

Efficient Primality Tests

Lars Reimers

its103503

Table of Contents

- Definition Prime/Coprime
- Complexity Classes
- Trivial Tests
- Miller-Rabin Test
- Shor's Algorithm
- Fermat's Little Theorem
- Agrawal-Kayal-Saxena Test

Definition Prime

*Let $p \in \mathbb{N}, p > 1$, then p is prime if
 $\forall n, n \in \mathbb{N}, n > 1, n < p : n \nmid p$*

Definition Coprime

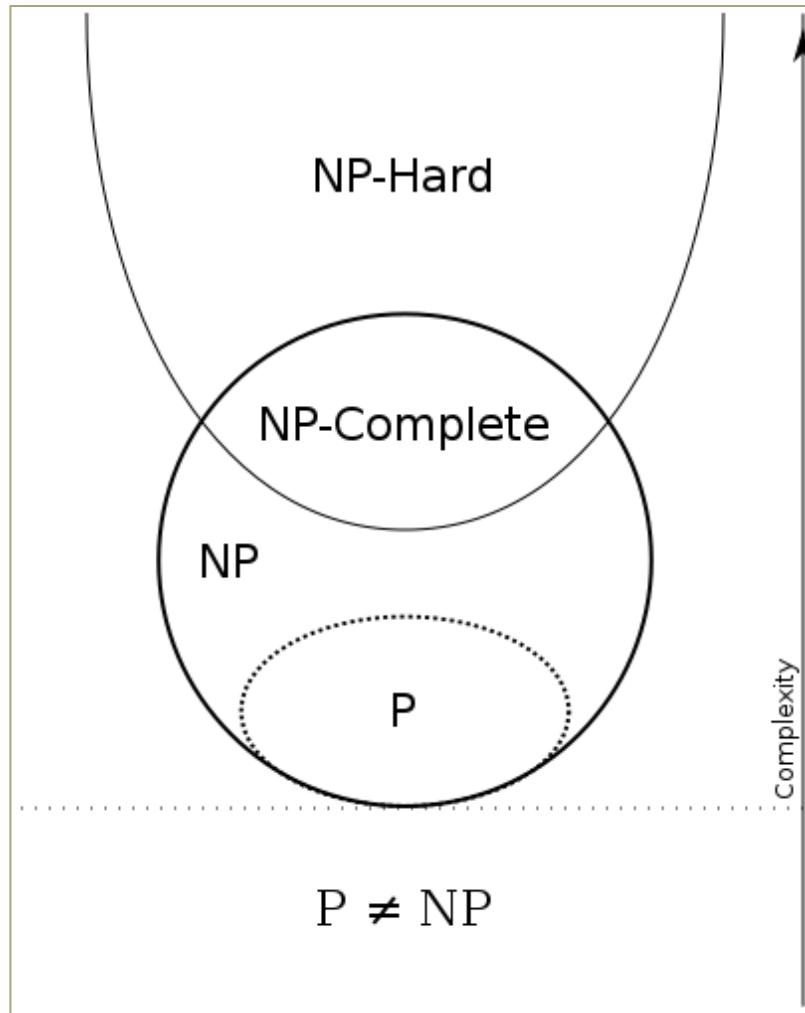
Let $p, q \in \mathbb{N}, p, q > 1$, then p is coprime to q if
 $\gcd(p, q) = 1$
also: $(p, q) = 1$

Complexity Classes

Time Complexity	Big O Notation	Example
constant time	$O(1)$	first item of a list
linear time	$O(n)$	$\min()$ of a list
polynomial time	$O(n^k)$	primality test
exponential time	$O(2^{p(n)})$	many games e.g. go
factorial time	$O(n!)$	traveling salesman

Name	Description	Example
P	polynomial time	primality test
NP	nondeterministic p. time	find a hamiltonian cycle
NP-hard	at least as hard as the hardest problem in NP	halting problem
NP-complete	intersection NP/NP-hard	find a hamiltonian cycle

Complexity Classes



Complexity Classes

Soft O

$$\tilde{O}(g(n)) = O(g(n) * \log^k g(n)) \text{ for some } k$$

Trivial Tests

```
def wilsonsTheorem(number):
    result = 1
    for i in range(number)[2:]:
        result *= i

    if result % number == -1:
```

```
benchmark()
```

```
wilsonsTheorem needed 0:00:00.000008 to determine that 17 is a prime (15 mul, 1 div, 0 root)
wilsonsTheorem needed 0:00:00.013335 to determine that 7919 is a prime (7917 mul, 1 div, 0 root)
wilsonsTheorem needed 0:00:00.055681 to determine that 16127 is a prime (16125 mul, 1 div, 0 root)
wilsonsTheorem needed 0:00:03.167039 to determine that 112909 is a prime (112907 mul, 1 div, 0 root)

-----
simplestPrimalityTest needed 0:00:00.010773 to determine that 112909 is a prime (0 mul, 112907 div, 0 root)
simplestPrimalityTest needed 0:00:01.450846 to determine that 16769023 is a prime (0 mul, 16769021 div, 0 root)
simplestPrimalityTest needed 0:00:02.380913 to determine that 27644437 is a prime (0 mul, 27644435 div, 0 root)

-----
simplePrimalityTest needed 0:00:00.000426 to determine that 27644437 is a prime (0 mul, 5255 div, 1 root)
simplePrimalityTest needed 0:00:00.000527 to determine that 39916801 is a prime (0 mul, 6315 div, 1 root)
simplePrimalityTest needed 0:00:00.002672 to determine that 1073676287 is a prime (0 mul, 32764 div, 1 root)
```

```
roots += 1
for i in range(root)[2:]:
    divisions += 1
    if number % i == 0:
        return False, _divisions, _roots, 0
return True, _divisions, _roots, 0
```

