# Primality Testing

**Theorem:** If $N$ is composite then has a divisor $a$ that satisfies

$$1 < a \leq \lfloor \sqrt{N} \rfloor.$$

## Trial Division Algorithm

```
Input N
for a from 2 to [√N] do {
    if a | N then {
        PRINT "N is composite & a is a divisor of N"
        STOP }}
PRINT "N is prime"
STOP
```

This ~~alogn~~ algorithm is _____

This means _____

The Holy Grail of Primality Testing is an algorithm that is _____.

No such algorithm has been found. The best deterministic primality test is the AKS Primality Test due to _____, _____, and _____ ( ).

This was found to be _____

In 2005, _____ and _____ gave a variant that is _____.

**Fermat's Little Theorem**
Let $p$ be prime, $a \in \mathbb{Z}$ and _____. Then
$\equiv$ (mod $p$)

**NOTE**: The converse is _____
For example _____
_____.

**Lemma** Let $p$ be _____, and $a \in \mathbb{Z}$.
If $a^2 \equiv 1 \pmod{p}$ then
$a \equiv$ _____.

**The a-Test** Let $a \in \mathbb{Z}$ with $a > 1$ be fixed.
Suppose $N$ is a positive _____
integer and $N > 1$.
Let $N - 1 =$ _____ where _____,
and assume $a <$ _____.
We say $N$ passes the a-Test if
(1)

(2)

and (3)

Theorem Let $N$ be an odd prime, and suppose $a \in \mathbb{Z}$ and $1 < a < N$.
Then $N$ _____.

Proof: Suppose $N$ is prime, odd, $a \in \mathbb{Z}$ and $1 < a < N$.

(1) Since $N$ is prime, $a < N$ we have _____.

(2)

(3) Let $N-1 = 2^r s$ where $r \geq 1$ and $s$ is odd.

Let $K = \{k \in \mathbb{Z}: \_\_\_\_\_\}$.

$K$ is nonempty since
Hence $K$ has a _____.

Case 1 $k_0 = 0$. Then

Case 2 _____. We have

Example $N = 341 = 11 \cdot 31$. Show that 341 fails the 2-test.

NOTE (1) Composite numbers which pass an a-Test are _____, but they _____.

(2) The smallest composite number that passes the 2-test is $N =$ _____.

Theorem If $2 < N <$ _____, then $N$ is prime if and only if _____

Theorem (_____
_____( ))
If ___ $< N <$ ___, then $N$ is prime if and only if it passes the a-Test for $a =$ _____

Theorem If $N <$ ____, then $N$ is prime if and only if ____.

Theorem (____, ____, and ____ ( ))
If $N <$ ____, then $N$ is prime if and only if ____

Theorem (Miller) $N$ is prime if and only if $N$ satisfies the a-Test for all
$a <$ ____.

Note $\approx$ . This yields a $O($ ) algorithm.

Theorem (Miller) If the ____ (GRH) is true, then $N$ is prime iff $N$ passes the a-Test for all

$a <$ ____.

## Generalized ~~Extended~~ Riemann Hypothesis

**Definition** Let $m$ be a positive integer. A **Dirichlet character mod $m$** is a function $\chi$: ___ $\longrightarrow$ ___ that satisfies

(1)

(2)

(3)

and (4)

**Example** Let $p$ be an odd prime and define $\chi(a) =$ { ___

Then $\chi$ is a Dirichlet character mod ___.

**Lemma** If $\chi$ is a Dirichlet character then

$\chi(1) =$ ___.

PROOF:

Exercise Find all Dirichlet characters mod 5.

**Definition** Let $\chi$ be a Dirichlet character. A **Dirichlet L-function** is defined by

$$L(s, \chi) :=$$

for

NOTE: $L(s, \chi)$ can be _____ to be _____ by analytic continuation.

What does this mean?

Let $f(z) = \sum_{n=0}^{\infty} z^n = 1 + z + z^2 + \cdots$.

Then

## The Generalized Riemann Hypothesis (GRH)

Suppose $L(s, \chi)$ is a Dirichlet $L$-function.

If $L(s, \chi) =$ ___ for ____

Then