MA/CSSE 473 – Design and Analysis of Algorithms **In-class Quiz Day 10**

Name:_____Solution_____ Score:____/ 11 circle your Section # 01(3rd) 02 (4th)

1. What does Fermat's Little Theorem say about $a^{N-1} \pmod N$
   a. if N is prime? **It is 1**

   b. if N is not prime? **Theorem says nothing**

2. Outline our (Carmichael-free) primality testing algorithm

   Randomly pick k numbers, all less than N.
   For each number a, if a^{N-1} is not congruent to 1 (mod N), N is composite.
   If all of them pass, there is a high probability ($> 1 - 0.5^k$) that N is prime.

3. What is a Carmichael number, and why are such numbers troublesome for primality testing?
   A composite number N with the property that $a^{N-1} \equiv 1 \pmod N$ for all a relatively prime to N.
   They thwart the above algorithm, because of that "high probability" thing

4. Is expressing N-1 as $2^t u$ (where u is odd) an expensive operation? Explain.

   Finding t is just counting zeroes at the end of binary representation Of N.
   Finding U is just shifting N right by t bits.

5. How does the Miller-Rabin test work?

   $a^{N-1} = a^{u(2^t)} = (\ldots((a^u)^2)^2\ldots)^2$ square t times

   Look at the results along the way. If we ever get 1 (mod N) after squaring, where the previous number was neither 1 not N-1 (mod N), then we have a nontrivial square root of 1 (mod N), which implies that N is not prime.

6. Example: N = 105. N-1 = 104 = (8) (13) , sot = 3, u = 13.

   a = 8
   $a^u = 8^{13} \equiv 8 \pmod{105}$ $(a^u)^2 = 64$ $64^2 \equiv 1 \pmod{105}$, so 64 is a non-trivial square root of 1 (mod 105)

   a = 29
   $a^u = 29^{13} \equiv 29 \pmod{105}$ $29^2 \equiv 1 \pmod{105}$, so 29 is a non-trivial square root of 1 (mod 105)

7. If there is a nontrivial square root of 1 (mod N), how do we know that N is composite?
   Prove the contrapositive.
   Show that if N is prime and $s^2 \equiv 1 \pmod N$, then s must be congruent to 1 or N-1 (mod N).

   $s^2 \equiv 1 \pmod N$. Subtract 1 from both sides:
   $s^2 - 1 \equiv 0 \pmod N$. Now factor:
   $(s - 1)(s + 1) \equiv 0 \pmod N$
   N divides (s - 1) (s + 1) [definition of congruence].
   N divides (s-1) or N divides (s+1) [because N is prime]
   Either $s \equiv 1$ or $s \equiv -1 \pmod N$, so s is NOT a nontrivial square root of 1 (mod N).

8. What does Lagrange's Theorem say about $\pi(N)$, the number of primes smaller than N (for large N)?

   $\pi(N) \approx N / \ln N$.

9. What does this imply about the probability of randomly finding an n-bit prime?

If N has n bits, then the probability than N is prime is approximately $(N / \ln N)) / 2^n \approx (2^n / \ln (2^n)) / 2^n \approx 1.44 / n$

10. What became clear to you as a result of today's discussion? (or write N/A)
    Any answer is OK; must have an answer.

11. Is there anything from today's discussion that was unclear, do you have questions, or is there anything else you want to tell me? (or write N/A)

    Any answer is OK; must have an answer.