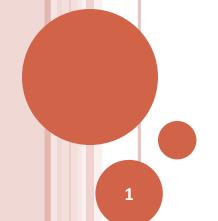
CS F364 Design & Analysis of Algorithms

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 $a^{n-1} = 1$ (mod n) for any a in Z_n^* .
 - o Call $a^{n-1} = 1 \pmod{n}$ as the Fermat congruence
 - Is the converse of Fermat's Theorem true?
 - oi.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;
 - if (gcd(a,n)!=1) return "composite";
 - if (aⁿ⁻¹ mod n == 1) return "prime"
 else return "composite";
 }
 - It would be necessary to prove that
 oif 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^* , $a^{n-1} = 1$ (mod n)
 - oe.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:
 - ohow 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