NUMBER THEORY
SPRING 2014

ASSIGNMENT 10.1
DUE APRIL 3

Exercise 1. Choose a large prime (30 to 40 digits) p, a primitive root r of p, and an exponent $a \in \{2, 3, 4, \cdots, p-2\}$. If you can, try to choose a prime no other student in the class is using. Email me your public key (p, r, b), where $b \equiv r^a \pmod{p}$, but keep a secret. I will email you back a pair (C, D) produced by ElGamal encryption with your public key. Once you receive it, decrypt this encoded message.

Exercise 2. I have chosen the public key (p, r, b), where

$$\begin{aligned} p &= 64495327731887693539738558691066839103388567300449, \\ r &= 3, \\ b &= 11027249263895705721540211643295707163844635357261. \end{aligned}$$

for ElGamal encryption. Choose an encryption exponent k (but don't tell me what it is!) and use my public key to send me an encrypted message. Since this will require you to convert a block of text to an integer, be sure to specify the way in which you made the conversion.

Exercise 3. Textbook exercise 30fgh

Exercise 4. Textbook exercise 33

Exercise 5. Textbook exercise 38