Math 116 Spring 2022
Homework 2

Due Friday, April 15th

Instructions for SageMath

You may use `factor` to check your answer to Problem 1.

You can use `k.<a> = FiniteField(p,impl='modn')` to set k to be $\mathbb{F}_p$ and a the multiplicative unit in k usually represented by the integer 1.

If $b \in \mathbb{F}_p$ then the `multiplicative_order` method of b returns the multiplicative order of b in $\mathbb{F}_p$. For example, if you want to find the multiplicative order of 2 in $\mathbb{F}_7$, then

```
k.<a> = FiniteField(7, impl='modn')
(2*a).multiplicative_order()
```

Here we write `(2*a)` to cooerce 2 into an element of $\mathbb{F}_7$. This can be used to check your answer to Problem 4.

The `log` method of b returns an integer x such that $m = b^x \pmod p$. For example, if you want to find the discrete logarithm $\log_3(5)$ in $\mathbb{F}_7$, then use the code

```
k.<a> = FiniteField(7, impl='modn')
(5*a).log(3)
```

This can be used to check your answer for Problem 7, and is needed for Problem 8.

An aside on syntax for people with Python experience

You may be upset that `k.<a> = blah` is not syntactically valid Python. Sage uses an IPython input transformation hook which rewrites

```
x.<y, z, w> = blah
```

into the syntactically valid Python code

```
x = blah; (y, z, w) = x._first_ngens(3))
```

If you are ever confused by the creepy IPython input rewrite hooks, my suggestion is to intentionally force a syntax error. The syntax error will show the rewritten code. For instance typing `726 +` results in the syntax error:

```
    Integer(726) +
                  ^
SyntaxError: invalid syntax
```

we see that Sage wrapped 726 with `Integer`. Likewise `726.2 +` results in:

```
    RealNumber("726.2") +
                         ^
SyntaxError: invalid syntax
```

This can make it a lot easier to understand what is going on.

Primes and Finite Fields

Problem 1. (1.30(c), by hand) Compute $\text{ord}_p(46375)$ for p equal to 3, 5, 7, and 11.

Problem 2. (1.31) Let p be a prime number. Prove that ord_p has the following properties.

(a) $\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b)$. (Thus ord_p resembles the logarithm function, since it converts multiplication into addition!)

(b) $\text{ord}_p(a + b) \geq \min\{\text{ord}_p(a), \text{ord}_p(b)\}$.

(c) If $\text{ord}_p(a) \neq \text{ord}_p(b)$, then $\text{ord}_p(a + b) = \min\{\text{ord}_p(a), \text{ord}_p(b)\}$.

A function satisfying these properties is called a valuation.

Problem 3. (1.32(a), by hand) Let $p = 47$ and let $a = 11$. Compute $a^{-1} \mod p$ in two ways:

(a) Use the extended Euclidean algorithm.

(b) Use the fast power algorithm and Fermat's little theorem.

Problem 4. (1.34, by hand) Recall that g is called a primitive root modulo p if the powers of g give all nonzero elements of $\mathbb{F}_p$.

(a) For which of the following is 2 a primitive root mod p?
(i) $p = 7$ (ii) $p = 13$ (iii) $p = 19$ (iv) $p = 23$

(b) Find a primitive root for $p = 29$ and for $p = 41$.

(c) Find all primitive roots modulo 11. Verify that there are exactly $\phi(10)$ of them, as asserted in Remark 1.32.

Symmetric Ciphers

Problem 5. (1.43(a)(c), by hand (you can use Sage for `xgcd`)) This problem is about the affine cipher. The affine cipher has key given by a pair of integers $k = (k_1, k_2)$. The encryption and decryption functions are given by

$$e_k(m) \equiv k_1 \cdot m + k_2 \pmod{p}, \quad \text{and} \quad d_k(c) \equiv k_1^{-1} \cdot (c - k_2) \pmod{p}.$$

(a) Let $p = 541$ and let the key be $k = (34, 71)$. Encrypt the message $m = 204$. Decrypt the ciphertext $c = 431$.

(b) Alice and Bob decide to use the prime $p = 601$ for their affine cipher. The value of p is public knowledge, and Eve intercepts the ciphertexts $c_1 = 324$ and $c_2 = 381$ and also manages to find out that the corresponding plaintexts are $m_1 = 387$ and $m_2 = 491$. Determine the private key and then use it to encrypt the message $m_3 = 173$.

Problem 6. (1.44(a)(c)) Consider the Hill cipher, defined by the same equations as the affine cipher except where now m, c, and k_2 are vectors of dimension n and k_1 is an $n \times n$ matrix.

(a) Let $p = 7$, $k_1 = \begin{smallmatrix} 1 & 3 \\ 2 & 2 \end{smallmatrix}$ and $k_2 = \left(\begin{smallmatrix} 5 \\ 4 \end{smallmatrix}\right)$.

  (i) Encrypt $m = \left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right)$.

  (ii) What is the matrix k^{-1} used for decryption?

  (iii) Decrypt the message $c = \left(\begin{smallmatrix} 3 \\ 5 \end{smallmatrix}\right)$?

(b) The following plaintext/ciphertext pairs were generated using a Hill cipher with the prime $p = 11$. Find the keys k_1 and k_2.

$$m_1 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}, \quad c_1 = \begin{pmatrix} 1 \\ 8 \end{pmatrix}, \quad m_2 = \begin{pmatrix} 8 \\ 10 \end{pmatrix}, \quad c_2 = \begin{pmatrix} 8 \\ 5 \end{pmatrix}, \quad m_3 = \begin{pmatrix} 7 \\ 1 \end{pmatrix}, \quad c_3 = \begin{pmatrix} 8 \\ 7 \end{pmatrix},$$

Diffie–Hellman

Problem 7. (2.4(a), by hand) Solve the congruence $2^x \equiv 13 \pmod{23}$.

Problem 8. (2.6, with sage) Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for a Diffie–Hellman key exchange. Alice sends Bob the value $A = 974$. Bob asks your assistance, so you tell him to use the secret exponent $b = 871$. What value B should Bob send to Alice, and what is their secret shared value? Can you figure out Alice's secret exponent?

Problem 9. (2.7) Let p be a prime and let g be an integer. The *Decision Diffie–Hellman Problem* is as follows. Suppose you are given three numbers A, B, and C. Suppose that

$$A \equiv g^a \pmod{p} \qquad \text{and} \qquad B \equiv g^b \pmod{p}$$

but you do not know a and b. The goal is to determine whether $C = g^{ab} \pmod{p}$.

(a) Prove that an algorithm to solve Diffie–Hellman can be used to solve Decision Diffie-Hellman.

(b) Do you think that the decision Diffie–Hellman problem is hard or easy? Why? See Exercise 6.40 for a related example in which the decision problem is easy, but it is believed that the associated computational problem is hard.