Set 3

(A) Axioms of $\mathbb{Z}$ in other number systems

(1) Which of the following are commutative rings? $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{N}, \mathbb{Z}/m, \mathbb{Z}[i]$.

(2) An element a in a commutative ring is called a *unit* if there is an element b such that $ab = 1$. What are the units of $\mathbb{Z}$? How about $\mathbb{Z}[i]$?

(3) If a is a unit in a commutative ring, the smallest positive integer n such that $a^n = 1$ is called the *order* of a. If no such power exists, we say a has infinite order. What are the orders of the units in $\mathbb{Z}$? What are the orders of the units in $\mathbb{Z}[i]$?

(4) An element a in a commutative ring is called a *zerodivisor* if there is some other element b for which $ab = 0$ (in other words, a is a divisor of 0). Show that 0 is the only zerodivisor in the number systems $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ and $\mathbb{Z}[i]$.

(5) What are the zerodivisors of $\mathbb{Z}/6$?

(6) (*__HW__*) Show that a zerodivisor in a commutative ring in which $1 \neq 0$ can never be a unit.

(7) Show that the number system $\mathbb{Z}/m$ cannot satisfy axioms (6) and (7). [Hint: if it did, and $1 \in P$, then $1 + 1 + \cdots + 1 \in P$. What if $1 \notin P$?]

(8) Show that the number system $\mathbb{Z}[i]$ cannot satisfy axioms (6) and (7). [Hint: analyze i and its powers]

(9) (For enthusiasts) Can there be a commutative ring in which $1 = 0$?

(B) Euclidean algorithm: applications to $\mathbb{Z}/m$

(1) Do the following equations admit solutions with $x, y \in \mathbb{Z}$? If yes, find a solution and, if not, explain why such solution is not possible. (Set 2, B (4) might be useful).

(i) $108x + 51y = 3$
(ii) $108x + 51y = 10$
(iii) $32x + 14y = 8$
(iv) $32x + 14y = 9$
(v) $3x + 7y = 1$

(2) Using (v) from the last problem, show that 3 is a unit in $\mathbb{Z}/7$. What are all the units in $\mathbb{Z}/7$?

(3) Find the units of $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}/4$, $\mathbb{Z}/5$, $\mathbb{Z}/6$ and $\mathbb{Z}/7$ (the last one you already did above). Which of these number systems are fields? (A field is a number system in which every nonzero element is a unit).

(4) Make a conjecture about when $\mathbb{Z}/n$ is a field, and prove it.

(5) (*__HW__*) More generally, show that an integer a is a unit in $\mathbb{Z}/m$ if and only if $\gcd(a, m) = 1$.

(6) Using the problem above, can you now explain the phenomenon observed in (Set 1 (D) (3))?

(7) Let n be a positive integer with $\gcd(3, n) = 1$. Show that there exists an integer x such that n divides $3x - 2$. [Hint: Using (5), begin by showing that one can solve the equation $3x = 2$ in $\mathbb{Z}/n$]

(C)

(1) Can you find solutions in $\mathbb{Z}[i]$ to the equation $(2 + i)x + (4 - i)y = 1$? Which Gaussian integers can be expressed in the form $(1 + i)x + (3 + 2i)y$ for some $x, y \in \mathbb{Z}[i]$?

(2) We call $\mathbf{U}_n$ the set of all units in $\mathbb{Z}/n$; this is also frequently denoted by $(\mathbb{Z}/n)^\times$. For each element of $\mathbf{U}_5$ (how many are there?), list its powers and find its order. Do the same for $\mathbf{U}_7$, $\mathbf{U}_8$, $\mathbf{U}_9$, $\mathbf{U}_{10}$, and $\mathbf{U}_{11}$. Having worked out so many examples, look for patterns; make some conjectures!

(3) For which integers k is $2^k \equiv 1 \pmod 5$? $\pmod 7$? $\pmod 8$?

(4) Solve the congruence $123x \equiv 999 \pmod{30031}$.

(D) Do the following proofs by justifying each step with one of the axioms from the integers given in class (or more primitive principles of logic or set theory not particular to the study of integer arithmetic, e.g. "if $a = b$ and $b = c$, then $a = c$").

(1) If $a, b, c \in \mathbb{Z}$, then $a|b$ and $a|c$ implies $a|(b + c)$.

(2) If $a, b, c \in \mathbb{Z}$, then $a|b$ and $b|c$ implies $a|c$.

(3) If $a \in \mathbb{Z}$, then $a \cdot 0 = 0$.

(E) Which of the following is true in $\mathbb{Z}$? Which is true in $\mathbb{Z}/m$? Prove your claims by using the axioms of $\mathbb{Z}$.

(1) In $\mathbb{Z}$, is it true that $a = bq + r$ implies $\gcd(a, b) = \gcd(b, r)$? If so, prove it using the axioms.

(2) If $\mathbb{Z}$, is it true that if $c \neq 0$ then $ac = bc \implies a = b$? If so, prove it using the axioms. Is this true in $\mathbb{Z}/n$?

(3) Using the axioms of $\mathbb{Z}$, show that every positive integer has a prime divisor.

(4) Let p_n be the n^{th} prime number, so that $p_1 = 2$, $p_2 = 3$, etc. Is it true that, for every n, the number $A_n = p_1 p_2 \cdots p_n + 1$ is prime?

(F) Suppose $ad - bc \neq 0$ for $a, b, c, d \in \mathbb{Z}$. For $r, s \in \mathbb{Z}$, does the system of linear equations

$$\begin{cases} ax + by = r \\ cx + dy = s \end{cases}$$

has a unique solution (x, y), and $x, y \in \mathbb{Q}$? If $ad - bc = \pm 1$, then is there a solution with x and y both integers? What happens in the number system $\mathbb{Z}/n$?