Solution for Math 301 Homework 3

Section 2.1

6. If $a \equiv b \pmod{n}$ and $k|n$, is it true that $a \equiv b \pmod{k}$? Justify your answer.

Solution: If $a \equiv b \pmod{n}$ and $k|n$, then $a - b = nr$ and $n = ks$ for some $r, s \in \mathbb{Z}$. We have

$$(a - b) = ksr \Rightarrow k|(a - b) \Rightarrow a \equiv b \pmod{k}.$$

12. If $p \geqslant 5$ and p is prime, prove that $[p] = [1]$ or $[p] = [5]$ in $\mathbb{Z}_6$. [Hint:Theorem 2.3 and Corollary 2.5.]

Solution: Suppose $p \geqslant 5$ is prime. Let $p = 6k + r$, where $k, r \in \mathbb{Z}$ and $0 \leqslant r < 6$. By Corollary 2.5, we have $[p] = [r]$. Consider the following cases:

1. $r = 0 \Rightarrow 6|p$, a contradiction.
2. $r = 2, 4 \Rightarrow 2|p$, a contradiction.
3. $r = 3 \Rightarrow 3|p$, a contradiction.

Therefore, we have $r = 1$ or 5. Hence, $[p] = [1]$ or $[5]$ in $\mathbb{Z}_6$.

14.

(a) Prove or disprove: If $ab \equiv 0 \pmod{n}$, then $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$

Solution: Let $n = 6$, $a = 2$ and $b = 3$. $ab = 2 \cdot 3 \equiv 0 \pmod{6}$ but $2, 3 \not\equiv 0 \pmod{6}$.

(b) Do part (a) when n is prime.

Solution: Suppose n is prime and $ab \equiv 0 \pmod{n}$. Then, by Theorem 1.5, we have

$$n|ab \Rightarrow n|a \text{ or } n|b \Rightarrow a \equiv 0 \pmod{n} \text{ or } b \equiv 0 \pmod{n}$$

16. If $[a] = [1]$ in $\mathbb{Z}_n$, prove that $(a, n) = 1$. Show by example that the converse may be false.

Solution: If $[a] = [1]$ in $\mathbb{Z}_n$, then $n|(a - 1) \Rightarrow a - 1 = nr$ for some $r \in \mathbb{Z}$. Since $1 = a - nr = a(1) + n(-r)$ is the smallest positive number that can be expressed in the form $au + bv$, we have $(a, n) = 1$.

Alternative explanation: Suppose $d = (a, n)$. Then

$$d|a \text{ and } d|n \Rightarrow d|(a - nr) \Rightarrow d|1.$$

Hence, $d = 1$.

A counterexample for the converse: Let $a = 2$, $n = 3$. Then $(2, 3) = 1$ but $[2] \neq [1]$ in $\mathbb{Z}_3$.

20.

(a) Prove or disprove: If $a^2 \equiv b^2 \pmod{n}$, then $a \equiv b \pmod{n}$ or $a \equiv -b \pmod{n}$.

Solution: The statement is not true. For a counterexample, let $a = 3$, $b = 1$ and $n = 8$. Then $a^2 \equiv 9 \equiv 1 \equiv b^2 \pmod{8}$. We have $a - b = 2$, $a - (-b) = a + b = 4$. Since $8 \nmid (a - b)$ and $8 \nmid (a - (-b))$, we have $a \not\equiv b \pmod{8}$ and $a \not\equiv -b \pmod{8}$.

(b) Do part (a) when n is prime.

Solution: Suppose n is prime and $a^2 \equiv b^2 \pmod{n}$. Then, by Theorem 1.5, we have

$$n|(a^2 - b^2) \Rightarrow n|(a-b)(a+b) \Rightarrow n|(a-b) \text{ or } n|(a+b).$$

$n|(a-b) \Rightarrow a \equiv b \pmod{n}$ and $n|(a+b) \Rightarrow n|(a-(-b)) \Rightarrow a \equiv -b \pmod{n}$.

22.

(a) Give an example to show that the following statement is false: If $ab \equiv ac \pmod{n}$ and $a \not\equiv 0 \pmod{n}$, then $b \equiv c \pmod{n}$.

