Quantitative Reasoning 28:
The Magic of Numbers

Homework **27**

Assigned on Wednesday December 3rd
Due at 12 noon **Monday** December 8th

Please submit problem sets at the end of the relevant lecture, or leave in the box labeled QR28 outside the Math Department's main office, on the third floor of the Science Center (Room 325).

Reading:

Gross-Harris, Chapter 22

Problems:

Please explain your reasoning and show your work.

1. Alice and Bob want to securely communicate over an unsecure line. They use the following scheme to convert a message into numbers (and vice versa): each letter corresponds to a number mod $N = 143$ in the following way:

A	B	C	D	E	F	G	H	I	J	K	L	M
34	2	106	17	10	119	16	37	68	102	76	82	92

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	12	109	47	101	63	30	69	45	133	80	128	89

   Alice tells Bob that, after having translated his message into a sequence of numbers, he should then raise each of them to the 103^{rd} power (reduced mod 143). One day, Alice receives the following message from Bob:

   21, 122, 140, 17, 2, 24, 67, 122, 140.

   Let's try to decode it!

(a) We know that the first letter in the message corresponds to some number x. Because of the way that Bob used to encode the message, We know that $x^{103} \equiv 21 \pmod{143}$. Solve this for x!

(b) This should give you the first letter in the message. What is it?

(c) Now decode the rest of the message!

(Of course, in practice this would be a terrible way to encode a message! Instead of converting one letter at a time into a number mod 143, you would convert a long string of letters at a time, say a chunk of 100 letters, into a number mod some HUGE number!)

2. This is a another problem about the public-key encryption system, though here we will not deal with the encoding, and assume that people already know the meaning of certain whole numbers. We use n to stand for the encryption modulus, and k to stand for the encryption exponent.

(a) Alice wishes to send a secret message to Bob using the public-key cryptographic protocol discussed in today's lecture (and in Chapter 22 of the book). Upon request, Bob sends her $n = 143$ and $k = 17$. If Alice wants to transmit the encrypted version of the message $m = 24$, what should she send Bob?

(b) Later, Ann wants to communicate with Bob. Bob chooses $p = 11$, $q = 17$, $k = 23$. After sending Ann $n = 187$ and $k = 23$, he receives from her the number 177. What was Ann's message?

(c) Eve listens in on a communication between Bob and Amanda. She knows that Bob transmitted to Amanda $n = 2047$, $k = 125$. Amanda responded with the number 2. What was Amanda's message? (Computational hint: $2^{11} = 2048 = 1 \pmod{2047}$. Use this to your advantage.)