NUMBER THEORY I
SPRING 2018

ASSIGNMENT 11.3
DUE APRIL 11

Exercise 1. Textbook exercise 3.6.

Exercise 2. Koblitz exercise IV.2.2.

Exercise 3. Let's build an RSA public key cryptosystem for the class. Choose realistic values for the encryption modulus n and encryption exponent e, and (use a computer to) find the decryption exponent d. Be sure it's not easy to factor n: I'm going to try my hardest. And don't tell me d! Once I have everyone's public keys I will "publish" a directory in another exercise and ask everyone to send encrypted messages to other members of the class (we'll use Maple for that, so don't worry if your key values are enormous). Just to give you an idea of what I'm expecting, here's my public key $K_E = (e, n)$:

$$\begin{aligned} e =& 53019033612697173850452491533414032447698055458230107841213061218041808375 \\ & 34711139663693379184628822015382917615082425919046515724034632287836644106 \\ & 59268011861012084364584250814446434805321355869097 7, \\ n =& 14964162729898105788684569421835754781481603923778961041678322180333144368 \\ & 22709860751513251318961222522907372192391605917282981442924650456478290351 \\ & 82956223609793921876215420154449162261241620514094 17. \end{aligned}$$