PRINT NAME: _____.

MATH 423:	HOMEWORK: PRELIMINARIES AND GROUPS ASSIGNMENT

Show **your** work carefully. Use full sentences, proper grammar and be precise. You don't have to copy the problem statement again, but, your solution must be self-contained. 60pts to earn here. Notice the order of the problem generally follows the videos which you are intended to watch. Please note there are ideas in the videos which I hope you learn even though there are not homework problems directly linked. I do not collect enough homework in this course to comprehensively cover all the concepts which comprise the course. It is important for you to watch, study and seek out additional questions as needed.

Problem 1: Use the Euclidean Algorithm to calculate $gcd(513, 187)$ and express $gcd(513, 187)$ as a $\mathbb{Z}$-linear combination of 513 and 187.
Remark: When I made the video which is given in the Week 1 videos I had not yet learned the easier *vector Euclidean Algorithm*, you might find the first about 8 minutes of this video from my 2021 number theory course helpful.

Problem 2: Use proof by mathematical induction to prove that

$$1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$$

for all $n \in \mathbb{N}$.

Problem 3: Let $n > 0$ be an integer. Let $a \in \mathbb{Z}$, define $[a]_n = \{a + nk \mid k \in \mathbb{Z}\}$. Use the definition given here to prove the following: if there exist $a, a', b, b' \in \mathbb{Z}$ such that $[a]_n = [a']_n$ and $[b]_n = [b']_n$ then $[a + b]_n = [a' + b']_n$ and $[ab]_n = [a'b']_n$.

Problem 4: Select Cayley Tables. Using the explicit notation given below:

(a.) Make addition and multiplication tables for $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$.

(b.) Make multiplication table for $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

Remark: *you can appreciate from (a.) why we use the notation in (b.) going forward when there is no danger of confusion. Generally, we use the notation $a = [a]_n$ when there is no danger of confusion. That said, beware there are problems where $[a]_n$ is a must. Part of this course is learning to understand which notation is appropriate.*

Problem 5: Let us use homework to introduct a formula for the inverse of a 2×2 matrix with entries in $\mathbb{Z}_n$: if $a, b, c, d \in \mathbb{Z}_n$ and $\gcd(n, ad - bc) = 1$ then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

where $(ad-bc)^{-1}$ is the multiplicative inverse of $ad-bc$ in $\mathbb{Z}_n$. Note, if $\gcd(n, ad-bc) \neq 1$ then $(ad - bc)^{-1}$ does not exist and the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is likewise not invertible. For example, in $\mathbb{Z}_{10}$ we have $3^{-1} = 7$ since $3(7) = 21 = 1$. We do **not** write $3^{-1} = 1/3$ in this context. The notation $1/3$ is not used in the context of modular arithmetic. Calculate the inverse of the following matrices if possible, if not explain why,

(a.) $\begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix}$ with entries from $\mathbb{Z}_{10}$,

(b.) $\begin{bmatrix} 2 & 2 \\ 1 & 4 \end{bmatrix}$ with entries from $\mathbb{Z}_{12}$,

Problem 6: Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 7 & 5 & 1 & 8 & 2 & 3 \end{pmatrix}$. Find the following:

(a.) a disjoint cycle factorization of σ,

(b.) write σ as a product of transpositions, is σ even or odd?

(c.) a disjoint cycle factorization of σ^{-1}

(d.) find the order of σ.

Problem 7: Use cycle notation for S_7, let $\sigma = (1356)$ and $\tau = (12)(3547)$. Calculate:

(a.) $\sigma\tau$,

(b.) $\tau\sigma$,

(c.) $\tau^2\sigma$

(d.) $\sigma\tau\sigma^{-1}$

Problem 8: Chapter 5, Exercise # 3 (permutation calculation)

Problem 9: Chapter 5, Exercise # 8 (permutation calculation)

Problem 10: Write each theorem and major definition which was given in video 4 of Week 1.

Problem 11: Chapter 2, Exercise # 25 (characterization of abelian group)

Problem 12: Chapter 2, Exercise # 46 (verify given set and operation form group)