality constructed using the hint given in that question is called Pratt certificate [Pratt, 1975].
2. Does PRIMES $\in$ co-NP?

PRIMES is in NP $\cap$ co-NP

1. Does PRIMES $\in$ NP?
   Yes, we saw in Question 3 of Assignment 1 that PRIMES is in NP. The certificate of primality constructed using the hint given in that question is called Pratt certificate [Pratt, 1975].
2. Does PRIMES $\in$ co-NP?
   It is equivalent to asking if $\overline{\text{PRIMES}} \in NP$. If $n > 1$ is not prime (*ie*, if n is composite), we can give a factor d of n with $1 < d < n$ as a certificate to prove that n is not prime. So, PRIMES is in co-NP as well.

Status of Primality Testing Before the AKS Paper

1. In 1975, Miller obtained a deterministic polynomial-time algorithm for primality testing using a property based on FLT assuming Extended Riemann Hypothesis (ERH).

Status of Primality Testing Before the AKS Paper

1. In 1975, Miller obtained a deterministic polynomial-time algorithm for primality testing using a property based on FLT assuming Extended Riemann Hypothesis (ERH).In 1980, Rabin modified his test to obtain an unconditional randomized poly-time algorithm.

Status of Primality Testing Before the AKS Paper

1. In 1975, Miller obtained a deterministic polynomial-time algorithm for primality testing using a property based on FLT assuming Extended Riemann Hypothesis (ERH).In 1980, Rabin modified his test to obtain an unconditional randomized poly-time algorithm.
2. In 1974, Solovay and Strassen obtained a randomized polynomial-time algorithm, which can be derandomized assuming ERH.

Status of Primality Testing Before the AKS Paper

1. In 1975, Miller obtained a deterministic polynomial-time algorithm for primality testing using a property based on FLT assuming Extended Riemann Hypothesis (ERH).In 1980, Rabin modified his test to obtain an unconditional randomized poly-time algorithm.
2. In 1974, Solovay and Strassen obtained a randomized polynomial-time algorithm, which can be derandomized assuming ERH.

Status of Primality Testing Before the AKS Paper (cont.)

3. A major breakthrough came in 1983, when a deterministic algorithm for primality testing was obtained by Adleman, Pomerance and Rumely, that runs in $(\log n)^{O(\log\log\log n)}$ time (all the previous deterministic algorithms required exponential time).

Status of Primality Testing Before the AKS Paper (cont.)

3. A major breakthrough came in 1983, when a deterministic algorithm for primality testing was obtained by Adleman, Pomerance and Rumely, that runs in $(\log n)^{O(\log\log\log n)}$ time (all the previous deterministic algorithms required exponential time).
4. In 1986, Goldwasser and Kilian proposed a randomized algorithm (based on Elliptic Curves) running in expected poly-time on $almost$ all inputs.

Status of Primality Testing Before the AKS Paper (cont.)

3. A major breakthrough came in 1983, when a deterministic algorithm for primality testing was obtained by Adleman, Pomerance and Rumely, that runs in $(\log n)^{O(\log\log\log n)}$ time (all the previous deterministic algorithms required exponential time).
4. In 1986, Goldwasser and Kilian proposed a randomized algorithm (based on Elliptic Curves) running in expected poly-time on $almost$ all inputs. A similar algorithm based on similar ideas was developed by Atkin.

Status of Primality Testing Before the AKS Paper (cont.)

3. A major breakthrough came in 1983, when a deterministic algorithm for primality testing was obtained by Adleman, Pomerance and Rumely, that runs in $(\log n)^{O(\log\log\log n)}$ time (all the previous deterministic algorithms required exponential time).
4. In 1986, Goldwasser and Kilian proposed a randomized algorithm (based on Elliptic Curves) running in expected poly-time on $almost$ all inputs. A similar algorithm based on similar ideas was developed by Atkin. Adleman and Huang modified the Goldwasser-Kilian algorithm in 1992 to obtain a randomized algorithm that runs in expected poly-time on all inputs.

Status of Primality Testing Before the AKS Paper (cont.)

3. A major breakthrough came in 1983, when a deterministic algorithm for primality testing was obtained by Adleman, Pomerance and Rumely, that runs in $(\log n)^{O(\log\log\log n)}$ time (all the previous deterministic algorithms required exponential time).
4. In 1986, Goldwasser and Kilian proposed a randomized algorithm (based on Elliptic Curves) running in expected poly-time on $almost$ all inputs. A similar algorithm based on similar ideas was developed by Atkin. Adleman and Huang modified the Goldwasser-Kilian algorithm in 1992 to obtain a randomized algorithm that runs in expected poly-time on all inputs.

In 2002, Agrawal, Kayal and Saxena proposed an algorithm. The AKS algorithm is an *unconditional deterministic poly-time* algorithm for primality testing.

A More General Result

Lemma 1

Let $a \in \mathbb{Z}$ and $n \geqslant 2$ be a natural number such that $\gcd(a, n) = 1$. Then n is prime if and only if

$$(X + a)^n = X^n + a \ (\text{mod } n) \tag{1}$$

A More General Result

Lemma 1

Let $a \in \mathbb{Z}$ *and* $n \geqslant 2$ *be a natural number such that* $\gcd(a, n) = 1$. *Then* n *is prime if and only if*

$$(X + a)^n = X^n + a \ (\textit{mod}\ n) \tag{1}$$

Proof.

From binomial theorem, coefficient of X^i in $(X + a)^n$ is $\binom{n}{i} a^{n-i}$.

A More General Result

Lemma 1

Let $a \in \mathbb{Z}$ *and* $n \geqslant 2$ *be a natural number such that* $\gcd(a, n) = 1$. *Then* n *is prime if and only if*

$$(X + a)^n = X^n + a \ (\textit{mod}\ n) \tag{1}$$

Proof.

From binomial theorem, coefficient of X^i in $(X + a)^n$ is $\binom{n}{i} a^{n-i}$.

$\boxed{\Rightarrow}$ Suppose n is prime. Then for any $0 < i < n$, $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ is divisible by n as $0 < i, n - i < n$. So, $(X + a)^n = X^n + a^n = X^n + a \ (\text{mod}\ n)$ for *any* a by Fermat's Last Theorem.

A More General Result

Lemma 1

Let $a \in \mathbb{Z}$ *and* $n \geqslant 2$ *be a natural number such that* $\gcd(a, n) = 1$. *Then* n *is prime if and only if*

$$(X + a)^n = X^n + a \ (\textit{mod}\ n) \tag{1}$$

Proof.

From binomial theorem, coefficient of X^i in $(X + a)^n$ is $\binom{n}{i} a^{n-i}$.

$\boxed{\Leftarrow}$ Suppose n is composite. Take a prime factor q of n. Then $q^k | n$ but $q^{k+1} \nmid n$ for some k.

A More General Result

Lemma 1

Let $a \in \mathbb{Z}$ *and* $n \geqslant 2$ *be a natural number such that* $\gcd(a, n) = 1$. *Then* n *is prime if and only if*

$$(X + a)^n = X^n + a \ (\textit{mod}\ n) \tag{1}$$

Proof.

From binomial theorem, coefficient of X^i in $(X + a)^n$ is $\binom{n}{i} a^{n-i}$.

$\boxed{\Leftarrow}$ Suppose n is composite. Take a prime factor q of n. Then $q^k | n$ but $q^{k+1} \nmid n$ for some k. Note that $\binom{n}{q} = \frac{n(n-1)\ldots(n-q+1)}{q!}$ is not divisible by q^k.

A More General Result

Lemma 1

Let $a \in \mathbb{Z}$ *and* $n \geqslant 2$ *be a natural number such that* $\gcd(a, n) = 1$. *Then* n *is prime if and only if*

$$(X + a)^n = X^n + a \ (\textit{mod}\ n) \tag{1}$$

Proof.

From binomial theorem, coefficient of X^i in $(X + a)^n$ is $\binom{n}{i} a^{n-i}$.

$\boxed{\Leftarrow}$ Suppose n is composite. Take a prime factor q of n. Then $q^k | n$ but $q^{k+1} \nmid n$ for some k. Note that $\binom{n}{q} = \frac{n(n-1)\ldots(n-q+1)}{q!}$ is not divisible by q^k. As $\gcd(n, a^{n-q}) = 1$ and n does not divide $\binom{n}{q}$, we get that the coefficient of X^q in $(X + a)^n$ is $\binom{n}{q} a^{n-q} \neq 0 \pmod{n}$. So, (1) cannot hold. $\square$

Some Prerequisites

Recall that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is an additive abelian group and $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative abelian group containing all elements of $\mathbb{Z}/p\mathbb{Z}$ except $\overline{0}$. Also, the distributive law holds: $\overline{b}(\overline{a}+\overline{c}) = \overline{b}\overline{a} + \overline{b}\overline{c}$. So, $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote this field by $\mathbb{F}_p$.

Some Prerequisites

Recall that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote this field by $\mathbb{F}_p$.
Now, in the polynomial ring $\mathbb{F}_p[X]$, if $h(X)$ is an irreducible polynomial of degree d, then $\mathbb{F}_p[X]/(h(X))$ is a finite field of order p^d (= no. of polynomials in $\mathbb{F}_p[X]$ of degree $< d$), where $(h(X))$ is the ideal generated by $h(X)$ in $\mathbb{F}_p[X]$.

