# Primality tests

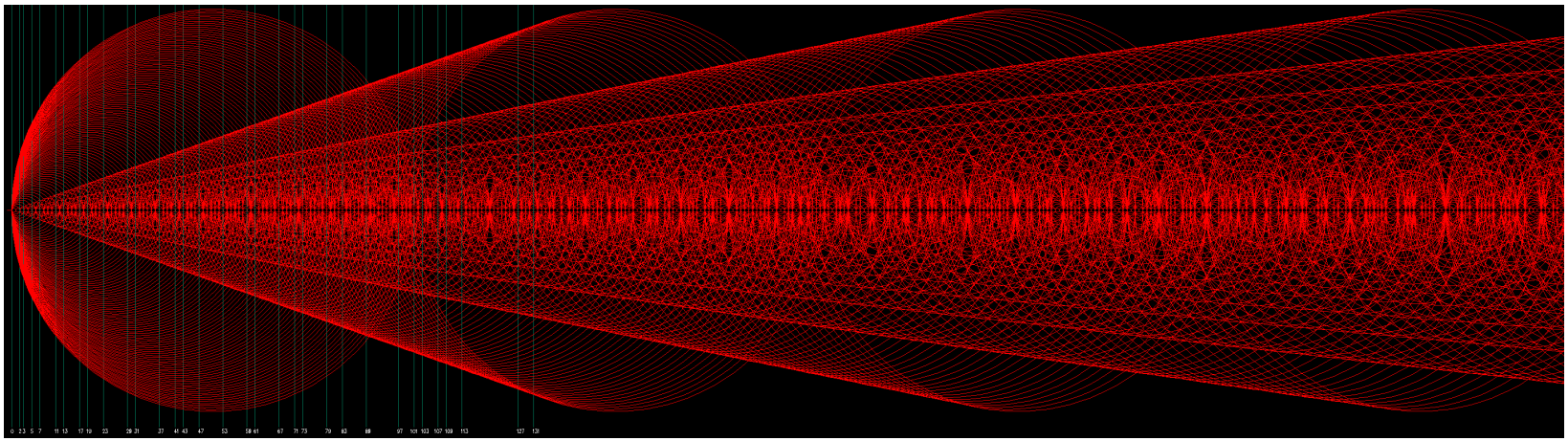
Hüseyin YAĞCI

Faculty of Engineering, Yasar University, Izmir

Number Theory Presentation

# Outline

# A short description of prime numbers



# Solovay-Strassen primality test

```
SolovayStrassen := function(n, k)
    for i := 1 to k do
        a := Random([2..(n-2)]);
        if Gcd(a, n) gt 1 then
            return n, "is composite.";
        end if;
        if Modexp(a, (n-1) div 2, n) ne JacobiSymbol(a, n) then
            return n,"is composite.";
        end if;
    end for;
    return n, "is probable prime.";
end function;
```

## Info

The algorithm returns "n is composite" with probability at least $1 - 2^{-k}$. The time complexity of the algorithm is $O((\log n)^3)$.

# Fermat's primality test

```
FermatPrimalityTest := function(n,k)
    for i := 1 to k do
        a := Random([2..(n-2)]);
        if Modexp(a, n-1, n) ne 1 then
            return n, " is composite";
        end if;
    end for;
    return n, "is maybe prime";
end function;
```

## Info

Theorem says that if $n$ is prime and $n$ does not divide the integer $a$, then $a^{n-1} \equiv 1 \pmod{n}$.

# Probable prime, Pseudo prime and Carmichael numbers

## Probable prime

An odd integer $p > 2$ is called a **probable prime to base** $a$ if $a^{p-1} \equiv 1 \pmod{p}$.

## Pseudo prime

A composite probable prime to base $a$ is called a **pseudoprime to base** $a$.

## Carmichael numbers

A **Carmichael numbers** is an odd composite positive integer which is a pseudoprime to every base.

