Testing Primality

A prime number N has no other divisors except 1 & N

Sieve of Eratosthenes

2

1) 2 \times N (2 does not divide N)
   Eliminate all other multiples of 2

3

3 \times N \rightarrow Eliminate all multiples of 3

If we want to test if N is prime
   find the prime factors of N

Algorithm 1(N)

\[ \text{for } x = 2, 3, 4, \ldots, N-1 \]
\[ \text{if } x \divides N \text{ then } \text{not prime} \]
\[ \text{N is a prime} \]

Complexity: \( O(N) \) : \( \frac{N}{2} \) times, the for loop execute \( \sqrt{N} \) times
Complexity: $O(N)$: # of times the test loop execute each division take $O(n^2)$ time

$n$ # of bits

$N = \frac{\log N}{2}$

$N = O(2^n)$

$O(2^n) \times O(n^2)$

Exponential time algorithm!

Algorithm $A(n)$

for $x = 2, 3, \ldots, \sqrt{N}$

check if $x | N$.

$O(\sqrt{N}) \times O(n^2)$

$O(2^{\frac{n}{2}}) \times O(n^2)$

$O(2^{\frac{2n}{2}})$

Prime mod 6 test $(N)$

Test integers between 2 and \( \sqrt{N} \)

mod 6 \{ 0, 1, 2, 3, 4, 5 \} \leftarrow \text{class}

Any integer can be written as $x = 6q + r$

\{ $6q + 0$, $6q + 1$, $6q + 2$, $6q + 3$, $6q + 4$, $6q + 5$ \}

$1 \div N$, $3 \div N$
If $2 \mid N$, $3 \nmid N$,

for testing primality we need to consider only integers of the form

1) $6q + 1$
2) $6q + 5$ or $6q - 1$

Then we have cut down the check by $\frac{2}{3}$

$\text{Alg } 3(N)$

Check $\frac{N}{3}$ N, return False

$\text{for } q = 1 \text{ to } \frac{N}{2}$

$x = 6q + 1$
$x' = 6q - 1$

if $x \mid N$ then False

if $x' \mid N$ then False

return true

$O\left(\frac{\sqrt{N}}{6}\right) \times O(n^2)$

$O\left(\frac{2^{n/2}}{6}\right) \times O(n^2) = O\left(2^{n/2} \times n^2\right)$

format's little theorem

\begin{align*}
100 \\
2, 3, 5, 7, 11, 13, 17 \\
10x < 100
\end{align*}
If \( N \) is prime, then for all \( 1 \leq a \leq N - 1 \)

\[
a^{N-1} \equiv 1 \mod N
\]

\(\mathcal{MSY}(N) :\)

for all \( a = 2, 3, 4, \ldots, N - 1 \)

\[
a^{N-1} \mod N \neq 1 \implies \text{false}
\]

\[
O(N), O(n^3)
\]

\[
\equiv O(2^\cdot n^2)
\]

Randomized primality testing

\(\rightarrow\) If \( N \) is prime

\[P(Yes) = 1\]

\(\rightarrow\) If \( N \) is not prime

\[P(Yes) \leq \frac{1}{2}\]

In \( k \) independent trials

\[
\left( \frac{1}{2} \right) \left( \frac{1}{2} \right) \cdots \left( \frac{1}{2} \right) \leq \frac{1}{2^k}
\]

If \( N \) is really prime, we always get the correct answer

If \( N \) is composite (not prime), and \( \varepsilon \) making a mistake

In \( k \) independent trials
we can choose $k=1000$ and $k=10000$

$$P(\text{mismatch}) \leq \frac{1}{2^k} \text{ or } \frac{1}{2^{10000}}$$

$$\text{IsPrime-One}(N)$$

$$\begin{cases} \text{select } a \text{ at random in the range } [2, N-1] \\
\text{Compute } \text{val} = a^{N-1} \mod N \\
\text{If } \text{val} = 1 \\
\quad \text{return True (Is prime)} \\
\text{else} \\
\quad \text{return False (not prime)} \end{cases}$$

Prove that $P(\text{mismatch}) \leq \frac{1}{2}$

$$\text{IsPrime-K}(N, k)$$

Repeat IsPrime-One $k$ times $\leftarrow P(\text{mismatch}) \leq \left(\frac{1}{2}\right)^k$

$O(k \cdot N^3) = O(N^3)$

$N = 2$

$k = 10000 \leftarrow \text{constant}$

Polytime primality testing!