Some Prerequisites

Recall that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote this field by $\mathbb{F}_p$.

Now, in the polynomial ring $\mathbb{F}_p[X]$, if $h(X)$ is an irreducible polynomial of degree d, then $\mathbb{F}_p[X]/(h(X))$ is a finite field of order p^d.

Note that the usual addition modulo n and multiplication modulo n in $\mathbb{Z}/n\mathbb{Z}$ obey distributive law. So, it is a ring. Call this ring Z_n.

Some Prerequisites

Recall that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote this field by $\mathbb{F}_p$.
Now, in the polynomial ring $\mathbb{F}_p[X]$, if $h(X)$ is an irreducible polynomial of degree d, then $\mathbb{F}_p[X]/(h(X))$ is a finite field of order p^d.
Note that $\mathbb{Z}/n\mathbb{Z}$ is a ring. Call this ring Z_n. The polynomials with coefficients in Z_n also form a ring $Z_n[X]$.

Some Prerequisites

Recall that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote this field by $\mathbb{F}_p$.

Now, in the polynomial ring $\mathbb{F}_p[X]$, if $h(X)$ is an irreducible polynomial of degree d, then $\mathbb{F}_p[X]/(h(X))$ is a finite field of order p^d.

Note that $\mathbb{Z}/n\mathbb{Z}$ is a ring. Call this ring Z_n. If $h(X) \in Z_n[X]$, then consider $(h(X)) = \{f(X)h(X) : f(X) \in Z_n[X]\}$ (= the ideal generated by $h(X)$ in $Z_n[X]$). Thus, we get the quotient ring $Z_n[X]/(h(X))$.

Some Prerequisites

Recall that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote this field by $\mathbb{F}_p$.

Now, in the polynomial ring $\mathbb{F}_p[X]$, if $h(X)$ is an irreducible polynomial of degree d, then $\mathbb{F}_p[X]/(h(X))$ is a finite field of order p^d.

Note that $\mathbb{Z}/n\mathbb{Z}$ is a ring. Call this ring Z_n. If $h(X) \in Z_n[X]$, we get the quotient ring $Z_n[X]/(h(X))$. We say $f(X) = g(X) \pmod{(h(X), n)}$ if they are same as elements of the ring $Z_n[X]/(h(X))$.

Some Prerequisites

Recall that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote this field by $\mathbb{F}_p$.

Now, in the polynomial ring $\mathbb{F}_p[X]$, if $h(X)$ is an irreducible polynomial of degree d, then $\mathbb{F}_p[X]/(h(X))$ is a finite field of order p^d.

Note that $\mathbb{Z}/n\mathbb{Z}$ is a ring. Call this ring Z_n. If $h(X) \in Z_n[X]$, we get the quotient ring $Z_n[X]/(h(X))$.

We use the symbol $\widetilde{\mathrm{O}}(t(n))$ to denote $\mathrm{O}(t(n) \cdot \mathrm{poly}(\log(t(n))))$, where $t(n)$ is some function of n. So, $\widetilde{\mathrm{O}}(\log^k(n)) = \mathrm{O}(\log^k(n) \cdot \mathrm{poly}(\log\log(n))) = \mathrm{O}(\log^{k+\epsilon}(n))$ for any $\epsilon > 0$.

Some Prerequisites

Recall that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote this field by $\mathbb{F}_p$.

Now, in the polynomial ring $\mathbb{F}_p[X]$, if $h(X)$ is an irreducible polynomial of degree d, then $\mathbb{F}_p[X]/(h(X))$ is a finite field of order p^d.

Note that $\mathbb{Z}/n\mathbb{Z}$ is a ring. Call this ring Z_n. If $h(X) \in Z_n[X]$, we get the quotient ring $Z_n[X]/(h(X))$.

$\widetilde{\mathrm{O}}(\log^k(n)) = \mathrm{O}(\log^k(n) \cdot \mathrm{poly}(\log\log(n))) = \mathrm{O}(\log^{k+\epsilon}(n))$ for any $\epsilon > 0$. By default, $\log$ means logarithm w.r.t. base 2 and $\ln$ means the natural logarithm (logarithm w.r.t. base e).

For $n \in \mathbb{N}$, $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, the order of a modulo n is defined as the order of $\overline{(a \mod n)}$ in $(\mathbb{Z}/n\mathbb{Z})^*$. We denote it by $\mathrm{o}_n(a)$.

Some Prerequisites

Recall that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote this field by $\mathbb{F}_p$.

Now, in the polynomial ring $\mathbb{F}_p[X]$, if $h(X)$ is an irreducible polynomial of degree d, then $\mathbb{F}_p[X]/(h(X))$ is a finite field of order p^d.

Note that $\mathbb{Z}/n\mathbb{Z}$ is a ring. Call this ring Z_n. If $h(X) \in Z_n[X]$, we get the quotient ring $Z_n[X]/(h(X))$.

$\widetilde{\mathrm{O}}(\log^k(n)) = \mathrm{O}(\log^k(n) \cdot \mathrm{poly}(\log\log(n))) = \mathrm{O}(\log^{k+\epsilon}(n))$ for any $\epsilon > 0$.

For $n \in \mathbb{N}$, $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, the order of a modulo n is defined as the order of $\overline{(a \mod n)}$ in $(\mathbb{Z}/n\mathbb{Z})^*$. We denote it by $\mathrm{o}_n(a)$. From Theorem 3, for $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, $\mathrm{o}_n(a) \mid \phi(n)$.

A Test of Primality Based on Lemma 1

From Lemma 1, we can get a simple test for primality: for an input n, choose a number a co-prime to n and check whether the equation (1) is satisfied or not. Unfortunately, this requires computing n coefficients of $(X + a)^n$.

A Test of Primality Based on Lemma 1

To reduce the number of coefficients to be evaluated, one may evaluate both sides of (1) modulo a polynomial of the form $X^r - 1$ for some small r:

$$(X + a)^n = X^n + a \ (\text{mod } (X^r - 1, n)) \tag{2}$$

A Test of Primality Based on Lemma 1

To reduce the number of coefficients to be evaluated, one may evaluate both sides of (1) modulo a polynomial of the form $X^r - 1$ for some small r:

$$(X + a)^n = X^n + a \ (\text{mod } (X^r - 1, n)) \tag{2}$$

As any prime n satisfies the equation (1), it satisfies (2) for all values of r. However, some composite number n may also satisfy the equation for a few values of a and r.

A Test of Primality Based on Lemma 1

To reduce the number of coefficients to be evaluated, one may evaluate both sides of (1) modulo a polynomial of the form $X^r - 1$ for some small r:

$$(X + a)^n = X^n + a \pmod{(X^r - 1, n)} \tag{2}$$

As any prime n satisfies the equation (1), it satisfies (2) for all values of r. However, some composite number n may also satisfy the equation for a few values of a and r. For $n = 4$, $a = 3$, $r = 2$, $(X + a)^n = (X + 3)^4 = X^4 + 6X^2 + 1 = X^4 + 2(X^2 - 1) + 3 = X^4 + 3 \pmod{(X^2 - 1, 4)}$.

A Test of Primality Based on Lemma 1

To reduce the number of coefficients to be evaluated, one may evaluate both sides of (1) modulo a polynomial of the form $X^r - 1$ for some small r:

$$(X + a)^n = X^n + a \ (\text{mod } (X^r - 1, n)) \tag{2}$$

As any prime n satisfies the equation (1), it satisfies (2) for all values of r. However, some composite number n may also satisfy the equation for a few values of a and r. AKS show that for some appropriately chosen r if the equation (2) is satisfied for a number of a's, then n is a prime number. The appropriate r and the number of a's for which (2) needs to be checked are both bounded by a polynomial in $\log(n)$.

A Test of Primality Based on Lemma 1

To reduce the number of coefficients to be evaluated, one may evaluate both sides of (1) modulo a polynomial of the form $X^r - 1$ for some small r:

$$(X + a)^n = X^n + a \ (\text{mod } (X^r - 1, n)) \tag{2}$$

As any prime n satisfies the equation (1), it satisfies (2) for all values of r. However, some composite number n may also satisfy the equation for a few values of a and r. AKS show that for some appropriately chosen r if the equation (2) is satisfied for a number of a's, then n is a prime number. The appropriate r and the number of a's for which (2) needs to be checked are both bounded by a polynomial in $\log(n)$. This gives a deterministic poly-time algorithm for testing primality.

A Lower Bound for LCM of first N Natural Numbers

Lemma 2

Let $LCM(N) := \text{lcm}(1, 2, ..., N)$ *be the least common multiple of first* N *natural numbers. Then for* $N \geqslant 7$, $LCM(N) \geqslant 2^N$.

