473: Instructor Notes from Day 11 slides:

Slide 4: Example (from Wikipedia)

Another example (Dasgupta p 33):

N=55 = 5*11. e = 3, d = 3-1 mod 40 = 27.

13^3 = 52 mod 55, 52^27 = 13 mod 55.

Slide 10: Proof of the property

x^(p-1) ≡ 1 (mod p), so any power of that (in particular $x^{k(p-1)(q-1)}$) ≡ 1 (mod p).

Thus $x^{1 + k(p-1)(q-1)} \equiv x$ (mod p).

Because p and q are prime, if p and q divide a number, so does pq.

Slide 11: RSA Security

We'd have to find d. This would be easy if we knew p and q, but factoring is hard.

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

Slide 12: Amortized efficiency analysis

To decrease an amount gradually or in installments, especially in order to write off an expenditure or liquidate a debt. *He obtained a mortgage with the interest payments **amortized** over the life of the loan.*

to write off a cost of (an asset) gradually.

Slide 13: Growable Array (implement ArrayList)

12+13+14+15+…+N = N(N+1)/2 – 11(12)/2 . Amortized Θ(N)

Do it only for the case

N= $12 \cdot 2^k + 1$. $12(1 + 2 + 4 + 2^k) = 12\,(2^{k+1} - 1) = 2(N-1) - 12 = 2N-14$. Amortized Θ(1)