

Practice Test 2, Solutions

Practice test 2 version 1 [allow 50 minutes. All questions equal weight]

- (1) For an integer $n > 1$ define what it means for two integers a, b to be congruent modulo n .

Prove that two integers are congruent modulo n if and only if their remainders are equal when divided by n .

Solution: For $a, b \in \mathbf{Z}$, a is congruent to b modulo n if and only if $a - b$ is divisible by n .

In symbols:

$$a \cong b \pmod{n} \iff n|(a - b)$$

Suppose that a has remainder r_1 and b has remainder r_2 when divided by n . Assume that $r_1 \geq r_2$, since if this is not the case, we can just change the role of a and b .

This means that $a = q_1n + r_1$ and $b = q_2n + r_2$ for some integers q_1, q_2 and $0 \leq r_1, r_2 < n$.

We will make use of the following results:

Result (1): If $n|(na + b)$ then $n|b$.

This is because $n|(na + b) \Rightarrow na + b = nq$ for some q . So $b = n(q - a)$, i.e., $n|b$.

Result (2): If $0 \leq r_2 \leq r_1 < n$, and if $n|(r_1 - r_2)$ then $r_1 = r_2$.

This is because $n|(r_1 - r_2) \Rightarrow r_1 - r_2 = nq$ for some $q \in \mathbf{Z}$, but this is only possible if $q = 0$, since $0 \leq r_1 - r_2 < n$, and the only value of nq in this range is 0. So $r_1 = r_2$.

So

$$\begin{aligned} a \cong b \pmod{n} &\iff n|(a - b) \\ &\iff n|(n(q_1 - q_2) + (r_1 - r_2)) \\ &\iff n|(r_1 - r_2) \quad (\text{because of result (1)}) \\ &\iff r_1 = r_2 \quad (\text{because of result (2)}) \end{aligned}$$

QED.

- (2) Prove that $66^{66} + 6$ is not divisible by 5

Solution:

$66 \cong 1 \pmod{5}$, so $66^{66} \cong 1^{66} \cong 1 \pmod{5}$. So $66^{66} + 6 \cong 1 + 6 \cong 7 \cong 2 \pmod{5}$. Since this is not 0, $66^{66} + 6$ can not be divisible by 5.

- (3) Let R be a ring. What additional properties (other than those satisfied by all rings) does R satisfy if

i) R is a field?

ii) R is an integral domain?

Solution:

A field is a commutative ring in which every nonzero element has a multiplicative inverse in the field.

An integral domain is a commutative ring in which every nonzero element can be cancelled, i.e., a commutative ring R is an integral domain if for $a \neq 0, b, c \in R$, $ab = ac \Rightarrow c = b$.

- (4) (i) List all the zero divisors in \mathbf{Z}_{24} .
(ii) List all the units in \mathbf{Z}_{24} , and give all their inverses.

Solution:

The zero divisors in \mathbf{Z}_{24} are all elements of the form \bar{a} where $0 \leq a \leq 23$ and $(a, 24) \neq 1$. These are:

$$2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22$$

The units in \mathbf{Z}_{24} are 1, 5, 7, 11, 13, 17, 19, 23.

Note that $1 \times 1 = 1, 5 \times 5 = 25 = 24 + 1, 7 \times 7 = 49 = 24 \times 2 + 1, 11 \times 11 = 121 = 24 \times 5 + 1, 13 \times 13 = 169 = 24 \times 7 + 1$.

From these computations,

$$\bar{1}^{-1} = \bar{1}, \bar{5}^{-1} = \bar{5}, xz\bar{7}^{-1} = \bar{7}, \bar{11}^{-1} = \bar{11}$$

We could continue directly, or could also note that $(\overline{-a})^{-1} = \overline{a^{-1}}$, since if $\bar{a}^{-1} = b$, then $\overline{ab} = \bar{1}$. So $(\overline{-a})(\overline{-b}) = \overline{-1} = \bar{1}$. So, since $\overline{23} = \overline{-1}, \overline{23} = \overline{-1}, \overline{19} = \overline{-5}, \overline{17} = \overline{-7}$, and $\overline{11} = \overline{-13}$, from the previous inverses, we get:

$$\overline{23}^{-1} = \overline{23}, \overline{19}^{-1} = \overline{19}, \overline{17}^{-1} = \overline{17}, \overline{11}^{-1} = \overline{11}.$$

(Note, this means that every element is its own inverse in U_{24} , i.e., all elements of this group except $\bar{1}$ have order 2.)