Algorithm for Primality Testing (AKS Algorithm)

Input: n (an integer > 1)

1. If ($n = a^b$ for some $a \in \mathbb{N}$ and $b > 1$),
   output COMPOSITE;
2. Find the smallest r such that $\mathrm{o}_r(n) > \log^2(n)$.
3. If $1 < \gcd(a, n) < n$ for some $a \in \mathbb{N}$ with $1 \leqslant a \leqslant r$,
   output COMPOSITE;
4. If $n \leqslant r$,
   output PRIME;
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 (AKS Algorithm)

Input: n (an integer > 1)

1. If ($n = a^b$ for some $a \in \mathbb{N}$ and $b > 1$),
   output COMPOSITE;
2. Find the smallest r such that $\mathrm{o}_r(n) > \log^2(n)$.
3. If $1 < \gcd(a, n) < n$ for some $a \in \mathbb{N}$ with $1 \leqslant a \leqslant r$,
   output COMPOSITE;
4. If $n \leqslant r$,
   output PRIME;
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;

Output of AKS Algorithm for Prime Input

Input: n (an integer > 1)

1. If ($n = a^b$ for some $a \in \mathbb{N}$ and $b > 1$), output COMPOSITE;
2. Find the smallest r such that $\mathrm{o}_r(n) > \log^2(n)$.
3. If $1 < \gcd(a, n) < n$ for some $a \in \mathbb{N}$ with $1 \leqslant a \leqslant r$, output COMPOSITE;
4. If $n \leqslant r$, output PRIME;
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;

Lemma 3

If n is prime, AKS algorithm returns PRIME.

Proof.

If n is prime, neither of steps 1 and 3 can return COMPOSITE.

Output of AKS Algorithm for Prime Input

Input: n (an integer > 1)

1. If ($n = a^b$ for some $a \in \mathbb{N}$ and $b > 1$), output COMPOSITE;
2. Find the smallest r such that $\mathrm{o}_r(n) > \log^2(n)$.
3. If $1 < \gcd(a, n) < n$ for some $a \in \mathbb{N}$ with $1 \leqslant a \leqslant r$, output COMPOSITE;
4. If $n \leqslant r$, output PRIME;
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;

Lemma 3

If n is prime, AKS algorithm returns PRIME.

Proof.

If n is prime, neither of steps 1 and 3 can return COMPOSITE. From Lemma 1, step 5 also cannot return COMPOSITE. □

AKS Algorithm Returns PRIME

Input: n (an integer > 1)

3. If $1 < \gcd(a, n) < n$ for some $a \in \mathbb{N}$ with $1 \leqslant a \leqslant r$, output COMPOSITE;
4. If $n \leqslant r$, output PRIME;
6. output PRIME;

We proved that if n is prime, AKS algorithm returns PRIME. To show the correctness of the algorithm, we need to show the converse as well, *ie*, we need to prove that if the algorithm returns PRIME, then n is prime.

AKS Algorithm Returns PRIME

Input: n (an integer > 1)

3. If $1 < \gcd(a, n) < n$ for some $a \in \mathbb{N}$ with $1 \leqslant a \leqslant r$, output COMPOSITE;
4. If $n \leqslant r$, output PRIME;
6. output PRIME;

We proved that if n is prime, AKS algorithm returns PRIME. To show the correctness of the algorithm, we need to show the converse as well, *ie*, we need to prove that if the algorithm returns PRIME, then n is prime.

Suppose the algorithm returns PRIME. If step 4 returns PRIME, then as $n \leqslant r$ and step 3 did not return COMPOSITE, for all $a \in \mathbb{N}$ with $1 \leqslant a < n$, $\gcd(a, n) = 1$. So, n is prime. (If n is composite, it would have a divisor d with $1 < d < n$. Then $1 < \gcd(d, n) = d < n$.) So, we just need to prove that if step 6 returns PRIME, then n is prime. For future analysis, assume that this is the case (*ie*, step 6 returns PRIME).

Bound on r

Recall step 2 of AKS algorithm: Find the smallest r such that $\mathrm{o}_r(n) > \log^2(n)$.

Bound on r

Recall step 2 of AKS algorithm: Find the smallest r such that $\mathrm{o}_r(n) > \log^2(n)$.

Lemma 4

There is a natural number $r \leqslant \max(3, \lceil \log^5(n) \rceil)$ *such that* $\mathrm{o}_r(n) > \log^2(n)$.

Bound on r

Lemma 4

There is a natural number $r \leqslant \max(3, \lceil \log^5(n) \rceil)$ *such that* $\mathrm{o}_r(n) > \log^2(n)$.

Proof.

For $n = 2$, we can take $r = 3$ as $3 \leqslant \max(3, \lceil \log^5(2) \rceil) = 3$ and $\mathrm{o}_3(2) = 2 > 1 = \log^2(2)$. For $n = 3$, we can take $r = 5$ as $5 \leqslant \max(3, \lceil \log^5(3) \rceil) = 11$ and $\mathrm{o}_5(3) = 4 > \log^2(3) \approx 2.51$. For $n = 4$, we can take $r = 11$ as $11 \leqslant \max(3, \lceil \log^5(4) \rceil) = 32$ and $\mathrm{o}_1\, 1(4) = 5 > 4 = \log^2(4)$. For $n = 5$, we can take $r = 7$ as $7 \leqslant \max(3, \lceil \log^5(5) \rceil) = 68$ and $\mathrm{o}_7(5) = 6 > \log^2(5) \approx 5.39$.

Bound on r

Lemma 4

There is a natural number $r \leqslant \max(3, \lceil \log^5(n) \rceil)$ *such that* $\mathrm{o}_r(n) > \log^2(n)$.

Proof.

Assume $n \geqslant 6$. Then $\log(n) \geqslant \log(6) > 5/2$ as $6^2 > 2^5$. So $\log^5(n) > \log^5(6) > 30$ and $B := \lceil \log^5(n) \rceil > 30$ and we can apply Lemma 2 for $LCM(B)$. Also, $\log^2(n) > (5/2)^2 = 25/4$ and $\log^3(n) > (5/2)^3 = 125/8 > 15$.

Bound on r

Proof.

Consider the smallest number r that does not divide the product

$$C := n^{\lfloor \log(B) \rfloor} \prod_{i=1}^{\lfloor \log^2(n) \rfloor} (n^i - 1).$$

Firstly, note that $C = n^{\lfloor \log(B) \rfloor} \prod_{i=1}^{\lfloor \log^2(n) \rfloor} (n^i - 1) < n^{\lfloor \log(B) \rfloor} \prod_{i=1}^{\lfloor \log^2(n) \rfloor} n^i \leqslant n^{\log(B) + \frac{1}{2}\log^2(n)(\log^2(n)+1)}$. Now, $\log(B) \leqslant \log(\log^6(n)) \leqslant 6\log(\log(n)) \leqslant 6\log(n) < 6\log(n) \times \frac{\log^3(n)}{15} = \frac{2}{5}\log^4(n)$. And $\frac{1}{2}\log^2(n) \leqslant \frac{1}{2}\log^2(n) \times \frac{\log^2(n)}{25/4} = \frac{8}{100}\log^4(n) < \frac{1}{10}\log^4(n)$. So, $\log(B) + \frac{1}{2}\log^2(n)(\log^2(n)+1) < \frac{2}{5}\log^4(n) + \frac{1}{2}\log^4(n) + \frac{1}{10}\log^4(n) = \log^4(n)$. So, $C < n^{\log^4(n)} = 2^{\log^5(n)} \leqslant 2^B$.

Bound on r

Lemma 4

There is a natural number $r \leqslant \max(3, \lceil \log^5(n) \rceil)$ *such that* $\mathrm{o}_r(n) > \log^2(n)$.

Proof.

Assume $n \geqslant 6$. $B := \lceil \log^5(n) \rceil$. Consider the smallest number r that does not divide the product

$$C := n^{\lfloor \log(B) \rfloor} \prod_{i=1}^{\lfloor \log^2(n) \rfloor} (n^i - 1).$$

$C < n^{\log^4(n)} = 2^{\log^5(n)} \leqslant 2^B$. Note that C cannot be divisible by all natural numbers $\leqslant B$ as $LCM(B) \geqslant 2^B$ and $C < 2^B$. So, $r \leqslant B$.

Bound on r

Proof.

Assume $n \geqslant 6$. $B := \lceil \log^5(n) \rceil$. Consider the smallest number r that does not divide the product $C := n^{\lfloor \log(B) \rfloor} \prod_{i=1}^{\lfloor \log^2(n) \rfloor} (n^i - 1)$.

$r \leqslant B$. We claim that $\gcd(r, n) = 1$. Otherwise, there will be a prime p dividing $\gcd(r, n)$. Let $r = p^k m$, where m is co-prime to p. As $p \geqslant 2$, $k \leqslant \log(r) \leqslant \log(B)$. So, $k \leqslant \lfloor \log(B) \rfloor$. As $p \mid n$, $p^k \mid C$. So, $m = \frac{r}{p^k}$ does not divide C. (Otherwise, both p^k and m will divide C and as p^k and m are co-prime, $r = p^k m$ will also divide C, contradiction!) But then $m < r$ and m does not divide C. Contradiction! So, $\gcd(r, n) = 1$. As $n^i - 1$ is not divisible by r for $1 \leqslant i \leqslant \lfloor \log^2(n) \rfloor$, $n^i \neq 1 \pmod{r}$ for $1 \leqslant i \leqslant \lfloor \log^2(n) \rfloor$. Hence, $\mathrm{o}_r(n) \geqslant \lfloor \log^2(n) \rfloor + 1 > \log^2(n)$. □

Towards Introspectivity

We have found an r such that $\mathrm{o}_r(n) > \log^2(n)$. As $n \geqslant 2$, $\mathrm{o}_r(n) > 1$. So, there is a prime factor p of n such that $\mathrm{o}_r(p) > 1$. (If not, then $\mathrm{o}_r(p) = 1$ and hence, $p = 1 \pmod r$ for all p dividing n, which will imply $n = 1 \pmod r$ contradicting $\mathrm{o}_r(n) > 1$.)

