

## PROBLEM DOMAIN – NUMBER THEORY

### Testing for Primes:

- A pseduo-primality-test
  - Pseudo-primes: Carmichael Numbers
  - Error Bounds

# PRIMALITY TESTING – APPROACH I

## ○ Randomized Algorithms

- Need a basic test:

- **Fermat's Theorem:** *If  $n$  is a prime, then  $a^{n-1} = 1 \pmod{n}$  for any  $a$  in  $Z_n^*$ .*

- Call  $a^{n-1} = 1 \pmod{n}$  as the *Fermat congruence*

- Is the converse of Fermat's Theorem true?

- i.e. If  $n$  is not prime is it guaranteed that

- there exists  $a$  in  $Z_n^*$  such that  $a$  does not satisfy Fermat congruence ?



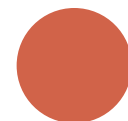
# PRIMALITY TESTING – APPROACH I

- Suppose the converse of Fermat's theorem were true.
  - Is this a randomized algorithm for primality testing?
  - $\text{prime}(n)$  {
    1. choose  $a$  in  $Z_n \setminus \{0\}$  at random;
    2. if  $(\gcd(a,n) \neq 1)$  return “composite”;
    3. if  $(a^{n-1} \bmod n == 1)$  return “prime”  
else return “composite”;}
  - It would be necessary to prove that
    - if  $a$  is in  $Z_n^*$ , then *with reasonably high probability*  $a$  fails to satisfy Fermat congruence



# PRIMALITY TESTING – CARMICHAEL NUMBERS

- The converse of Fermat's theorem is not true:
  - there exist pseudo-primes i.e. composite numbers  $n$  for which all in  $Z_n^*$  satisfy the Fermat congruence
    - These are referred to as Carmichael numbers
- Definition: Carmichael numbers:
  - A Carmichael number is a composite  $n$  such that for all  $a$  in  $Z_n^*$ ,  $a^{n-1} = 1 \pmod{n}$ 
    - e.g. 561 ( $= 3 \times 11 \times 17$ ), 1729 ( $= 7 \times 13 \times 19$ )
- Consequent questions:
  1. Can we eliminate Carmichael numbers?
  2. For non-Carmichael numbers  $n$ :
    - how dense (or sparse) is the set  $Z_n^*$  in elements  $a$  that satisfy Fermat congruence?



# PRIMALITY TESTING – APPROACH I

- The proposed algorithm (see previous slide) fails for Carmichael numbers:
  - There are an infinite number of Carmichael numbers
    - A finite elimination set – e.g. a list of Carmichael numbers computed offline - cannot be used.
  - The density of Carmichael numbers is very low
    - So, it may be within acceptable limits of error – even if all of them are not eliminated



# FERMAT CONGRUENCE

## ○ Definition $F_n$ :

- For any number  $n$ , define the set  $F_n$  of elements that satisfy Fermat Congruence

○ i.e.  $F_n = \{ a \in \mathbb{Z}_n^* \mid a^{n-1} = 1 \pmod{n} \}$

## ○ Special cases

- $F_n = \mathbb{Z}_n$  for prime  $n$ .
- $F_n = \mathbb{Z}_n^*$  for Carmichael numbers  $n$ .
- $F_n \neq \mathbb{Z}_n^*$  for other  $n$  (by elimination)



# FERMAT CONGRUENCE

## Lemma $F_n$ :

- For a composite non-Carmichael number  $n$ ,

$$|F_n| \leq (1/2) * |Z_n^*|$$

## Proof:

- Since  $n$  is not prime nor a Carmichael number  $F_n \neq Z_n^*$
- Claim:  $(F_n, *)$  is a group [Exercise: Prove this!]
- Corollary:  $(F_n, *)$  is a proper sub-group of  $(Z_n^*, *)$ 
  - [Exercise: Prove this!]
- Sub-Group Size Theorem:
  - If  $(H, .)$  is a sub-group of the group  $(G, .)$  then  $|H| \mid |G|$
- Since  $|F_n| \neq |Z_n^*|$ 
  - $|F_n| / |Z_n^*| \leq 1/2$



# A PSEUDO-PRIMALITY TEST

- This randomized algorithm

```
prime(n) {  
  choose a in  $Z_n \setminus \{0\}$  at random;  
  if (gcd(a,n)==1) {  
    if ( $a^{n-1} \bmod n == 1$ ) return "prime"  
    else return "composite"; }  
  } else return "composite";  
}
```

will err with probability  $\leq \frac{1}{2}$  for non-Carmichael  
composite numbers  $n$  (by Lemma  $F_n$ )

