

## 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  $\lfloor \sqrt{N} \rfloor$  do {

  if  $a \mid N$  then {

    PRINT "N is composite & a is a divisor of N"

    STOP }

PRINT "N is prime"

STOP

This ~~slow~~ 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 \_\_\_\_\_,

\_\_\_\_\_ end \_\_\_\_\_ ( )

This was found to be \_\_\_\_\_

In 2005, \_\_\_\_\_ end \_\_\_\_\_

gave a variant that is \_\_\_\_\_

Fermat's Little Theorem

Let  $p$  be prime,  $a \in \mathbb{Z}$  and  $a \not\equiv 0 \pmod{p}$ . Then  

$$a^p \equiv a \pmod{p}$$

NOTE: The converse is  $a^p \equiv a \pmod{p} \implies p \text{ is prime}$

For example  $2^4 \equiv 2 \pmod{4}$  but 4 is not prime.

Lemma Let  $p$  be prime, and  $a \in \mathbb{Z}$ .

If  $a^2 \equiv 1 \pmod{p}$  then

$$a \equiv \pm 1 \pmod{p}$$

The a-Test Let  $a \in \mathbb{Z}$  with  $a > 1$  be fixed.

Suppose  $N$  is a positive integer and  $N > 1$ .

Let  $N-1 = \prod_{i=1}^k p_i^{e_i}$  where  $p_i$  are primes,

and assume  $a < N$ .

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  $K = \{k \in \mathbb{Z} : \text{_____}\}$

$K$  is nonempty since  
 Hence  $K$  has a \_\_\_\_\_

Case 1  $k_0 = 0$ . Then

Case 2 \_\_\_\_\_ We have

(p. 6)

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  $2 < N < \dots$ , then  $N$  is prime if and only if \_\_\_\_\_.

Theorem ( \_\_\_\_\_ )

If  $2 < N < \dots$ , then  $N$  is prime if and only if it passes the  $a$ -Test for  $a =$  \_\_\_\_\_.

Theorem If  $N < \dots$ , then  $N$  is prime if and only if  $\dots$

Theorem ( $\dots$ ,  $\dots$ , and  $\dots$ )

If  $N < \dots$ , then  $N$  is prime if and only if  $\dots$

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

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

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

$a < \dots$

# Generalized

(p-7)

## The Extended Riemann Hypothesis

Definition Let  $m$  be a positive integer.

A Dirichlet character mod  $m$

is a function  $\chi: \dots \rightarrow \dots$   
that satisfies

(1)

(2)

(3)

and (4)

Example Let  $p$  be an odd prime and

define  $\chi(a) = \begin{cases} \dots \\ \dots \end{cases}$

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

Lemma If  $\chi$  is a Dirichlet character then

$\chi(1) = \dots$

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 the ----- by  
 analytic continuation.

What does this mean?

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

Then

## The Generalized Riemann Hypothesis (GRH)

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

If  $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$

Then