- (5) Is the group of units in \mathbf{Z}_{10} cyclic? If it is not, explain why not, and if it is, give a generator.

Solution: $U_{10} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ We have $\bar{3}^2 = \bar{9}, \bar{3}^3 = \bar{27} = \bar{7}$ and $\bar{3}^4 = \bar{81} = \bar{1}$.

So all elements of U_{10} can be written in the form \bar{a}^n for some $n \in \mathbf{Z}$, so U_{10} is cyclic, generated by $\bar{3}$.

(Note, it's also generated by $\bar{7}$, so this question has more than one correct answer.)

Practice test 2 version 2 [allow 50 minutes. All questions equal weight]

- (1) Prove that if a, b, n are integers $n > 1$, then if $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

Solution: if $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then for some $q_1, q_2 \in \mathbf{Z}$, we have

$$a_1 - a_2 = nq_1, \text{ and } b_1 - b_2 = nq_2,$$

which we can rewrite as

$$a_1 = a_2 + nq_1, \text{ and } b_1 = b_2 + nq_2,$$

so

$$a_1 b_1 = a_2 b_2 + nq_1 b_2 + nq_2 a_2 + n^2 q_1 q_2,$$

so

$$a_1b_1 - a_2b_2 = n(q_1b_2 + q_2a_2 + nq_1q_2),$$

i.e., $n|(a_1b_1 - a_2b_2)$, i.e., $a_1b_1 \cong a_2b_2 \pmod n$. QED.

- (2) Prove that if a ring R is a field, then R is also an integral domain.

Solution: Suppose that R is a field, and for some $a, b, c \in R$, with $a \neq 0$, we have $ab = ac$. Since R is a field, a has an inverse a^{-1} , so $a^{-1}(ab) = a^{-1}(ac)$, so since multiplication in R is associative, $(a^{-1}a)b = (a^{-1}a)c$, so $b = c$.

QED.

- (3) Find an integer x , with $0 \leq x \leq 30$ which is a solution of the equation $\bar{7}x = \bar{2}$ in \mathbf{Z}_{30} .

Solution: We will have $x = \bar{7}^{-1} \times \bar{2}$.

The inverse of $\bar{7}$ is \bar{t} where $7t + 30s = 1$. We can find t using the Euclidean algorithm.

$$30 = 7 \times 4 + 2$$

$$7 = 2 \times 3 + 1$$

So $1 = 7 - 2 \times 3 = 7 - (30 - 7 \times 4) \times 3 = 13 \times 7 - 30 \times 3$, so $t = 13$, and so $x = \bar{26}$.

Alternative method: Note, from $30 = 7 \times 4 + 2$, we get $7 \times 4 \equiv -2 \pmod 7$, so $7 \times (-4) \equiv 2 \pmod 7$, so the solution is $x = \overline{-4} = \bar{26}$. This method is less systematic, but gives the right answer, and if you want, you can also use observations that work for the particular case you're considering.

- (4) Prove that if R is a finite ring, and $a \in R$ is not a zero-divisor, then a is a unit. (You may assume basic properties of multiplication in rings, such as $a \times 0 = 0$ for all $a \in R$, and distributivity of multiplication over addition and subtraction.)

Solution: Suppose that $|R| = n$, and $R = \{r_1, r_2, \dots, r_n\}$. Consider the set $S = \{r_1a, r_2a, \dots, r_na\}$. There are n elements in S , since if $r_ia = r_ja$, since a is not a zero divisor, $r_i = r_j$. So we must have $R = S$. So, since $1 \in R$, we have $1 = r_ia$ for some r_i , so r_i is the inverse of a , so a is invertible, i.e., a unit.

QED