CS / MCS 401 Week #1 Exercises

Exercise 1.2-2 (page 13).

Exercise 1-1 (page 13). Omit the first two functions, lg(*n*) and sqrt(*n*), and then fill in the 1-minute, 1-day, and 1-year columns only.

A. Show how to compute a^{109} (mod m) using 10 modular multiplications. Be sure to indicate exactly where each multiplication occurs.

B. Show how to compute a^5 (mod m) using 3 modular multiplications. Noting that $25 = 5^2$ and $125 = 5^3$, show how to compute a^{25} (mod m) using 6 modular multiplications, and then how to compute a^{125} (mod m) using 9 modular multiplications. (Your result will demonstrate that fast exponentiation algorithm given in class is not always optimal with regard to the number of multiplications.)