# Math 116 Spring 2022
# Homework 1
## Due Friday, April 8th

You should familiarize yourself with Sage before starting to do the homework. For example, you can type `help(ShiftCryptosystem)` to get the Sage documentation about `ShiftCryptosystem`.

Here is some sample code using `ShiftCryptosystem`:

```
shift_system = ShiftCryptosystem(AlphabeticStrings())
message = "The shift cryptosystem generalizes the Caeser cipher"
plaintext = shift_system.encoding(message)
print("plaintext:", plaintext)
key = 7
encode = shift_system(key)
ciphertext = encode(plaintext)
print("ciphertext:", ciphertext)
decode = shift_system(shift_system.inverse_key(key))
print("Decoding ciphertext gives plaintext?", plaintext == decode(ciphertext))
```

You can try pasting this into Sage and executing it. You should get the output:

```
plaintext: THESHIFTCRYPTOSYSTEMGENERALIZESTHECAESARCIPHER
ciphertext: AOLZOPMAJYFWAVZFZALTNLULYHSPGLZAOLJHLZHYJPWOLY
Decoding ciphertext gives plaintext? True
```

**Problem 1.** (Shift Cipher, modified 1.1, with Sage)

(a) Use `ShiftCryptosystem` to shift

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

forward by 11 letters.

(b) Use `ShiftCryptosystem` to shift 7 letters backwards to decrypt

```
AOLYLHYLUVZLJYLAZILAALYAOHUAOLZLJYLAZAOHALCLYFIVKFNBLZZLZ
```

**Problem 2.** (Simple substitution cipher, modified 1.3, with Sage)

(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
```

**Problem 3.** (Divisibility) Remark 1.9 says: "One way to compute quotients and remainders is by long division. You can speed up the process using a simple calculator. The first step is to divide $a$ by $b$ on your calculator, which will give a real number. Throw away the part after the decimal point to get the quotient $q = \lfloor a/b \rfloor$. Then the remainder $r$ can be computed as $r = a - b \cdot q$.

"If you need just the remainder, you can instead take the decimal part (also sometimes called the fractional part) of $a/b$ and multiply it by $b$."

(a) 1.7(d). Using a simple calculator and the method described in Remark 1.9, compute the quotient and remainder resulting from 1498387487 divided by 76348.

(b) 1.8(d). Using a simple calculator and the method described in Remark 1.9, compute the remainder resulting from 1498387487 divided by 76348.

**Problem 4.** (Greatest Common Divisors 1.9(a) and 1.10(a), by hand) Use the extended Euclidean algorithm by hand to compute $\gcd(291, 252)$ and to find integers $u$ and $v$ so that $291u + 252v = \gcd(291, 252)$. Check your answer in Sage with `xgcd`.

**Problem 5.** (1.11) Let $a$ and $b$ be positive integers.

(a) Suppose that there are integers $u$ and $v$ satisfying $au + bv = 1$. Prove that $\gcd(a, b) = 1$.

(b) Suppose that there are integers $u$ and $v$ satisfying $au + bv = 6$. Is it necessarily true that $\gcd(a, b) = 6$? If not, give a specific counterexample, and describe all of the possible values of $\gcd(a, b)$?

(c) Suppose that $(u_1, v_1)$ and $(u_2, v_2)$ are two solutions in integers to the equation $au + bv = 1$. Prove that $a$ divides $v_2 - v_1$ and that $b$ divides $u_2 - u_1$.

(d) Let $g = \gcd(a, b)$ and let $(u_0, v_0)$ be a solution in integers to $au + bv = g$. Prove that every other solution has the form $u = u_0 + kb/g$ and $v = v_0 - ka/g$ for some integer $k$. (This is the second part of Theorem 1.11.)

**Problem 6.** (Modular Arithmetic, by hand)

(a) 1.17(a). Find the integer $n$ between 0 and 762 such that $347 + 513 \equiv n \pmod{763}$.

(b) 1.17(c). Find the integer $n$ between 0 and 352 such that $153 \cdot 287 \equiv n \pmod{353}$.

(c) 1.17(h). Find the integer $n$ between 0 and 96 such that $23^3 \cdot 19^5 \cdot 11^5 \equiv n \pmod{97}$.

**Problem 7.** (Modular Arithmetic 1.18, by hand) Find all values of $x$ between 0 and $m - 1$ that are solutions of the following congruences.

(a) $x + 17 \equiv 23 \pmod{37}$

(b) $x + 42 \equiv 19 \pmod{51}$

(c) $x^2 \equiv 3 \pmod{11}$

(d) $x^2 \equiv 2 \pmod{13}$

(e) $x^2 \equiv 1 \pmod{8}$

(f) $x^3 - x^2 + 2x - 2 \equiv 0 \pmod{11}$

(g) $x \equiv 1 \pmod{5}$ and $x \equiv 2 \pmod{7}$ (Find all solutions with $0 \leq x < 35$.)

**Problem 8.** (Modular Arithmetic 1.22, by hand) Let $m$ be an integer.

(a) Suppose that $m$ is odd. What integer between 1 and $m-1$ is the inverse of 2 mod $m$?

(b) Suppose that $m \equiv 1 \pmod{b}$. What integer between 1 and $m-1$ is the inverse of $b$ mod $m$?