CS3235 Tutorial for week 4
(Aug 30-Sept 3, 2004)

August 28, 2004

1. In class, we saw that the *generators* for the table $a^n \bmod 11$ were 2, 6, 7 and 8. Find a large generator (perhaps one larger than, say, 50) a for the table $a^n \bmod 263$. Clearly show *how* you discovered/calculated the generator.
Clue: Note that $p = 263$ is a prime, and that $p = 2q + 1$ where $q = 131$ is also a prime. As a result, the prime p is commonly called a *safe* prime.

2. Explain *why* it is easy to find generators for a table modulo a *safe* prime. Can you devise a reasonable test to exclude non-generators for a non-safe prime?

3. Plot graphs of $a^n \bmod 263$ (y-axis) versus n (x-axis) for your generator, and for a non-generator (perhaps - say 52) in $a^n \bmod 131$. Compare the two graphs. Can you think of something *useful* you can do with the sequence of numbers in your generator? Can you explain why $52^n \bmod 131$ has the particular period it has?

4. Use Fermat's theorem to show the inverse of $a = 6$ and $a = 7$ in the integers modulo 35521. Describe exactly how you did this. What limits your technique?

5. Alice is going to send a message to Bob using RSA *encryption*. Bob had previously choosen some initial values $p = 71$, $q = 97$, and $E = 41$, and had then calculated $N = pq$, $x = (p-1)(q-1)$, and $D = 5081$ (which is the multiplicate inverse of E in the field Z_x). Bob publishes (gives to everybody) a key $K_{\text{Public}} = (N, E)$, but keeps private the key $K_{\text{Private}} = (N, D)$.

(a) If Alice wanted to encode the message "Hi", she might use theASCII values as integers: "H" is the integer $m_1 = 72$. "i" is the integer $m_2 = 105$. To send message m to Bob, Alice should send the value $m^E \bmod N$ (she can find out E and N because Bob has *published* them). What two values will Alice transmit to Bob? Show your working.

(b) When Bob receives the two values, he calculates $m^D \bmod N$. Show the calculation for each message.

(c) Why is this process different from other encryption processes?