Miller-Rabin Test

- Input: $n \geq 5$
- Pick a from $\{2, 3, \dots, n - 2\}$
- Calculate d (odd) and j such that
$$n - 1 = d * 2^j$$
- Check if

$$a^d \equiv 1 \pmod{n}$$

or

$$a^{d*2^r} \equiv -1 \pmod{n}, 0 \leq r < j$$

- If either condition is not fulfilled, n is composite
- *Strong pseudoprimes (to base a)* also fulfill these conditions
- Multiple choices for $a \Rightarrow$ higher probability of n being prime
- For $n < 318.665.857.834.031.151.167.461$ it's enough to test $a = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$

Shor's Algorithm

- Requires a quantum computer
- Formulated 1994
- Not a primality test
 - Finds prime factors of an input n
- Polynomial time
- Once scalable, modern asymmetric cryptography would break
- Information about quantum mechanics and quantum cryptography (including Shor's algorithm) can be found on Gerd Beuster's website:
<http://intern.fh-wedel.de/mitarbeiter/gb/veranstaltungsarchiv/sose-2017-seminar-it-sicherheit/>

Fermat's Little Theorem

$$a^p = a \pmod{p}, p \text{ is prime}, a \in \mathbb{Z}$$

Agrawal-Kayal-Saxena Test

- „PRIMES is in P“, 2002
- Manindra Agrawal, Neeraj Kayal, Nitin Saxena
- Indian Institute of Technology Kanpur
- First primality test in polynomial time complexity
- $\tilde{O}(\log^{\frac{21}{2}} n)$
- Improvement by Carl Pomerance and Hendrik W. Lenstra Jr.
 - $\tilde{O}(\log^6 n)$

Agrawal-Kayal-Saxena Test

Input: integer $n > 1$.

1. If $n = a^b$ for $a \in \mathbb{N}$ and $b > 1$, output COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output COMPOSITE.
4. If $n \leq r$, 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.

Agrawal-Kayal-Saxena Test

Input: integer $n > 1$.

1. If $n = a^b$ for $a \in \mathbb{N}$ and $b > 1$, output COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output COMPOSITE.
4. If $n \leq r$, 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.

$o_r(a) \Rightarrow$ smallest number k such that $a^k \equiv 1 \pmod{r}$ with $a \in \mathbb{Z}, r \in \mathbb{N}, (a, r) = 1$

$\phi(r) \Rightarrow$ number of numbers less than r that are coprime to r with $r \in \mathbb{N}$

Agrawal-Kayal-Saxena Test

- Theorem 4.1: The algorithm returns PRIME if and only if n is prime
- Lemma 4.2: If n is prime, the algorithm returns PRIME

Input: integer $n > 1$.

1. If $n = a^b$ for $a \in \mathbb{N}$ and $b > 1$, output COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output COMPOSITE.
4. If $n \leq r$, 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.

Agrawal-Kayal-Saxena Test

- For polynomial $f(X)$ and number $m \in \mathcal{N}$, m is introspective for $f(X)$ if

$$[f(X)]^m = f(X^m) (\text{mod } X^r - 1, p)$$

- If m is introspective for $f(X)$ and $g(X)$ it is also introspective for $f(X) * g(X)$

Agrawal-Kayal-Saxena Test

- $I = \left\{ \left(\frac{n}{p}\right)^i * p^j \mid i, j \geq 0 \right\}$
- $G = \text{set of all residues of numbers in } I \text{ modulo } r$
- $t = |G|$
- $P = \left\{ \prod_{a=0}^{\ell} (X + a)^{e_a} \mid e_a \geq 0 \right\}$
- $\ell = \lfloor \sqrt{\phi(r)} \log n \rfloor$
- $r^{th} \text{ cyclotomic polynomial} = \prod_{1 \leq k \leq n \text{ with } (k,n)=1} (x - e^{2i\pi \frac{k}{n}})$
- $Q_r(X) = r^{th} \text{ cyclotomic polynomial over } F_p$
- $h(x) = \text{irreducible factor of degree } o_r(n) \text{ of } Q_r(X)$
- $p = \text{prime divisor of } n$
- $\mathcal{G} = \text{set of all residues of polynomials in } P \text{ modulo } h(x) \text{ and } p$

Agrawal-Kayal-Saxena Test

- $|\mathcal{G}| \geq \binom{t+\ell}{t-1} \geq n^{\sqrt{t}}$
- $|\mathcal{G}| \leq n^{\sqrt{t}}$, if n is not a power of p
- $n = p^k, k > 0$
- If $k > 1$, step 1 returns COMPOSITE
- Otherwise $n = p \Rightarrow n$ is prime