473: Instructor Notes from Day 9 slides:

Slide 2 Day 09:

Because modular arithmetic shows up a lot of places in algorithms

In particular, in cryptography and security.

Slide 3: Extended Euclid algorithm

I got the message loud and clear from Tuesday's in-class quiz: I went too fast on modular inverse and division. We will do them again.

Slide 6: Revisit: Modular division

Theta(n^3) again. We do Euclid, followed by multiplication.

Slide 7: Recap: Fermat's Little Theorem

Why is it called "little theorem"

Because of his "last theorem", written in 1637, margin of book. Not proven until 1995.

Slide 11: How many "false positives"?

The diagram on next slide is from Dasgupta, page 26.

Last bullet if ab = ac, we can just divide by a, since gcd(a, N) = 1

Slide 14: 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