# Euler probable prime

```
EulerPobablePrime := function(n,k)
    a := Random([2..k]);
    for i := 0 to k do
        if Gcd(a,n) gt 1 then
            return "n is composite.";
        end if;
        if Modexp(a, (n - 1) div 2, n) eq 1 then
            return "n is a Euler probable prime.";
        end if;
        if Modexp(a, (n - 1) div 2, n) eq n-1 then
            return "n is a Euler probable prime.";
        end if;
    end for;
    return "n is composite";
end function;
```

## Info

An Euler probable prime to base $a$ was defined as an integer $n$ for which $gcd(a, n) = 1$ and $a^{(n-1)/2} \equiv (a/n) \pmod{n}$. An Euler pseudoprime to base $a$ is a composite Euler probable prime to base $a$.

# Miller-Rabin primality test

```
StrongProbablePrime := function(n, a)
    nminusone := n - 1;
    counter := 0;
    while (nminusone mod 2) eq 0 do
        nminusone := nminusone div 2;
        counter := counter + 1;
    end while;
    d := (n - 1) div 2^counter ;
    if Modexp(a, d, n) eq 1 then
        return true;
    end if;
    for r := 0 to counter-1 do
        if Modexp(a, d * (2 ^ r), n) eq n-1 then
            return true;
        end if;
    end for;
    return false;
end function;

MillerRabin := function(n, k)
    for i := 1 to k do
        a := Random([2..(n - 2)]);
        if StrongProbablePrime(n, a) eq false then
            return n, "is composite";
        end if;
    end for;
    return n, "is prime";
end function;
```

## Info

The algorithm returns "n is composite" with probability at least $1 - 4^{-k}$. The time complexity of the algorithm is $O((\log n)^3)$.

# Methods of primality testing

- Method one:

```
x:= Select random big number
if probablePrime(x) eq true then
    return x,' is probable prime.';
else
    return x, ' is composite.';
```

- Method two:

```
x:= Select random big number
if probablePrime(x) eq true then
 if strongProbablePrime(x) eq true tnen
     return x,' is probable prime.';
else
    return x, ' is composite.';
```

- Method three:

```
x:= Select a number (not big)
while available
    construct(x);
```

# Th 11.1

## Theorem 11.1

Strong probable primes are Euler probable primes. Every strong probable prime is an Euler probable prime to the same base. Every strong pseudoprime is an Euler pseudoprime to the same base.

## Proof

The definition says that we will get $\pm 1$ at some step before the last step in computing $a^{n-1}$ mod $n$, and this number will be squared at least once.

# Th 11.5-7

## Theorem 11.5, Solovay - Strassen

If $n$ is an odd composite positive integer, then the number of bases $a$ in $1 \leq a < n$ with $gcd(a, n) = 1$ to which $n$ is an Euler pseudoprime is $\leq \phi(n)/2$.

## Theorem 11.7, Miller - Rabin

For each odd composite integer $n$, the number of bases to which $n$ is a strong pseudoprime is $\leq (n - 1/4)$.
For each odd composite integer $n > 9$, the number of bases to which $n$ is a strong pseudoprime is $\leq (\phi(n)/4)$.

# Th 11.5-7 Proof

## Proof, Solovay - Strassen and Miller - Rabin

For a Carmichael number $n$, group of all pseudoprime bases is all of $R_n$. One can prove that for every composite $n > 1$ there is at least one $a$ in $1 < a < n$ with $gcd(a, n) = 1$ so that $n$ is not an Euler pseudoprime to base $a$. Hence, the group of all Euler pseudoprime bases for $n$ is always a proper subgroup of $R_n$. Since the order of a subgroup divides the order of the whole group,by Lagrange's theorem, the number of Euler pseudoprime bases for $n$ must be $\leq$ half the size of $R_n$. $\leq (\phi(n)/4)$ for Th 11.7.

Thank you.