CS F364
Design & Analysis of Algorithms

PROBLEM DOMAIN – NUMBER THEORY

Testing for Primes:

- A pseudo-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 $a^{n-1} = 1$ (mod 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?
  - prime(n) {
    1. choose a in $Z_n \setminus \{0\}$ at random;
    2. if (gcd(a,n)!=1) return "composite";
    3. if (a^{n-1} mod 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: *<u>Carmichael numbers</u>*:
  - 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 x 11 x 17), 1729 (= 7 x 13 x 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. $F_n = \{ a \text{ in } Z^*_n \mid a^{n-1} = 1 \pmod{n} \}$
- Special cases
  - $F_n = Z_n$ for prime n.
  - $F_n = Z^*_n$ for Carmichael numbers n.
  - $F_n \ != Z^*_n$ for other n (by elimination)

Fermat Congruence

Lemma F_n :

- For a composite non-Carmichael number n,

  $|F_n| <= (1/2) * |Z^*_n|$

Proof:

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

A Pseudo-Primality Test

- This randomized algorithm

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

will err with probability <= ½ for non-Carmichael composite numbers n (by Lemma F_n)