Math 103A, Fall 2019

Modern Algebra I, HW 0

Not to be handed in. For your personal use only. Will not be graded.

Problem A. Let $a, b \in \mathbb{Z}$ be two integers. Recall that a divides b if one can write $b = qa$ for some $q \in \mathbb{Z}$. When that happens the notation we use is $a|b$. Prove the following two properties, for any three $a, b, c \in \mathbb{Z}$:

(a) $a|a$.

(b) $a|b \wedge b|c \Longrightarrow a|c$.

Suppose $a|b$ and $b|a$. Can one deduce that $a = b$? What if a, b are both nonzero?

Problem B. Given $a, b \in \mathbb{Z}$ with $a > 0$, there are uniquely determined $q, r \in \mathbb{Z}$ such that the following two conditions are satisfied simultaneously:

(i) $b = qa + r$,

(ii) $0 \leq r < a$.

(This is called "division with remainder".)

(a) Let $a = 17$ and $b = 2019$. Find the corresponding pair q, r.

(b) In general, suppose d is a common divisor of a and b. That is $d|a$ and $d|b$. Deduce that $d|r$.

(c) Use the observation in part (b) to find the greatest common divisor of 143 and 221. Then write it in the form

$$\text{GCD}(143, 221) = 143x + 221y$$

for suitable integer coefficients $x, y \in \mathbb{Z}$. ("Euclid's Algorithm".)

Problem C. A prime number is an integer $p > 1$ whose only positive divisors are 1 and p.

(a) List all the prime numbers less than 20.

(b) Factor 60 as a product of prime numbers.

(c) Is there an $n > 1$ such that $4^n - 1$ is a prime number?

Problem D. For any positive integer $n \in \mathbb{N}$ and any real number $x \neq 1$ the following very useful formula holds:

$$1 + x + x^2 + x^3 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}. \tag{1}$$

(Known as the "Geometric Sum Formula".)

(a) Prove the formula (1) above using mathematical induction on n.

(b) Infer that 5 divides $6^n - 1$ for all $n \in \mathbb{N}$. (`Hint`: Take $x = 6$.)

Problem E. Consider the following two subsets of $\mathbb{N}$.

$$A = \{2, 3, 5, 7, 11, 13, 17, 19\}, \qquad B = \{1, 3, 4, 11, 17, 18\}.$$

(a) Find their cardinalities $|A|$ and $|B|$.

(b) List the elements of their union $A \cup B$ and intersection $A \cap B$.

(c) How many subsets does B have?

(d) Which of the following statements are true?

(i) $1 \in A$

(ii) $A \subseteq B$

(iii) $B \subseteq A$

(iv) $x \in A \iff x$ is a prime number

(v) $x \in B \implies x < 100$

Problem F. Let $\mathrm{GL}_N(\mathbb{R})$ be the set of invertible[1] $N \times N$–matrices A with all its entries in $\mathbb{R}$. Verify in gory detail that $\mathrm{GL}_N(\mathbb{R})$ constitutes a group under matrix multiplication. (Called the "General Linear" group.)

(a) Verify the relation $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na \\ 0 & 1 \end{pmatrix}$ for all $n \in \mathbb{Z}$ – possibly negative.

(b) For any integer $n > 1$ find a 2×2–matrix A such that $A^n = I$ but none of the preceding powers $A, A^2, \ldots, A^{n-1}$ equal I. (`Hint`: Try a rotation matrix $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ for a suitable angle θ.)

[1]This means there is an $N \times N$–matrix B such that $AB = BA = I =$ the identity matrix.