An Algorithmic Analysis of Several Primality Tests

Isaac Stallcup

December 3, 2017

1 Introduction

Primality testing algorithms:

1. Wilson's Theorem (known to perform very poorly): An integer $p > 1$ is prime $\iff$ $(p-1)! \equiv -1 \mod p$ [2].

2. Pseudoprimality test: An integer $p > 1$ is prime $\iff$ $\forall a \not\equiv 0 \mod p, a^{p-1} \equiv 1 \mod p$ [2].

3. Miller-Rabin: Given an integer $n \geq 5$, output either `True` or `False`. If the result is `True`, n is "probably prime", and if the result is `False` n is definitely composite [2]. The algorithm has the following steps.

   (a) Compute the unique integers m and k such that m is odd and $n - 1 = 2^k * m$.

   (b) Choose some random a with $1 < a < n$.

   (c) Set $b \equiv a^m \mod n$. If $b \equiv \pm 1 \mod n$, return `True`.

   (d) If $b^{2^r} \equiv -1 \mod n$ for any $1 \leq r \leq k-1$, return `True`. Otherwise return `False`.

4. AKS Primality test [1]. This algorithm returns `False` if an integer $n > 1$ is composite, and `True` if it is prime.

   (a) If $(n = a^b$ for $a \in \mathbb{N}$ and $b > 1 \in \mathbb{N}$, return `False`.

   (b) Find the smallest r such that the order of $n \mod r > (\log_2 n)^2$.

   (c) Two mini-versions:
   If $1 < \gcd(a, n) < n$ for some $a \leq r$, return `False`; OR
   For all $2 \leq a \leq \min(r, n-1)$, check that a does not divide n; if $a|n$ for some $2 \leq a \leq \min(r, n-1)$, output `False`

   (d) If $n \leq r$, return `True`.

   (e) For $a = 1$ to $\lfloor \sqrt{\phi(r)} log_2 n \rfloor$ do
   if $((X + a)^n \neq X^n + a \mod \gcd(X^r - 1, n)$ return `False`

   (f) Return `True`

Pseudocodes:

1. Wilson's primality test Inputs: $p > 1$ Outputs: `True` if p is prime; otherwise `False`.

```
function wilson_primality_test(p)
    if (mod((p-1)!,p) == -1):
        return True
    else:
        return False
```

2. Exhaustive pseudoprimality test Inputs: $p > 1$ Outputs: `True` if p is prime; otherwise `False`.

```
function exh_primality_test(p)
    a = 1
    while (a ≠ 0 mod p):
        if (mod(a^{p-1},p) != 1):
            return False
        a = a  +1
    return True
```

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in p. *Annals of mathematics*, pages 781–793, 2004.

[2] William Stein. *Elementary number theory: Primes, congruences, and secrets: A computational approach.* Springer Science & Business Media, 2008.