Fermat's Little Theorem

If $N$ is prime, then for all $1 \leq a \leq N-1$

$$a^{N-1} \equiv 1 \mod N$$

all such $a$ are relatively prime.
\[ A^{N-1} \equiv 1 \pmod{N} \]

**Proof:**

Approach 1:

We know that \( a \) is relatively prime to \( N \) if \( \gcd(a, N) = 1 \).

\[ a^{N-1} \cdot a \equiv 1 \cdot a \pmod{N} \]

\[ a^N \equiv a \pmod{N} \]

We have to show that \( N \mid a^N - a \). Show this!

Approach 2:

Let \( \mathbb{Z}_N^+ = \{ 1, 2, 3, \ldots, N-1 \} \) be the positive remainders modulo \( N \).

Pick any \( a \in \mathbb{Z}_N^+ \).

Let \( a \cdot \mathbb{Z}_N^+ = \{ 1.a, 2.a, 3.a, \ldots, N-1.a \} \).

For example, if \( N = 5 \):

\[ \mathbb{Z}_5^+ = \{ 1, 2, 3, 4 \} \]

\[ 2 \cdot \mathbb{Z}_5^+ = \{ 2, 4, 1, 3 \} = \{ 2 \cdot 1, 2 \cdot 2, 2 \cdot 3, 2 \cdot 4 \} \pmod{5} \]

\[ a \cdot \mathbb{Z}_N^+ = \mathbb{Z}_N^+ \]

We get the same numbers, but simply permuted.

\[ \mathbb{Z}_{N-1}^+ = \{ 1, 2, 3, \ldots, N-1 \} \]
\[ Z^+_N = \{ 1, 2, 3, \ldots, N-1 \} \]

Can this happen \[ a \cdot i \equiv a \cdot j \mod N \] for \( i \neq j \)?

Assume that \( i \neq j \)

\[ \text{If } a \cdot i \equiv a \cdot j \mod N \quad \text{then } a, N \text{ are relatively prime} \]

\[ i \equiv j \mod N \]

\[ 1 \times 2 \times 3 \times \ldots \times N-1 = \frac{(a \cdot 1) \times (a \cdot 2) \times \cdots \times (a \cdot N)}{(N-1)!} \]

\[ \frac{(N-1)!}{a} = \frac{N!}{a \cdot (N-1)!} \mod N \]

Divide by \((N-1)!\) on both sides

\[ 1 \equiv a^{N-1} \mod N \]

\[ a^{N-1} \equiv 1 \mod N \]

Randomized Algorithms

\[ \rightarrow \text{ how to bound the probability of error} \]

\[ \text{IsPrime One (N)} \]

Pick a \( a \) at random \( 2, \ldots, N-1 \)
If \( a^{N-1} \equiv 1 \pmod{N} \) return true
otherwise return false

\[
\text{Prob: } \ Pr(b \mid N, \alpha) \leq \frac{1}{2}
\]
\[
\text{Prob (calling } N \text{ a prime when } N \text{ is composite)} \leq \frac{1}{2}
\]

\[
\text{If } a \text{ is relatively prime to } N \text{, and } a^{N-1} \not\equiv 1 \pmod{N}
\]

then for all \( b \in \{1, \ldots, N-1\} \) such that \( b^{N-1} \equiv 1 \pmod{N} \)

it's true that

\[
(a \cdot b)^{N-1} \not\equiv 1 \pmod{N}
\]

If \( N \) is not prime
we may find \( b^{N-1} \equiv 1 \pmod{N} \)
then we have a pair

\[
(a \cdot b)^{N-1} \not\equiv 1 \pmod{N}
\]

\[
\Rightarrow \text{ at most } \frac{1}{2} \text{ the values in the range } [1, 2, \ldots, N-1] \text{ can pass the } \alpha \text{ prime test.}
\]

\[
\text{Prob} \leq \frac{1}{2}
\]
$\exists x \in \mathbb{N}$

$b^{n-1} \equiv 1 \pmod{N}$

$(a \cdot b)^{n-1} = (a^{n-1})(b^{n-1}) \pmod{N}$

$\rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \equiv 1 \pmod{N}$

Carmichael Numbers: Very rare

Composites numbers (not prime)

$\forall a \text{ relatively prime to } N$

$a^{N-1} \equiv 1 \pmod{N}$

for Carmichael $\not\in \left(\frac{1}{2}\right)$

Is prime has to modified
to get it work for all numbers