CSC006P1M: Design and Analysis of Algorithms
Lecture 11 *(Primality Testing)*

Sumit Kumar Pandey

September 13, 2022

Primality Testing

Given a positive integer $n > 1$, check whether n is a prime or not?

Divisors of a Prime

A prime has only two divisors - 1 and itself.

Check the divisibility of n from 2 to $n - 1$.

Primality Testing

IsPrimeV1(n)

Input: n (a positive integer greater than 1)
Output: B (bool: True if prime else False)

```
begin
    B := True
    for i := 2 to n − 1 do
        if i divides n then
            B := False;
            break;
end
```

$T(n) = ?.$
$T_b(n) = 1.$
$T_w(n) = n - 2.$
$T(n) = O(n).$

Can we do better?

Yes

We do not need to check till $n-2$. It is enough to check till $\lfloor n/2 \rfloor$.

IsPrimeV2(n)

Input: n (a positive integer greater than 1)

Output: B (bool: True if prime else False)

```
begin
    B := True
    for i := 2 to ⌊n/2⌋ do
        if i divides n then
            B := False;
            break;
end
```

$T(n) = O(n)$.

Primality Testing

Can we do better?

Yes

We do not need to check till $\lfloor n/2 \rfloor$. It is enough to check till $\lfloor \sqrt{n} \rfloor$.

Reason:

- Let $n = ab$ where $1 < a \leq b < n$.
- If $a > \sqrt{n}, b > \sqrt{n}$, then $n = ab > \sqrt{n}\sqrt{n} = n$, a contradiction.

IsPrimeV3(n)

Input: n (a positive integer greater than 1)
Output: B (bool: True if prime else False)
```
begin
    B := True
    for i := 2 to ⌊√n⌋ do
        if i divides n then
            B := False;
            break;
end
```
$T(n) = O(\sqrt{n})$.

Can we do better?

Yes

AKS Algorithm.

Agrawal, Manindra; **Kayal**, Neeraj; **Saxena**, Nitin (2004). "PRIMES is in P". Annals of Mathematics. 160(2): 781–793. doi:10.4007/annals.2004.160.781. JSTOR 3597229

$T_{AKS}(n) = \tilde{O}(\lg^{15/2} n)$, where $g(n) = \tilde{O}(f(n))$ if $g(n) = O(f(n) \lg^k f(n))$ for some $k \geq 0$.

Primality Testing

AKS algorithm is a remarkable achievement. However, in practice, we do not use this one for primality testing. Instead, we choose probabilistic (randomized) algorithms like Solovay-Strassen or Miller-Rabin.

In practice, probabilistic algorithms like Solovay-Strassen or Miller-Rabin perform better than the deterministic AKS algorithm.

But, there is a chance of error with the probabilistic algorithms.

Fermat's Little Theorem

Let p be a prime number. Suppose $\gcd(a, p) = 1$. Then, $a^{p-1} \equiv 1 \mod p$.

IsPrimeV4(n)

Input: n (a positive integer greater than 1)
Output: B (bool: True if prime else False)
begin
  $B :=$ False
  Choose a random integer a, $1 \leq a \leq n-1$;
  $b := a^{n-1} \mod n$;
  if $b \equiv 1 \mod n$ then $B :=$ True;
end

Carmichael Numbers

Let n be an odd composite number. If $a^{n-1} \equiv 1 \mod n$ for all a such that $\gcd(a, n) = 1$, then n is called Carmichael numbers.

- The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$.
- Carmichael numbers are extremely rare, but it is known that there are infinitely many of them.

Carmichael Numbers

Theorem

A Carmichael number n is of the form $n = p_1 \cdots p_r$, where the p_i are distinct primes, $r \geq 3$, and $(p_i - 1) \mid (n - 1)$ for $i = 1, \cdots, r$.

Let

$$L_n = \{\alpha \mid 1 \leq \alpha \leq n-1 \text{ and } \alpha^{n-1} = 1\}.$$

Theorem

If n is prime, then $L_n = \mathbb{Z}_n^*$. If n is composite and $L_n \subsetneq \mathbb{Z}_n^*$, then $|L_n| \leq (n-1)/2$.

$\mathbb{Z}_n^* = \{a \mid 1 \leq a \leq n-1 \text{ and } \gcd(a, n) = 1\}.$

Carmichael Numbers

If n is a Carmichael number, $L_n = \mathbb{Z}_n^*$.

Primality Testing

Theorem

If n is prime, then $L_n = \mathbb{Z}_n^*$. If n is composite and $L_n \subsetneq \mathbb{Z}_n^*$, then $|L_n| \leq (n-1)/2$.

Proof:

- If n is prime, then $L_n = \mathbb{Z}_n^*$ (from Fermat's Little Theorem).
- L_n is a subgroup of $\mathbb{Z}_n^*$.
- So, $|L_n|$ divides $|\mathbb{Z}_n^*|$ and hence $|\mathbb{Z}_n^*| = m|L_n|$ for some $m \geq 1$.
- If $L_n \subsetneq \mathbb{Z}_n^*$, then $m \geq 2$.
- Thus, $|L_n| \leq (n-1)/2$.

Theorem

If n is prime, then $L_n = \mathbb{Z}_n^*$. If n is composite and $L_n \subsetneq \mathbb{Z}_n^*$, then $|L_n| \leq (n-1)/2$.

Error Probability

If n is not a Carmichael number, then the error probability of the algorithm IsPrimeV4 is $\leq 1/2$.

Can we get rid off Carmichael numbers?

MillerRabin(n)

Input: n (a positive integer greater than 1)
Output: B (bool: True if prime else False)
begin
    $B :=$ False
    Write $n - 1 = 2^k m$, where m is odd and $k \geq 0$;
    Choose a random integer a, $1 \leq a \leq n - 1$;
    $b := a^m \mod n$;
    if $b \equiv 1 \mod n$ then $B :=$ True;
    else
        for $i := 0$ to $k - 1$ do
            if $b \equiv -1 \mod n$ then $B :=$ True;
            else $b := b^2 \mod n$;
end

The Miller-Rabin Algorithm

The Miller-Rabin algorithm for **composites** is a **yes**-biased algorithm.

The Error Probability

The error probability can be shown to be at most $1/4$.

$T(n) = O(\lg n)$ (if we consider the cost of multiplication is c (a constant)), otherwise
$T(n) = O(\lg^3 n)$.

Thank You