

# Primes

# Infinite Primes

- Proof:  
Consider a finite set of primes. Multiply these together, then add one. This number is not divisible by any of these primes. Either this number is prime or is divisible by a prime not in the finite set. Either way, there is another prime.

# The Density of Primes

- $n / (\ln(n) - 1)$

# Twin Prime Conjecture

- There are an infinite number of twin primes (primes with difference 2)
- Unproven

# Goldbach's Conjecture

- All natural numbers can be written as the sum of two primes
- Unproven

# Fermat Primality Test

**Inputs:**  $n$ : a value to test for primality;  $k$ : a parameter that determines the number of times to test for primality

**Output:** *composite* if  $n$  is composite, otherwise *probably prime*

repeat  $k$  times:

    pick  $a$  randomly in the range  $(1, n - 1]$

    if  $a^{(n-1)} \neq 1 \pmod n$ , then return *composite*

return *probably prime*

- Use Modular Exponentiation to calculate the mod
- Flaw: Carmichael Numbers

# Solovay-Strassen

```
Inputs:  $n$ , a value to test for primality;  $k$ , a parameter that determines the accuracy of the test  
Output: composite if  $n$  is composite, otherwise probably prime  
repeat  $k$  times:  
  choose  $a$  randomly in the range  $[1, n - 1]$   
   $x \leftarrow \left(\frac{a}{n}\right)$   
  if  $x = 0$  or  $a^{(n-1)/2} \not\equiv x \pmod{n}$  then return composite  
return probably prime
```

- $(a|n)$  is the Legendre Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ +1 & \text{if } a \not\equiv 0 \pmod{p} \text{ and for some integer } x, x^2 \equiv a \pmod{p} \\ -1 & \text{if there is no such } x. \end{cases}$$

# Miller-Rabin

**Input:**  $n > 2$ , an odd integer to be tested for primality;  
**Input:**  $k$ , a parameter that determines the accuracy of the test  
**Output:** *composite* if  $n$  is composite, otherwise *probably prime*  
write  $n - 1$  as  $2^s \cdot d$  with  $d$  odd by factoring powers of 2 from  $n - 1$   
LOOP: repeat  $k$  times:  
    pick  $a$  randomly in the range  $[2, n - 1]$   
     $x \leftarrow a^d \bmod n$   
    if  $x = 1$  or  $x = n - 1$  then do next LOOP  
    for  $r = 1 \dots s - 1$   
         $x \leftarrow x^2 \bmod n$   
        if  $x = 1$  then return *composite*  
        if  $x = n - 1$  then do next LOOP  
    return *composite*  
return *probably prime*

[http://en.wikipedia.org/wiki/Miller-Rabin\\_primality\\_test](http://en.wikipedia.org/wiki/Miller-Rabin_primality_test)

# Sieve of Eratosthenes

- Find primes up to  $N$
- (discussed in class first day)

# Mersenne Prime

- $M_n = 2^n - 1$
- $2^{43,112,609} - 1$  is the largest prime number known
- The exponent  $n$  must be prime
- Special Number Field Sieve is fast at checking primality for  $r^n \pm s$ , where  $r$  and  $s$  are small

# Generate Number Field Sieve (GNFS)

- The most efficient classical algorithm known for factoring integers greater than 100 digits.
- Can't factor prime powers ( $3^7$ )

[http://en.wikipedia.org/wiki/General\\_number\\_field\\_sieve](http://en.wikipedia.org/wiki/General_number_field_sieve)