Solution: Let $a = 2$, $b = 3$, $c = 0$ and $n = 6$. Then

$$2 \cdot 3 \equiv 0 \equiv 2 \cdot 0 \pmod{6} \text{ and } 2 \not\equiv 0 \pmod{n} \text{ but } 3 \not\equiv 0 \pmod{6}.$$

(b) Prove that the statement in part (a) is true whenever $(a, n) = 1$.

Solution: Suppose $(a, n) = 1$ and $ab \equiv ac \pmod{n}$. Then by Theorem 1.4, we have

$$n|(ab - ac) \Rightarrow n|a(b-c) \Rightarrow n|(b-c) \Rightarrow b \equiv c \pmod{n}.$$

Appendix C

15. What is wrong with the following "proof" that all roses are the same color. It suffices to prove the statement: In every set of n roses, all the roses in the set are the same color. If $n = 1$, the statement is certainly true. Assume the statement is true for $n = k$. Let S be a set of $k + 1$ roses. Remove one rose (call it rose A) from S; there are k roses remaining, and they must all be the same color by the induction hypothesis. Replace rose A and remove a different rose (call it rose B). Once again there are k roses remaining that must all be the same color by the induction hypothesis. Since the remaining roses include rose A, all the roses in S have the same color. This proves that the statement is true when $n = k + 1$. Therefore, the statement is true for all n by induction.

Solution: The conclusion "Since the remaining roses include rose A, all the roses in S have the same color." does not hold as in the following example.

Let $S = \{A,\ B\}$ be a set of two roses with two different colors A and B. Each of $S\backslash\{A\}$ and $S\backslash\{B\}$ is a set contains only one rose. Thus, each of these sets contains roses of the same color but we cannot conclude that all roses in S are of the same color.

17. Let x be a real number greater than -1. Prove that for every positive integer n, $(1+x)^n \geqslant 1+nx$.

Solution: Let $P(n)$ be the statement that $(1+x)^n \geqslant 1+nx$.
For $n = 1$, we have $(1+x)^n = 1+x = 1+nx$. Therefore, $P(1)$ is true.

Suppose $P(k)$ is true for some $k \geqslant 1$. Since $x \geqslant -1 \Rightarrow (1+x) \geqslant 0$, we have

$$(1+x)^{k+1} = (1+x)(1+x)^k \geqslant (1+x)(1+kx) = 1+(k+1)x+kx^2 \geqslant 1+(k+1)x.$$

So $P(k+1)$ is also true. Hence, by the Principle of Mathematical Induction, $P(n)$ is true for all $n \geqslant 1$.

Appendix D

11. Let $\sim$ be defined on the set $\mathbb{R}^*$ of nonzero real numbers by $a \sim b$ if and only if $a/b \in \mathbb{Q}$. Prove that $\sim$ is an equivalence relation.

Solution:

(i) **Reflxive:** $a \in \mathbb{R}^* \Rightarrow a/a = 1 \in \mathbb{Q} \Rightarrow a \sim a$.

(ii) **Symmetric:** Let $a,\ b \in \mathbb{R}^*$. $a \sim b \Rightarrow a/b \in \mathbb{Q} \Rightarrow b/a = (a/b)^{-1} \in \mathbb{Q} \Rightarrow b \sim a$.

(iii) **Transitive:** Let $a,\ b,\ c \in \mathbb{R}^*$.

$$a \sim b \text{ and } b \sim c \Rightarrow a/b,\ b/c \in \mathbb{Q} \Rightarrow c/a = (a/b)(b/c) \in \mathbb{Q} \Rightarrow a \sim c.$$

Therefore, $\sim$ is an equivalence relation on $\mathbb{R}$.

17. Let $\sim$ be a symmetric and transitive relation on a set A. What is wrong with the following "proof" that $\sim$ is reflexive: $a \sim b$ implies $b \sim a$ by symmetry; then $a \sim b$ and $b \sim a$ implies $a \sim a$ by transitivity. [Also see Exercise 8(f).]

Solution: The problem is that given $a \in A$, there might not be any $b \in A$ such that $a \sim b$. For example, let $A = \{a,\ b\}$ and $\sim$ is defined on A with only $b \sim b$. Then $\sim$ is a symmetric and transitive relation on A but $\sim$ is not reflexive because $a \not\sim a$.