Towards Introspectivity

Input: n (an integer > 1)

3. If $1 < \gcd(a, n) < n$ for some $a \in \mathbb{N}$ with $1 \leqslant a \leqslant r$, output COMPOSITE;
4. If $n \leqslant r$, output PRIME;
6. output PRIME;

We have found an r such that $\mathrm{o}_r(n) > \log^2(n)$. So, there is a prime factor p of n such that $\mathrm{o}_r(p) > 1$.

As we have assumed that step 6 returns PRIME, we must have $p > r$. [If $p \leqslant r$ and $p < n$, then step 3 would return COMPOSITE as $1 < p = \gcd(p, n) < n$ with $1 \leqslant p \leqslant r$. If $p \leqslant r$ and $p = n$, then $n \leqslant r$ and step 4 would return PRIME.]

Towards Introspectivity

Input: n **(an integer** > 1**)**

3. **If** $1 < \gcd(a, n) < n$ **for some** $a \in \mathbb{N}$ **with** $1 \leqslant a \leqslant r$**, output COMPOSITE;**
4. **If** $n \leqslant r$**, output PRIME;**
6. **output PRIME;**

We have found an r such that $\mathrm{o}_r(n) > \log^2(n)$. So, there is a prime factor p of n such that $\mathrm{o}_r(p) > 1$.

As we have assumed that step 6 returns PRIME, we must have $p > r$.

Moreover, note that $\gcd(n, r) = 1$. So, $p, n \in (\mathbb{Z}/r\mathbb{Z})^*$.

Towards Introspectivity

Input: n **(an integer** > 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;

We have found an r such that $\mathrm{o}_r(n) > \log^2(n)$. So, there is a prime factor p of n such that $\mathrm{o}_r(p) > 1$.

As we have assumed that step 6 returns PRIME, we must have $p > r$.

Moreover, note that $\gcd(n, r) = 1$. So, $p, n \in (\mathbb{Z}/r\mathbb{Z})^*$.

Take $\ell = \lfloor \sqrt{\phi(r)} \log(n) \rfloor$. As step 5 does not return COMPOSITE, we must have $(X+a)^n = X^n + a \pmod{(X^r - 1, n)}$ for all a with $1 \leqslant a \leqslant \ell$. For $a = 0$, $(X+a)^n = X^n = X^n + a \pmod{(X^r - 1, n)}$ trivially.

Towards Introspectivity

Input: n **(an integer** > 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;

We have found an r such that $\mathrm{o}_r(n) > \log^2(n)$. So, there is a prime factor p of n such that $\mathrm{o}_r(p) > 1$.
As we have assumed that step 6 returns PRIME, we must have $p > r$.
Moreover, note that $\gcd(n, r) = 1$. So, $p, n \in (\mathbb{Z}/r\mathbb{Z})^*$.
Take $\ell = \lfloor \sqrt{\phi(r)} \log(n) \rfloor$. As step 5 does not return COMPOSITE, we must have $(X+a)^n = X^n + a \pmod{(X^r - 1, n)}$ for all a with $0 \leqslant a \leqslant \ell$. So,

$$(X+a)^n = X^n + a \pmod{(X^r - 1, p)} \qquad (3)$$

for all a with $0 \leqslant a \leqslant \ell$.

Towards Introspectivity

Take $\ell = \lfloor \sqrt{\phi(r)} \log(n) \rfloor$.

$$(X + a)^n = X^n + a \pmod{(X^r - 1, p)} \tag{3}$$

for all a with $0 \leqslant a \leqslant \ell$. From Lemma 1,

$$(X + a)^p = X^p + a \pmod{(X^r - 1, p)} \tag{4}$$

for all a with $0 \leqslant a \leqslant \ell$.

Towards Introspectivity

$$(X+a)^n = X^n + a \pmod{(X^r-1, p)} \tag{3}$$

for all a with $0 \leqslant a \leqslant \ell$.

$$(X+a)^p = X^p + a \pmod{(X^r-1, p)} \tag{4}$$

for all a with $0 \leqslant a \leqslant \ell$. Now, note that $(X^p)^{\frac{n}{p}} + a = X^n + a = (X+a)^n = ((X+a)^p)^{\frac{n}{p}} = (X^p+a)^{\frac{n}{p}} \pmod{(X^r-1, p)}$. As $\gcd(p, r) = 1$, there exist integers k, s such that $kr+sp = 1$. $X = X^{kr+sp} = (X^r)^k X^{ps} = X^{ps}$ in $\mathbb{F}_p[X]/((X^r-1))$ as $X^r = 1$ in $\mathbb{F}_p[X]/((X^r-1))$. Hence, $(X+a)^{\frac{n}{p}} = (X^{ps}+a)^{\frac{n}{p}} = ((X^s+a)^p)^{\frac{n}{p}} = (X^s+a)^n$ in $\mathbb{F}_p[X]/((X^r-1))$. From (3), $(X^s+a)^n = X^{ns}+a$ in $\mathbb{F}_p[X]/((X^{rs}-1))$. So, $(X^s+a)^n = X^{ns}+a$ in $\mathbb{F}_p[X]/((X^r-1))$. So, $(X+a)^{\frac{n}{p}} = X^{ns}+a = (X^{ps})^{\frac{n}{p}}+a = X^{\frac{n}{p}}+a$ in $\mathbb{F}_p[X]/((X^r-1))$.

Towards Introspectivity

$$(X+a)^n = X^n + a \pmod{(X^r-1, p)} \tag{3}$$

for all a with $0 \leqslant a \leqslant \ell$.

$$(X+a)^p = X^p + a \pmod{(X^r-1, p)} \tag{4}$$

for all a with $0 \leqslant a \leqslant \ell$. Hence,

$$(X+a)^{\frac{n}{p}} = X^{\frac{n}{p}} + a \pmod{(X^r-1, p)} \tag{5}$$

for all a with $0 \leqslant a \leqslant \ell$. Note that each of n, $\frac{n}{p}$ and p satisfies

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

for m for any a with $0 \leqslant a \leqslant \ell$.

Introspectivity

Definition 3

Let $f(X)$ be a polynomial and $m \in \mathbb{N}$. m is said to be introspective for $f(X)$, if $[f(X)]^m = f(X^m) \pmod{(X^r - 1, p)}$.

Introspectivity

Definition 3

Let $f(X)$ be a polynomial and $m \in \mathbb{N}$. m is said to be introspective for $f(X)$, if $[f(X)]^m = f(X^m) \pmod{(X^r - 1, p)}$.

From the previous slide, we know that each of n, $\frac{n}{p}$ and p is introspective for $X + a$ for any a with $0 \leqslant a \leqslant \ell$.

Introspectivity

Definition 3

Let $f(X)$ be a polynomial and $m \in \mathbb{N}$. m is said to be introspective for $f(X)$, if $[f(X)]^m = f(X^m) \pmod{(X^r - 1, p)}$.

From the previous slide, we know that each of n, $\frac{n}{p}$ and p is introspective for $X + a$ for any a with $0 \leqslant a \leqslant \ell$.
We shall now prove two short lemmata about introspectivity.

Introspective Numbers are Closed Under Multiplication

Lemma 5

If m and m' are introspective numbers for $f(X)$, then $m \cdot m'$ is also introspective for $f(X)$.

Introspective Numbers are Closed Under Multiplication

Lemma 5

If m and m' are introspective numbers for $f(X)$, then $m \cdot m'$ is also introspective for $f(X)$.

Proof.

$[f(X)]^m = f(X^m) \pmod{(X^r - 1, p)}$ and $[f(X)]^{m'} = f\left(X^{m'}\right) \pmod{(X^r - 1, p)}$. Replacing X by $X^{m'}$ in the first equation, we get $\left[f\left(X^{m'}\right)\right]^m = f\left(X^{mm'}\right) \pmod{(X^{m'r} - 1, p)}$.

Introspective Numbers are Closed Under Multiplication

Lemma 5

If m and m' are introspective numbers for $f(X)$, then $m \cdot m'$ is also introspective for $f(X)$.

Proof.

$[f(X)]^m = f(X^m) \pmod{(X^r - 1, p)}$ and $[f(X)]^{m'} = f\left(X^{m'}\right) \pmod{(X^r - 1, p)}$. Replacing X by $X^{m'}$ in the first equation, we get $\left[f\left(X^{m'}\right)\right]^m = f\left(X^{mm'}\right) \pmod{(X^{m'r} - 1, p)}$. As $X^r - 1$ divides $X^{m'r} - 1$, $((X^{m'r} - 1)) \subseteq ((X^r - 1))$. So, $\left[f\left(X^{m'}\right)\right]^m = f\left(X^{mm'}\right) \pmod{(X^r - 1, p)}$.

Introspective Numbers are Closed Under Multiplication

Lemma 5

If m and m' are introspective numbers for $f(X)$, then $m \cdot m'$ is also introspective for $f(X)$.

Proof.

