# Math 116, Homework 1

Chi-Yun Hsu

Familiarize yourself with SageMath before you begin to do the homework. For example, you can type `ShiftCryptosystem?` to get information of the command `ShiftCryptosystem`. An example code to use the command is copied below from the information:

```
S = ShiftCryptosystem(AlphabeticStrings())
P = S.encoding("The shift cryptosystem generalizes the Caesar cipher."); P
K=7
E = S(K)
C = E(P); C
D = S(S.inverse_key(K))
P==D(C)
```

Once you press `Shift` + `Enter`, you gain the output

```
THESHIFTCRYPTOSYSTEMGENERALIZESTHECAESARCIPHER
AOLZOPMAJYFWAVZFZALTNLULYHSPGLZAOLJHLZHYJPWOLY
True
```

1. (Shift Cipher, modified 1.1)
   (a) Use `ShiftCryptosystem` by shifting 11 letters forward to encrypt

   "A page of history is worth a volume of logic"

   (b) Use `ShiftCryptosystem` by shifting 7 letters backward to decrypt

   AOLYLHYLUVZLJYLAZILAALYAOHUAOLZLJYLAZAOHALCLYFIVKFNBLZZLZ

2. (Simple Substitution Cipher, modified 1.3)
   (a) Use `SubstitutionCryptosystem` with key `SCJAXUFBQKTPRWEZHVLIGYDNMO` to encrypt

   "The gold is hidden in the garden"

   (b) Use `SubstitutionCryptosystem` with the same key to decrypt

   IBXLX JVXIZ SLLDE VAQLL DEVAU QLB

3. (Divisibility) Do problem 1.7(d), 1.8(d) using a simple calculator.
4. (Greatest Common Divisors) Do Problem 1.9(a), 1.10(a) by hand, and then check your answers using `xgcd` in SageMath.
5. Problem 1.11
6. (Modular Arithmetic) Problem 1.17(a)(c)(h), 1.18, 1.22