10/30/19 Class Notes

Matthew Bender

November 7, 2019

For RSA, we need big prime numbers

So we need an "is-prime" function

fermat test(n) for k from 1 to 20:

pick a random a from (2,n-1)
  compute x = a$^{n-1} \pmod n$
  $if(x \neq 1 \pmod n)$
    return **composite**
  else
    continue

return **prime**

The fermat test is a good way for checking primes, but it does have noticable problems

- lots of pseudoprimes
- carmichael numbers

To fix this, we will introduce the Solovay Strassen Test

Solovay Strassen (n):
  for k from 1 to 20
    pick a random a from (2,n-1)
    compute $x = [\frac{a}{n}]$ (Jacobi Symbol)
    compute $y = a^{(n-1)/2} \pmod n$

    if($x \not\equiv y \pmod n$)
      return **composite**
    else
      continue

  return **prime**

Example:

Test $n = 25$ using $a = 7$

Compute $[\frac{a}{n}] \Rightarrow [\frac{7}{25}] \Rightarrow [\frac{25}{7}] \Rightarrow [\frac{4}{7}] \Rightarrow [\frac{2}{7}][\frac{2}{7}] \Rightarrow (1)(1) \Rightarrow 1$

$x = 1$

Compute $y = 7^{(25-1)/2} \equiv 7^{12} \pmod{25}$

$7^2 \equiv 49 \equiv 24 \pmod{25}$

$7^4 \equiv (7^2)^2 \equiv 24^2 \equiv (-1)^2 \equiv 1 \pmod{25}$

$7^8 \equiv 1 \pmod{25}$

$7^{12} \equiv 1 \pmod{25}$

Solovay Strassen says "probably prime" because $x \equiv y$

Now pick a new a

$a = 3$

Compute $[\frac{a}{n}] \Rightarrow [\frac{3}{25}] \Rightarrow [\frac{25}{3}] \Rightarrow [\frac{1}{3}] \Rightarrow 1$

Compute $3^{(25-1)/2}$

$3^{12} \equiv 3^8 \times 3^4$

$3^2 \equiv 9 \pmod{25}$

$3^4 \equiv 9^2 \equiv 81 \equiv 6 \pmod{25}$

$3^8 \equiv (3^4)^2 \equiv 6^2 \equiv 36 \equiv 11 \pmod{25}$

$3^8 \times 3^4 \equiv 6 \times 11 \equiv 66 \equiv 16 \pmod{25}$

Solovay Strassen says 25 is composite because $1 \not\equiv 16$

There is a test that's even better than Solovay Strassen, with fewer pseudoprimes

Miller-Rabin test(n):

Write $2^k m$ [m is odd]

Pick a random a in [2, n-1] (the goal is to compute $a^{n-1} \pmod{n}$)

Step 1: compute $b_0 \equiv a^m \pmod{n}$

If $b_0 \equiv 1$ or $-1 \pmod{n}$

n is probably prime (continue)

Step 2:

for j from 1 to k-1 [k is the power from 2]

compute $b_j = b_{j-1}^2 \pmod{n}$

if $b_j \equiv 1 \pmod{n}$

return composite

if $b_j \equiv -1 \pmod{n}$

```
        say  probably prime [continue]

If we finish the loop and b_{k-1} ≢ ±1 (mod n)
   return composite
Else the number is prime
```

For Miller-Rabin, at most, 1/4 of the possible a values say **probably prime** for composite n