$[f(X)]^m = f(X^m) \pmod{(X^r - 1, p)}$ and $[f(X)]^{m'} = f\left(X^{m'}\right) \pmod{(X^r - 1, p)}$. As $X^r - 1$ divides $X^{m'r} - 1$, $((X^{m'r} - 1)) \subseteq ((X^r - 1))$. So, $\left[f\left(X^{m'}\right)\right]^m = f\left(X^{mm'}\right) \pmod{(X^r - 1, p)}$. Now, the second equation gives $[f(X)]^{m \cdot m'} = \left[[f(X)]^{m'}\right]^m = \left[f\left(X^{m'}\right)\right]^m = f\left(X^{mm'}\right) \pmod{(X^r - 1, p)}$. □

Polynomials with Same Introspective Number are Closed Under Multiplication

Lemma 6

If m is introspective for polynomials $f(X)$ and $g(X)$, then m is also introspective for $f(X) \cdot g(X)$.

Polynomials with Same Introspective Number are Closed Under Multiplication

Lemma 6

If m is introspective for polynomials $f(X)$ and $g(X)$, then m is also introspective for $f(X) \cdot g(X)$.

Proof.

$[f(X)]^m = f(X^m) \pmod{(X^r - 1, p)}$ and $[g(X)]^m = g(X^m) \pmod{(X^r - 1, p)}$. So, $[f(X) \cdot g(X)]^m = [f(X)]^m \cdot [g(X)]^m = f(X^m) \cdot g(X^m) \pmod{(X^r - 1, p)}$. □

Defining The First Group

As both p and $\frac{n}{p}$ are introspective for $X + a$ for any a with $0 \leqslant a \leqslant \ell$, from Lemma 5, $\left(\frac{n}{p}\right)^i p^j$ is introspective for $X + a$ for all $i, j \geqslant 0$ (trivially true for $i = j = 0$) for any a with $0 \leqslant a \leqslant \ell$.

Defining The First Group

As both p and $\frac{n}{p}$ are introspective for $X + a$ for any a with $0 \leqslant a \leqslant \ell$, from Lemma 5, $\left(\frac{n}{p}\right)^i p^j$ is introspective for $X + a$ for all $i, j \geqslant 0$ (trivially true for $i = j = 0$) for any a with $0 \leqslant a \leqslant \ell$. So, from Lemma 6, for any $i, j \geqslant 0$, $\left(\frac{n}{p}\right)^i p^j$ is introspective for the polynomial $\prod_{a=0}^{\ell}(X+a)^{e_a}$, where $e_a \geqslant 0$ for all a (again if all $e_a = 0$, this is trivially true as any number is introspective for the constant polynomial 1).

Defining The First Group

As both p and $\frac{n}{p}$ are introspective for $X + a$ for any a with $0 \leqslant a \leqslant \ell$, from Lemma 5, $\left(\frac{n}{p}\right)^i p^j$ is introspective for $X + a$ for all $i, j \geqslant 0$ (trivially true for $i = j = 0$) for any a with $0 \leqslant a \leqslant \ell$. So, from Lemma 6, for any $i, j \geqslant 0$, $\left(\frac{n}{p}\right)^i p^j$ is introspective for the polynomial $\prod_{a=0}^{\ell}(X+a)^{e_a}$, where $e_a \geqslant 0$ for all a (again if all $e_a = 0$, this is trivially true as any number is introspective for the constant polynomial 1). Thus, every number in $I := \left\{\left(\frac{n}{p}\right)^i p^j : i, j \geqslant 0\right\}$ is introspective for every polynomial in $P := \left\{\prod_{a=0}^{\ell}(X+a)^{e_a} : e_a \geqslant 0 \text{ for } 0 \leqslant a \leqslant \ell\right\}$.

Defining The First Group

Every number in $I := \left\{ \left(\frac{n}{p}\right)^i p^j : i, j \geqslant 0 \right\}$ is introspective for every polynomial in $P := \left\{ \prod_{a=0}^{\ell} (X+a)^{e_a} : e_a \geqslant 0 \right\}$. Consider $G :=$ the set of residues of numbers in I modulo r. As $\gcd(n, r) = 1 = \gcd(p, r)$ and $\left(\frac{n}{p}\right)^i p^j = n^i p^{j-i}$, G is a subset of $(\mathbb{Z}/r\mathbb{Z})^*$. As I is closed under multiplication, G is also closed under multiplication modulo r. So, G is a subgroup of $(\mathbb{Z}/r\mathbb{Z})^*$. [If a finite subset G of a group H is closed under group operation, then G is a subgroup.] Let $t := |G|$. Then as $n \in I$ and $\mathrm{o}_r(n) > \log^2(n)$, $t = |G| \geqslant |\overline{n}| = \mathrm{o}_r(n) > \log^2(n)$.

Cyclotomic Polynomials over Finite Fields

Definition 4

Let $\mathbb{F}$ be a finite field of characteristic p and r be a natural number not divisible by p. $\xi \in \overline{\mathbb{F}}$ is called a primitive r-th root of unity, if $\xi^r = 1$ and $\xi^m \neq 1$ for any natural number $m < r$.

Cyclotomic Polynomials over Finite Fields

Definition 4

Let $\mathbb{F}$ be a finite field of characteristic p and r be a natural number not divisible by p. $\xi \in \overline{\mathbb{F}}$ is called a primitive r-th root of unity, if $\xi^r = 1$ and $\xi^m \neq 1$ for any natural number $m < r$.

Definition 5

Let $\mathbb{F}_q$ be a finite field with q elements and characteristic p and let r be a natural not divisible by p. Then the r-th cyclotomic polynomial $Q_r(X)$ over $\mathbb{F}_q$ is the monic polynomial, whose roots are *precisely* the primitive r-th roots of unity in $\overline{\mathbb{F}_q}$.

Cyclotomic Polynomials over Finite Fields

Definition 4

Let $\mathbb{F}$ be a finite field of characteristic p and r be a natural number not divisible by p. $\xi \in \overline{\mathbb{F}}$ is called a primitive r-th root of unity, if $\xi^r = 1$ and $\xi^m \neq 1$ for any natural number $m < r$.

Definition 5

Let $\mathbb{F}_q$ be a finite field with q elements and characteristic p and let r be a natural not divisible by p. Then the r-th cyclotomic polynomial $Q_r(X)$ over $\mathbb{F}_q$ is the monic polynomial, whose roots are *precisely* the primitive r-th roots of unity in $\overline{\mathbb{F}_q}$.

Put another way, if $\mathcal{S}$ is the set of primitive r-th roots of unity in $\overline{\mathbb{F}_q}$, then the r-th cyclotomic polynomial $Q_r(X) = \prod_{\xi \in \mathcal{S}}(X - \xi)$.

Some Facts about $Q_r(X)$ over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

Some Facts about $Q_r(X)$ over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

1. $Q_r(X) \in \mathbb{F}_q[X]$.

Some Facts about $Q_r(X)$ over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

1. $Q_r(X) \in \mathbb{F}_q[X]$.
2. $Q_r(X)$ divides $X^r - 1$ in $\mathbb{F}_q[X]$.

Some Facts about $Q_r(X)$ over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

1. $Q_r(X) \in \mathbb{F}_q[X]$.
2. $Q_r(X)$ divides $X^r - 1$ in $\mathbb{F}_q[X]$.
3. Degree of $Q_r(X)$ is $\phi(r)$.

Some Facts about $Q_r(X)$ over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

1. $Q_r(X) \in \mathbb{F}_q[X]$.
2. $Q_r(X)$ divides $X^r - 1$ in $\mathbb{F}_q[X]$.
3. Degree of $Q_r(X)$ is $\phi(r)$.
4. $Q_r(X)$ factors into irreducible factors of degree $\mathrm{o}_r(q)$ in $\mathbb{F}_q[X]$.

Some Facts about $Q_r(X)$ over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

1. $Q_r(X) \in \mathbb{F}_q[X]$.
2. $Q_r(X)$ divides $X^r - 1$ in $\mathbb{F}_q[X]$.
3. Degree of $Q_r(X)$ is $\phi(r)$.
4. $Q_r(X)$ factors into irreducible factors of degree $\mathrm{o}_r(q)$ in $\mathbb{F}_q[X]$.

For our purpose, we take $q = p$, *ie*, $\mathbb{F}_q = \mathbb{F}_p$. Then $Q_r(X)$ factors into irreducible factors of degree $\mathrm{o}_r(p)$.

Defining the Second Group

Let the r-th cyclotomic polynomial over $\mathbb{F}_p(X)$ be $Q_r(X)$. We know that $Q_r(X)$ factors into irreducible factors of degree $\mathrm{o}_r(p)$.

Defining the Second Group

Let the r-th cyclotomic polynomial over $\mathbb{F}_p(X)$ be $Q_r(X)$. We know that $Q_r(X)$ factors into irreducible factors of degree $\mathrm{o}_r(p)$. Let $h(X)$ be one such irreducible factor. Since $\mathrm{o}_r(p) > 1$, the degree of $h(X)$ is $\mathrm{o}_r(p) > 1$. Now, as $h(X) \in \mathbb{F}_p[X]$ is irreducible, $\mathbb{F} := \mathbb{F}_p[X]/((h(X))$ is a field.

Defining the Second Group

Let the r-th cyclotomic polynomial over $\mathbb{F}_p(X)$ be $Q_r(X)$. We know that $Q_r(X)$ factors into irreducible factors of degree $\mathrm{o}_r(p)$. Let $h(X)$ be one such irreducible factor. Since $\mathrm{o}_r(p) > 1$, the degree of $h(X)$ is $\mathrm{o}_r(p) > 1$. Now, as $h(X) \in \mathbb{F}_p[X]$ is irreducible, $\mathbb{F} := \mathbb{F}_p[X]/((h(X))$ is a field.

