Quantitative Reasoning 28:
The Magic of Numbers

Homework 31

Assigned on May 4
Due at 5:00 p.m. May 6

Please submit problem sets to the boxes outside the Math Department's main office, on the third floor of the Science Center (Room 325).

Reading:

Gross-Harris, Chapter 24

Problems:

Please explain your reasoning and show your work.

1. Alice and Bob decide to use the password protocol we discussed in class. They choose $p = 59$, and 2 as a multiplicative generator (mod 59). Alice chooses $k = 13$ as her secret exponent, and so she sends Bob $2^{13} = 50$ (mod 59). Bob chooses $m = 17$ as his secret exponent, and so he sends Alice $2^{17} = 33$ (mod 59). Now, what is their password?

2. Amanda is communicating with someone she hopes is Bob. For their digital signatures, Amanda and Bob have previously chosen $p = 31$ and 3 as a multiplicative generator (mod 31) (recall from the last homework that 3 is, in fact, a generator in arithmetic (mod 31)). Amanda has 7 as her secret exponent, and thus has published 17, which is 3^7 (mod 31), as the pubic part of her signature. She also knows that Bob has previously published 4 as the public part of his signature. If Amanda now receives a message claiming to be from Bob with the signature 16, should she believe that it's actually from Bob or not?