473: Instructor Notes from Day 10 slides:

Slide 4: Where are we now?

Do the test for k randomly-generated values of a < N.

Probability of error is < (1/2)^k

If k=100, dasGupta says the probability of error is less than the probability of a cosmic ray flipping some bits and messing up your computer's computation

Slide 6: The algorithm (modified)

Note that this algorithm may produce a “false prime”, but the probability is very low.

Slide 7: Miller-Rabin test

u is odd?

Or should I say "u are odd". To most of the world outside Rose-Hulman, if you would take this course or any 400-level MA/CSSE course, U must be odd!

Note that this factorization of N-1 can be fast. Just count how many bits at the end of N-1 are 0 to get t, and then bit-shift N-1 to get u.

ON BOARD: Note that aN-1 = au(2^t) =(…((au)2)2…)2 square t times

Slide 11: Example (first Carmichael number)

Work through another example with the students. N = 105.

Suppose we first try a = 8. (Use the modexp interactive program).

Enter 8, 104, 105: Get 1. So it passes the Fermat test.

What is u? (13). Do 8^13 (8), 8^26(64), 8^52 (1)

Then 29^104 = 1. 29^13 = 29, 29^26 = 1