The second group $\mathcal{G}$ is defined as the set of all residues of polynomials in $P = \left\{\prod_{a=0}^{\ell}(X+a)^{e_a} : e_a \geqslant 0 \text{ for } 0 \leqslant a \leqslant \ell\right\}$ modulo $h(X)$ and p with usual multiplication.

Defining the Second Group

Let the r-th cyclotomic polynomial over $\mathbb{F}_p(X)$ be $Q_r(X)$. We know that $Q_r(X)$ factors into irreducible factors of degree $\mathrm{o}_r(p)$. Let $h(X)$ be one such irreducible factor. Since $\mathrm{o}_r(p) > 1$, the degree of $h(X)$ is $\mathrm{o}_r(p) > 1$. Now, as $h(X) \in \mathbb{F}_p[X]$ is irreducible, $\mathbb{F} := \mathbb{F}_p[X]/((h(X))$ is a field.

The second group $\mathcal{G}$ is defined as the set of all residues of polynomials in $P = \left\{\prod_{a=0}^{\ell}(X+a)^{e_a} : e_a \geqslant 0 \text{ for } 0 \leqslant a \leqslant \ell\right\}$ modulo $h(X)$ and p with usual multiplication. Alternatively, $\mathcal{G}$ is the subgroup of $\mathbb{F}^*$ generated by the elements of the form $X + a$ for $0 \leqslant a \leqslant \ell$.

The Two Groups

Every number in $I := \left\{ \left(\frac{n}{p}\right)^i p^j : i, j \geqslant 0 \right\}$ is introspective for every polynomial in $P := \left\{ \prod_{a=0}^{\ell} (X+a)^{e_a} : e_a \geqslant 0 \right\}$. $G :=$ the set of residues of numbers in I modulo r. G is a subgroup of $(\mathbb{Z}/r\mathbb{Z})^*$. Let $t := |G|$. Then as $n \in I$ and $\mathrm{o}_r(n) > \log^2(n)$, $t = |G| \geqslant |\overline{n}| = \mathrm{o}_r(n) > \log^2(n)$.

The Two Groups

Every number in $I := \left\{ \left(\frac{n}{p}\right)^i p^j : i, j \geqslant 0 \right\}$ is introspective for every polynomial in $P := \left\{ \prod_{a=0}^{\ell} (X+a)^{e_a} : e_a \geqslant 0 \right\}$. $G :=$ the set of residues of numbers in I modulo r. G is a subgroup of $(\mathbb{Z}/r\mathbb{Z})^*$. Let $t := |G|$. Then as $n \in I$ and $\mathrm{o}_r(n) > \log^2(n)$, $t = |G| \geqslant |\overline{n}| = \mathrm{o}_r(n) > \log^2(n)$.

$\mathcal{G}$ is defined as the set of all residues of polynomials in $P = \left\{ \prod_{a=0}^{\ell} (X+a)^{e_a} : e_a \geqslant 0 \text{ for } 0 \leqslant a \leqslant \ell \right\}$ modulo $h(X)$ and p with usual multiplication. Alternatively, $\mathcal{G}$ is the subgroup of $\mathbb{F}^*$ generated by the elements of the form $X+a$ for $0 \leqslant a \leqslant \ell$.

Lower Bound on the size of $\mathcal{G}$

Lemma 7 (Hendrik Lenstra Jr.)

$|\mathcal{G}| \geqslant \binom{t+\ell}{t-1}$

Lower Bound on the size of $\mathcal{G}$

Proof.

$h(X)$ is an irreducible factor of the cyclotomic polynomial $Q_r(X)$ over $\mathbb{F}_p$. So, $h(X) = 0$ in $\mathbb{F}_p[X]/(h(X)) = \mathbb{F}$, or, $Q_r(X) = 0$ in $\mathbb{F}$. Hence, X is a primitive r-th root of unity in $\mathbb{F}$ as the only roots of $Q_r(X)$ are the primitive r-th roots of unity in $\overline{\mathbb{F}_p}$.

Lower Bound on the size of $\mathcal{G}$

Proof.

We claim that distinct polynomials of degree $< t$ in P map to different elements in $\mathcal{G}$.

Let $f(X)$ and $g(X)$ be two polynomials of degree $< t$ in P. If $f(X) = g(X)$ in $\mathbb{F}$, then for any $m \in \mathbb{N}$, $[f(X)]^m = [g(X)]^m$ in $\mathbb{F}$. In particular, for any $m \in I$, $[f(X)]^m = [g(X)]^m$. As any number in I is introspective for f and g, $f(X^m) = [f(X)]^m \pmod{(X^r - 1, p)}$ and $g(X^m) = [g(X)]^m \pmod{(X^r - 1, p)}$ in $\mathbb{F}$. As $h(X)$ divides $Q_r(X)$ and $Q_r(X)$ divides $X^r - 1$, we get: $f(X^m) = g(X^m)$ in $\mathbb{F}$. As $X^r = 1$ in $\mathbb{F}$, $X^m = X^{m \bmod r}$. So, X^m is a root of the polynomial $Q(Y) := f(Y) - g(Y)$ for any $m \in G$.

Lower Bound on the size of $\mathcal{G}$

Proof.

As X is a primitive r-th root of unity in $\mathbb{F}$, $X^m \neq X^{m'}$ in $\mathbb{F}$ for distinct $m, m' \in G$. Hence, there are at least $t = |G|$ distinct roots of $Q(Y)$ in $\mathbb{F}$. However, as the degree of $Q(Y)$ is less than t, $Q(Y)$ cannot have t distinct roots in $\mathbb{F}$. Thus, we get a contradiction! Hence, $f(X) \neq g(X)$ in $\mathbb{F}$.

Lower Bound on the size of $\mathcal{G}$

Proof.

As $\gcd(r, n) = 1$, $n \in (\mathbb{Z}/r\mathbb{Z})^*$ and $\log^2(n) < o_r(n) \leqslant |(\mathbb{Z}/r\mathbb{Z})^*| = \phi(r) \leqslant r$. Now, if $1 \leqslant i \neq j \leqslant \ell$, then $i \neq j$ in $\mathbb{F}_p$, since $\ell = \lfloor \sqrt{\phi(r)\log(n)} \rfloor \leqslant \sqrt{r}\log(n) < r < p$. So, the elements X, $X+1, X+2, ..., X+\ell$ are distinct in $\mathbb{F}$. Also, since degree of h is > 1, $X + a \neq 0$ in $\mathbb{F}$ for every a, $0 \leqslant a \leqslant \ell$. So there exist at least $\ell + 1$ distinct polynomials of degree 1 in $\mathcal{G}$.

Lower Bound on the size of $\mathcal{G}$

Proof.

We want to find no. of distinct polynomials of degree $< t$ in $P = \left\{\prod_{a=0}^{\ell}(X+a)^{e_a} : e_a \geqslant 0\right\}$. Call this number N_P. N_P is same as the no. of ways, we can choose e_a's with $e_a \geqslant 0$ and $\sum_{0 \leqslant a \leqslant \ell} e_a \leqslant t-1$.

Lower Bound on the size of $\mathcal{G}$

Proof.

We want to find no. of distinct polynomials of degree $< t$ in $P = \left\{\prod_{a=0}^{\ell}(X+a)^{e_a} : e_a \geqslant 0\right\}$. Call this number N_P. N_P is same as the no. of ways, we can choose e_a's with $e_a \geqslant 0$ and $\sum_{0\leqslant a\leqslant \ell} e_a \leqslant t-1$.

Take $(t-1)$ identical balls and $(\ell+1)$ identical sticks. Arrange them in a row. Let e_0 be the no. of balls, that are on the left of first stick. Let e_1 be the no. of balls between the first stick and the second stick. ... Let e_ℓ be the no. of balls between the ℓ-th stick and $(\ell+1)$-th stick. Thus, there is a one-to-one correspondence between such permutations and polynomials of degree $< t$ in P. Hence, $N_P = \frac{(t-1+\ell+1)!}{(t-1)!(\ell+1)!} = \binom{t+\ell}{t-1}$. Therefore, there exist at least $\binom{t+\ell}{t-1}$ distinct polynomials of degree $< t$ in $\mathcal{G}$. □

Upper bound on the size of $\mathcal{G}$

Lemma 8

If n is not a power of p, then $|\mathcal{G}| \leqslant n^{\sqrt{t}}$.

Proof.

Consider the set

$$J = \left\{ \left(\frac{n}{p}\right)^i \cdot p^j : 0 \leqslant i, j \leqslant \lfloor \sqrt{t} \rfloor \right\}.$$

J is a subset of I. Now, if $\left(\frac{n}{p}\right)^{i_1} \cdot p^{j_1} = \left(\frac{n}{p}\right)^{i_2} \cdot p^{j_2}$ for $(i_1, j_1) \neq (i_2, j_2)$, then $n^{i_1 - i_2} = p^{j_2 - j_1 - i_2 + i_1}$. So, n will be a power of p. Hence, if n is not a power of p, then the set J has $(\lfloor \sqrt{t} \rfloor + 1)^2 > t$ distinct elements.

Upper bound on the size of $\mathcal{G}$

Lemma 8

If n is not a power of p, then $|\mathcal{G}| \leqslant n^{\sqrt{t}}$.

Proof.

