**Project GF2**

**This is an individual project and you are required to work on this project alone. The total of this project is 100 points.**

***Specifications:***

In this project you are required to write the java program “GF2.java” to implement the second type of finite field GF(*pn*) where *p* is a prime number and *n* is a positive integer, and four operations “+”, “−”, “\*”, and “/”, respectively.

Specifically, your program will read parameters and polynomials from a file named “input.txt” (under the same directory of the program). Then your program should create a file named “output.txt” (under the same directory of the program) and write the results to “output.txt”. Please check the attached sample files “input.txt” and “output.txt”.

In “input.txt”:

1. First line is the prime number *p*.
2. Second line is the degree *n* of the irreducible polynomial *m*(*x*) over Z*p*.
3. Third line is the coefficients of *m*(*x*), from the leading coefficient to the constant, separated by one blank space.
4. Fourth line is the degree of *f*(*x*) over Z*p*.
5. Fifth line is the coefficients of *f*(*x*), from the leading coefficient to the constant, separated by one blank space.
6. Sixth line is the degree of *g*(*x*) over Z*p*.
7. Seventh line is the coefficients of *g*(*x*), from the leading coefficient to the constant, separated by one blank space.

In “output.txt”:

1. First line is the coefficients of *f*(*x*) + *g*(*x*) in GF(*pn*), from the leading coefficient to the constant, separated by one blank space.
2. Second line is the coefficients of *f*(*x*) − *g*(*x*) in GF(*pn*), from the leading coefficient to the constant, separated by one blank space.
3. Third line is the coefficients of *f*(*x*) \* *g*(*x*) in GF(*pn*), from the leading coefficient to the constant, separated by one blank space.
4. Fourth line is the coefficients of *f*(*x*) / *g*(*x*) in GF(*pn*), from the leading coefficient to the constant, separated by one blank space (don’t forget to handle the case of *g*(*x*) = 0).

Remark: The leading coefficient should not be 0 unless the polynomial is 0.

Example 1: Let *p* = 3, *m*(*x*) = *x*2 + 1, *f*(*x*) = 2*x*, *g*(*x*) = *x* + 1, then *f*(*x*) + *g*(*x*) = 1 instead of 0*x* + 1. Thus the first line of “output.txt” should be 1 instead of 0 1.

Example 2: Let *p* = 3, *m*(*x*) = *x*2 + 1, *f*(*x*) = 2*x* + 2, *g*(*x*) = *x* + 1, then *f*(*x*) + *g*(*x*) = 0 instead of 0*x* + 0. Thus the first line of “output.txt” should be 0 instead of 0 0.

***Submission and Testing:***

You are required to submit a single java file “GF2.java” to blackboard. It will be tested using command line. First,

“javac GF2.java”

will be entered to the command line to compile it, and then

“java GF2”

will be entered to the command line to run it.

The files “GF2.java” and “input.txt” will be placed under the same directory. Your program should output the file “output.txt” to the same directory. Be certain that your program compiles and runs correctly before you submit it!