18.781, Fall 2007 Problem Set 3
Due: FRIDAY, September 28

1. Complete the following problems from Niven-Zuckerman-Montgomery (henceforth NZM):

   NZM 2.3: 15, 17, 21, 29, 32, 37, 44

   NZM 2.6: 3, 4, 6, 10

2. ANOTHER CHOICE OF PARI PROGRAMS:

   - Describe your failed but clever attempts to factor the following RSA challenge number:

     ```
     RSA-704

     Prize: $30,000

     Status: Not Factored

     Decimal Digits: 212

     74037563479561712828046796097429573142593188889231
     28908493623263897276503402826627689199641962511784
     39958943305021275853701189680982867331732731089309
     00552505116877063299072396380786710086096962537934
     650563796359

     Decimal Digit Sum: 1009
     ```

     These are listed on the RSA website: http://www.rsa.com/rsalabs/node.asp?id=2092

   - Read the 2-page section 2.5 in NZM on public key cryptography, and encrypt and decrypt a short message, using primes large enough so that it isn't completely silly. I'll include a sample code in the hand-outs section of the website.