As $|G| = t$, at least two numbers in J must be equal in G. Let m_1 and m_2 be two such numbers in J. Then $m_1 = m_2 \pmod{r}$. Without loss of generality, $m_1 > m_2$. Note that $X^{m_1} - X^{m_2} = X^{m_2}(X^{m_1 - m_2} - 1)$. So,

$$X^{m_1} = X^{m_2} \pmod{X^r - 1}.$$

Hence, for any polynomial f, $f\left(X^{m_1}\right) = f\left(X^{m_2}\right) \pmod{X^r - 1}$.

Upper bound on the size of $\mathcal{G}$

Lemma 8

If n is not a power of p, then $|\mathcal{G}| \leqslant n^{\sqrt{t}}$.

Proof.

For any polynomial f, $f\left(X^{m_1}\right) = f\left(X^{m_2}\right) \pmod{X^r - 1}$. Let $f(X) \in P$. Then

$$\begin{aligned}
[f(X)]^{m_1} &= f\left(X^{m_1}\right) \pmod{(X^r - 1), p} \\
&= f\left(X^{m_2}\right) \pmod{(X^r - 1), p} \\
&= [f(X)]^{m_2} \pmod{(X^r - 1), p}.
\end{aligned}$$

Thus, $[f(X)]^{m_1} = [f(X)]^{m_2}$ in the field $\mathbb{F}$. In other words, $f(X) \in \mathcal{G}$ is a root of the polynomial $Q(Y) := Y^{m_1} - Y^{m_2}$ in the field $\mathbb{F}$.

Upper bound on the size of $\mathcal{G}$

Lemma 8

If n is not a power of p, then $|\mathcal{G}| \leqslant n^{\sqrt{t}}$.

Proof.

If $f(X)$ is a polynomial in $\mathcal{G}$, $[f(X)]^{m_1} = [f(X)]^{m_2}$ in the field $\mathbb{F}$. In other words, $f(X) \in \mathcal{G}$ is a root of the polynomial $Q(Y) := Y^{m_1} - Y^{m_2}$ in the field $\mathbb{F}$. This is true for any polynomial $f(X) \in \mathcal{G}$. So, $Q(Y)$ has at least $|\mathcal{G}|$ distinct roots in $\mathbb{F}$. As the degree of $Q(Y)$ is $m_1 \leqslant \left(\frac{n}{p}\right)^{\sqrt{t}} \cdot p^{\sqrt{t}} = n^{\sqrt{t}}$.

This shows $|\mathcal{G}| \leqslant n^{\sqrt{t}}$. □

Proof of Correctness of AKS Algorithm

Input: n (an integer > 1)

1. If ($n = a^b$ for some $a \in \mathbb{N}$ and $b > 1$), output COMPOSITE;
2. Find the smallest r such that $\mathrm{o}_r(n) > \log^2(n)$.
3. If $1 < \gcd(a, n) < n$ for some $a \in \mathbb{N}$ with $1 \leqslant a \leqslant r$, output COMPOSITE;
4. If $n \leqslant r$, output PRIME;
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;

We proved that if n is prime, then AKS algorithm returns PRIME. We also noted that if for some input n, the algorithm returns PRIME in step 4, then n is prime. To complete the proof, we need to prove that if for some input n, the algorithm returns PRIME in step 6, then n is prime. We assumed that this was the case to define and study the groups G and $\mathcal{G}$. As the algorithm did not return COMPOSITE in step 1, n is not a non-trivial power of p. If $n \neq p^1$, then n is not a power of p and we can apply Lemma 8.

Proof of Correctness of AKS Algorithm

Lemma 9

If AKS algorithm returns PRIME in step 6 for some input n, then n is prime.

Proof of Correctness of AKS Algorithm

Proof.

For $t = |G|$ and $\ell = \lfloor \sqrt{\phi(r)}\log(n) \rfloor$, we have $\phi(r) \geqslant t > \log^2(n)$, $r \geqslant \phi(r) > \log^2(n)$, $\ell \leqslant \sqrt{r}\log(n) < r$ and $\ell \geqslant \lfloor \sqrt{t}\log(n) \rfloor$. Now, Lemma 7 gives

$$
\begin{aligned}
|\mathcal{G}| &\geqslant \binom{t+\ell}{t-1} = \binom{t+\ell}{\ell+1} \\
&\geqslant \binom{\ell+1+\lfloor \sqrt{t}\log(n) \rfloor}{\lfloor \sqrt{t}\log(n) \rfloor} \text{ (since } t > \sqrt{t}\log(n)) \\
&\geqslant \binom{2\lfloor \sqrt{t}\log(n)1 \rfloor + 1}{\lfloor \sqrt{t}\log(n) \rfloor} \text{ (since } \ell \geqslant \lfloor \sqrt{t}\log(n) \rfloor)
\end{aligned}
$$

Proof of Correctness of AKS Algorithm

Proof.

Now, note that for $m \geqslant 2$, $\binom{2m+1}{m} = \frac{(2m+1)(2m)...(m+2)}{m(m-1)...1} = \frac{2m+1}{m} \cdot \frac{2m}{m-1} \cdot ... \cdot \frac{m+2}{1} > 2^{m+1}$. As AKS algorithm returns PRIME for $n = 2, 3$, we can consider $n \geqslant 4$. Then $\lfloor \sqrt{t} \log(n) \rfloor \geqslant \lfloor \log^2(n) \rfloor \geqslant 2$. Hence, we have

$$|\mathcal{G}| \geqslant \binom{2\lfloor \sqrt{t} \log(n) 1 \rfloor + 1}{\lfloor \sqrt{t} \log(n) \rfloor} \geqslant 2^{\lfloor \sqrt{t} \log(n) \rfloor + 1} > n^{\sqrt{t}}.$$

But if n is not a power of p, from Lemma 8, $|\mathcal{G}| \leqslant n^{\sqrt{t}}$. So, $n = p^1 = p$ is prime. □

Theorem 5

For input n, AKS algorithm returns PRIME if and only if n is prime.

Running Time of AKS Algorithm

Before finding the running time of AKS algorithm, note that for two m bit numbers,

1. addition can be performed in time $\mathrm{O}(m) = \widetilde{\mathrm{O}}(m)$ time. (schoolbook addition)
2. multiplication can be performed in time $\mathrm{O}(m \log(m)) = \widetilde{\mathrm{O}}(m)$ (Harvey-Hoeven algorithm)
3. division can be performed in time $\mathrm{O}(m \log(m)) = \widetilde{\mathrm{O}}(m)$ (Newton-Raphson division with Harvey-Hoeven algorithm used for multiplication)

Running Time of AKS Algorithm

Before finding the running time of AKS algorithm, note that for two m bit numbers,

1. addition can be performed in time $\mathrm{O}(m) = \widetilde{\mathrm{O}}(m)$ time. (schoolbook addition)
2. multiplication can be performed in time $\mathrm{O}(m \log(m)) = \widetilde{\mathrm{O}}(m)$ (Harvey-Hoeven algorithm)
3. division can be performed in time $\mathrm{O}(m \log(m)) = \widetilde{\mathrm{O}}(m)$ (Newton-Raphson division with Harvey-Hoeven algorithm used for multiplication)

The same operations for two polynomials of degree $\leqslant d$ with coefficients having m bits can be performed in time $\widetilde{\mathrm{O}}(d \cdot m)$.

Running Time of AKS Algorithm

Input: n (an integer > 1)

1. If ($n = a^b$ for some $a \in \mathbb{N}$ and $b > 1$), output COMPOSITE;
2. Find the smallest r such that $\mathrm{o}_r(n) > \log^2(n)$.
3. If $1 < \gcd(a, n) < n$ for some $a \in \mathbb{N}$ with $1 \leqslant a \leqslant r$, output COMPOSITE;
4. If $n \leqslant r$, output PRIME;
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;

Theorem 6

The time complexity of AKS algorithm is $\tilde{O}(\log^{21/2}(n))$.

Running Time of AKS Algorithm

Input: n **(an integer** > 1**)**

1. **If** ($n = a^b$ **for some** $a \in \mathbb{N}$ **and** $b > 1$), **output COMPOSITE;**

Proof.

The first step of the algorithm takes time $\tilde{O}(\log^3(n))$ [If $n = a^b$ for some $a, b \geqslant 2$, then $b \leqslant \log(n)$. Hence, for $b = 2, 3, ..., \lfloor \log(n) \rfloor$, use binary search to see if there is $a > 1$ with $n = a^b$.]

Running Time of AKS Algorithm

Input: n **(an integer** > 1**)**

2. **Find the smallest** r **such that** $\mathrm{o}_r(n) > \log^2(n)$.

Proof.

In step 2, the algorithm needs to find an r with $\mathrm{o}_r(n) > \log^2(n)$. This can be done by considering $1, 2, 3, \ldots$ sequentially and checking if r takes that value by testing if $\gcd(n, r) = 1$ and if $n^k \neq 1 \pmod{r}$ for every $1 \leqslant k \leqslant \log^2(n)$. For a fixed r, this amounts to computing at most $\mathrm{O}(\log^2(n))$ multiplications modulo r. So, for a fixed r, it will take at most $\widetilde{\mathrm{O}}(\log^2(n)\log(r))$ time. From Lemma 4, there exists an $r \leqslant 3\log^5(n)$ with $\mathrm{o}_r(n) > \log^2(n)$. So, it is sufficient to check first $3\log^5(n)$ numbers for finding the desired r. Hence, overall it will take time $\widetilde{\mathrm{O}}(\log^2(n)\log(\log^5(n))\log^5(n)) = \widetilde{\mathrm{O}}(\log^7(n))$.

