Directions:

- Complete the exercises below and either write up or type up your solutions. Solutions must be submitted as PDF or Word documents, uploaded to the appropriate assignment area on Blackboard.
- If you choose to submit handwritten work, it must be neat and legible; if you do your handwritten work on paper, it must be **scanned to a PDF file** and submitted to Blackboard. Instructions and practice for scanning work to PDFs is given in the Startup Assignment. **Do not just take a picture, and do not submit a graphics file (JPG, PNG, etc.)** — such submissions will not be graded.
- Your work will be graded using the EMPX rubric and evaluated **not just on the basis of a right or wrong answer, but on the quality, completeness, and clarity of your work**. Therefore you need to show all work and explain your reasoning on each item.
- Every item must have a good-faith effort at a complete and correct response. If any item is left blank, or shows minimal effort (such as answering "I don't know"), or is significantly incomplete, the entire assignment will be graded "X" (Not Assessable) and you will have to spend a token to revise it.

---

1. A **Gaussian integer** is a complex number whose real and imaginary parts are both integers. The set of Gaussian integers is usually denoted $\mathbb{Z}[i]$, so the definition is:

$$\mathbb{Z}[i] = \{a + bi \ : \ a, b \in \mathbb{Z}\}$$

For example, $3 - i \in \mathbb{Z}[i]$ but $\frac{1}{2} + 2i \notin \mathbb{Z}[i]$. (Why?) We can make $\mathbb{Z}[i]$ into a number system by defining addition and multiplication to be the same operations we use for ordinary complex numbers.

(a) Prove that $\mathbb{Z}[i]$ is closed under addition and multiplication.

(b) Explain why the following properties hold in $\mathbb{Z}[i]$: addition is associative, multiplication is associative, addition is commutative, multiplication is commutative, and multiplication distributes over addition. **NOTE WELL: This can be done without lengthy computational proofs!** You can explain why all of these properties hold in just 1-3 sentences with virtually no computation if you think about the properties of $\mathbb{C}$.

(c) Does $\mathbb{Z}[i]$ have an additive identity? If so, what is it? Prove that you're correct.

(d) Does $\mathbb{Z}[i]$ have a multiplicative identity? If so, what is it? Prove that you're correct.

(e) Does every element of $\mathbb{Z}[i]$ have an additive inverse? Give either a proof or a specific counterexample. (Remember, the additive inverse of an element in $\mathbb{Z}[i]$ must be another element of $\mathbb{Z}[i]$ — especially, we need to be sure the real and imaginary parts are integers.)

(f) Does every nonzero element of $\mathbb{Z}[i]$ have a multiplicative inverse? Give either a proof or a specific counterexample. (Remember, the multiplicative inverse of an element in $\mathbb{Z}[i]$ must be another element of $\mathbb{Z}[i]$ — especially, we need to be sure the real and imaginary parts are integers.)

2. It's possible not only to examine "number" systems on their own, but also to **combine** systems. For example we can look at the set of 2×2 matrices with entries that are something other than real numbers! Define the following set:

$$M_{2\times2}(\mathbb{Z}_2) = \left\{ \begin{pmatrix} [a] & [b] \\ [c] & [d] \end{pmatrix} \ : \ [a], [b], [c], [d] \in \mathbb{Z}_2 \right\}$$

So, these are 2×2 matrices whose entries aren't numbers at all, but classes from $\mathbb{Z}_2 = \{[0], [1]\}$. We define addition of these matrices to be regular matrix addition (add corresponding entries) but then the "addition" inside the matrices is addition from $\mathbb{Z}_2$. We can define multiplication similarly: multiply two matrices in $M_{2\times2}(\mathbb{Z}_2)$ by multiplying them like you normally would, but then any arithmetic on the individual entries is done in $\mathbb{Z}_2$.

(a) How many matrices are in $M_{2\times2}(\mathbb{Z}_2)$? Explain. (Spoiler: It's a finite set.)

(b) Compute the sum and show your work:

$$\begin{pmatrix} [1] & [1] \\ [1] & [0] \end{pmatrix} + \begin{pmatrix} [0] & [1] \\ [0] & [1] \end{pmatrix}$$

(c) Compute the products and show your work:

$$\begin{pmatrix} [1] & [1] \\ [1] & [0] \end{pmatrix} \cdot \begin{pmatrix} [0] & [1] \\ [0] & [1] \end{pmatrix} \text{ and } \begin{pmatrix} [0] & [1] \\ [0] & [1] \end{pmatrix} \cdot \begin{pmatrix} [1] & [1] \\ [1] & [0] \end{pmatrix}$$

(d) Is multiplication in $M_{2\times2}(\mathbb{Z}_2)$ commutative? Give either a proof or a specific counterexample.

(e) What other properties from The Big Table in class seem to be satisfied by $M_{2\times2}(\mathbb{Z}_2)$? Are there any that definitely are false? For those that appear to be true, give a reason (not necessarily a proof; just looking for your thoughts here). For any that are false, give a counterexample.