Running Time of AKS Algorithm

Input: n **(an integer** > 1**)**

3. **If** $1 < \gcd(a, n) < n$ **for some** $a \in \mathbb{N}$ **with** $1 \leqslant a \leqslant r$**, output COMPOSITE;**

Proof.

The third step requires computing gcd of r pairs of numbers. Each gcd computation takes time at most $\mathrm{O}(\log^2(n))$ (Euclidean algorithm). So, the time complexity of this step is $\mathrm{O}(r \log^2(n)) = \mathrm{O}(\log^7(n))$.

Running Time of AKS Algorithm

Input: n **(an integer** > 1**)**

4. **If** $n \leqslant r$**, output PRIME;**

Proof.

The time complexity of step 4 is $\mathrm{O}(\log(n))$.

Running Time of AKS Algorithm

Input: n **(an integer** > 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;

Proof.

In step 5, the algorithm verifies at most $\lfloor \sqrt{\phi(r)} \log(n) \rfloor$ equations. Verifying each equation requires $\mathrm{O}(\log(n))$ multiplications of polynomials of degree $\leqslant r$ with coefficients having $\leqslant \log(n) + 1$ bits and then taking each product modulo $X^r - 1$ and n. So, each equation can be verified in time $\widetilde{\mathrm{O}}(r \log^2(n))$ steps. Thus the time complexity of step 5 is $\widetilde{\mathrm{O}}(r \log^2(n) \sqrt{\phi(r)} \log(n)) = \widetilde{\mathrm{O}}(r^{3/2} \log^3(n)) = \widetilde{\mathrm{O}}(\log^{21/2}(n))$ as $r \leqslant 3 \log^5(n)$. □

Improving Time Complexity Bound of AKS Algorithm

If either of Artin's conjecture or Sophie-Germain Prime Density Conjecture is true, then the time complexity of AKS algorithm can be shown to be $\widetilde{\mathrm{O}}(\log^6(n))$.

Improving Time Complexity Bound of AKS Algorithm

If either of Artin's conjecture or Sophie-Germain Prime Density Conjecture is true, then the time complexity of AKS algorithm can be shown to be $\widetilde{\mathrm{O}}(\log^6(n))$.
Although Sophie-Germain Prime Density Conjecture has not been proved, a related result was proved by Goldfeld and was later improved by Fouvry. Fouvry's result gives time complexity $\widetilde{\mathrm{O}}(\log^{15/2}(n))$ for AKS algorithm.

Improving Time Complexity Bound of AKS Algorithm

If either of Artin's conjecture or Sophie-Germain Prime Density Conjecture is true, then the time complexity of AKS algorithm can be shown to be $\widetilde{\mathrm{O}}(\log^6(n))$.

Although Sophie-Germain Prime Density Conjecture has not been proved, a related result was proved by Goldfeld and was later improved by Fouvry. Fouvry's result gives time complexity $\widetilde{\mathrm{O}}(\log^{15/2}(n))$ for AKS algorithm.

Lenstra and Pomerance later gave a modified version of AKS algorithm, that runs in time $\widetilde{\mathrm{O}}(\log^6(n))$ unconditionally.

References

1. Agrawal, M., Kayal, N., & Saxena, N. (2002). Primes is in P. Annals of Mathematics 160. 781-793.
2. Agrawal, M., Kayal, N., & Saxena, N. Primes is in P. Updated version.
3. https://terrytao.wordpress.com/2009/08/11/the-aks-primality-test/
4. https://en.wikipedia.org/wiki/Computational_complexity_of_mathematical_operations

Thank You!

Appendix A: Proof of LCM Lemma

Lemma 2

Let $LCM(N) := \text{lcm}(1, 2, ..., N)$ be the least common multiple of first N natural numbers. Then for $N \geqslant 7$, $LCM(N) \geqslant 2^N$.

Appendix A: Proof of LCM Lemma

Lemma 2

Let $LCM(N) := \text{lcm}(1, 2, ..., N)$ be the least common multiple of first N natural numbers. Then for $N \geqslant 7$, $LCM(N) \geqslant 2^N$.

Proof.

The result holds for $N = 7, 8$. Assume $N \geqslant 9$.

Appendix A: Proof of LCM Lemma

Lemma 2

Let $LCM(N) := \mathrm{lcm}(1, 2, ..., N)$ be the least common multiple of first N natural numbers. Then for $N \geqslant 7$, $LCM(N) \geqslant 2^N$.

Proof.

The result holds for $N = 7, 8$. Assume $N \geqslant 9$. For $1 \leqslant m \leqslant n$, consider the integral $I_{m,n} = \int_0^1 x^{m-1}(1-x)^{n-m} = \sum_{r=0}^{n-m}(-1)^r \binom{n-m}{r} \frac{1}{m+r}$. Also, from beta function, $I_{m,n} = \frac{1}{m\binom{n}{m}}$. As $LCM(n)I_{m,n} \in \mathbb{Z}$, $m\binom{n}{m}$ divides $LCM(n)$.

Appendix A: Proof of LCM Lemma

Lemma 2

Let $LCM(N) := \text{lcm}(1, 2, ..., N)$ *be the least common multiple of first* N *natural numbers. Then for* $N \geqslant 7$, $LCM(N) \geqslant 2^N$.

Proof.

The result holds for $N = 7, 8$. Assume $N \geqslant 9$. For $1 \leqslant m \leqslant n$, consider the integral $I_{m,n} = \int_0^1 x^{m-1}(1-x)^{n-m} = \sum_{r=0}^{n-m}(-1)^r \binom{n-m}{r} \frac{1}{m+r}$. Also, from beta function, $I_{m,n} = \frac{1}{m\binom{n}{m}}$. As $LCM(n)I_{m,n} \in \mathbb{Z}$, $m\binom{n}{m}$ divides $LCM(n)$. So, $n\binom{2n}{n}$ and $(2n+1)\binom{2n}{n} = (n+1)\binom{2n+1}{n+1}$ both divides $LCM(2n+1)$. So, $LCM(2n+1) \geqslant n(2n+1)\binom{2n}{n} \geqslant n4^n \geqslant 2^{2n+2}$ for $n \geqslant 4$. □

Appendix B: Cyclotomic Polynomials over Finite Field

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

Appendix B: Cyclotomic Polynomials over Finite Field

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

1. $Q_r(X) \in \mathbb{F}_q[X]$.

Proof Sketch.

Let $\tilde{Q}_r(X)$ be the r-th cyclotomic polynomial over $\mathbb{Q}$. From Algebra II, we know that $\tilde{Q}_r(X) \in \mathbb{Z}[X]$ and has degree $\phi(r)$. Consider $\tilde{Q}_r(X)$ in $\mathbb{F}[X]$. Note that $\tilde{Q}_r(X)$ divides $X^r - 1$ and hence, is separable. As $X^r - 1 = \prod_{d|r} \tilde{Q}_d(X)$, any root of $\tilde{Q}_r(X)$ is a primitive r-th root of unity. Conversely, for a primitive r-th root $\xi \in \overline{\mathbb{F}_q}$, ξ is a root of $X^r - 1$ but for any $1 \leqslant d < r$, ξ is not a root of $\tilde{Q}_d(X)$ (as it divides $X^d - 1$). So, ξ is a root of $\tilde{Q}_r(X)$. Hence, $\tilde{Q}_r(X) = Q_r(X)$. □

Appendix B: Cyclotomic Polynomials over Finite Field

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

2. $Q_r(X)$ divides $X^r - 1$ in $\mathbb{F}_q[X]$.

Follows from the proof of (1).

Appendix B: Cyclotomic Polynomials over Finite Field

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

3. Degree of $Q_r(X)$ is $\phi(r)$.

Follows from the proof of (1).

Appendix B: Cyclotomic Polynomials over Finite Field

Let $\mathbb{F}_q$ be a finite field with characteristic p and let r be a natural not divisible by p. Let the r-th cyclotomic polynomial over $\mathbb{F}_q(X)$ be $Q_r(X)$.

4. $Q_r(X)$ factors into irreducible factors of degree $\mathrm{o}_r(q)$ in $\mathbb{F}_q[X]$.

Proof Sketch.

If $\xi \in \overline{\mathbb{F}_q}$ be a root of $Q_r(X)$, the order of ξ in the multiplicative group $\mathbb{F}_q^*$ is r. Note that if $[\mathbb{F}_q(\xi) : \mathbb{F}_q] = s$, then $\mathbb{F}_q(\xi)$ has q^s elements. As $\mathbb{F}_q(\xi)^*$ is a multiplicative group, $\xi^{q^s-1} = 1$. Conversely, the roots of the polynomial $X^{q^{s'}-1} - 1 = 0$ are precisely the non-zero elements of $\mathbb{F}_{q^{s'}}$. So, $[\mathbb{F}_q(\xi) : \mathbb{F}_q]$ is the smallest natural number s for which $X^{q^s-1}-1 = 0$. Alternatively, it is the smallest natural number s for which $q^s - 1 = 0 \pmod{r}$. So, $[\mathbb{F}_q(\xi) : \mathbb{F}_q] = \mathrm{o}_r(q)$. □