

Name: Solutions

15 minutes

Each problem is worth 4 points. You may invoke any theorem that was proved in class, provided you make it clear which result you are using. For example, you might say something like “since  $a \mid b$  and  $a \mid c$ , we have  $a \mid bc$ ,” or “by the transitive property of congruence modulo  $n$ .”

**Problem 1.** Let  $a, b, c, x, y \in \mathbb{Z}$ . Prove that if  $a \mid b$  and  $a \mid c$ , then  $a \mid (bx + cy)$ .

*Proof.* Suppose  $a \mid b$  and  $a \mid c$ . By a theorem from class,  $a$  divides any multiple of  $b$  and  $a$  divides any multiple of  $c$ . In particular,  $a \mid bx$  and  $a \mid cy$ . By another theorem from class,  $a$  divides the sum of any two integers it divides, so  $a \mid bx + cy$ .  $\square$

*Alternative proof.* By the definition of divisibility, there exist  $k, \ell \in \mathbb{Z}$  such that  $ka = b$  and  $\ell a = c$ . Thus,  $bx + cy = (ka)x + (\ell a)y = a(kx + \ell y)$ . Since  $kx + \ell y \in \mathbb{Z}$ ,  $a \mid bx + cy$ .  $\square$

**Problem 2.** Define a relation  $\sim$  on  $\mathbb{Z}$  by  $a \sim b$  if and only if  $a \mid b$ . Prove that  $\sim$  is reflexive and transitive, but not symmetric.

*Proof.* We check each of the three properties.

*Reflexive:* Let  $a \in \mathbb{Z}$ . Then  $a \mid a$  since  $a = a \cdot 1$ . Thus,  $a \sim a$ .

*Transitive:* Suppose  $a \sim b$  and  $b \sim c$ . Then  $a \mid b$  and  $b \mid c$ . There exist  $k, \ell \in \mathbb{Z}$  such that  $ka = b$  and  $\ell b = c$ . Then we see that  $c = \ell b = \ell(ka) = (\ell k)a$ . Since  $\ell k \in \mathbb{Z}$ , we can conclude that  $a \mid c$ . Thus,  $a \sim c$ .

*Symmetric:* Notice that  $1 \mid 0$  since  $1 \cdot 0 = 0$ . So  $1 \sim 0$ . But  $0 \nmid 1$  since  $0 \cdot k = 0$  for all  $k \in \mathbb{Z}$  and  $0 \neq 1$ . Thus,  $0 \not\sim 1$ . Therefore,  $\sim$  is not symmetric.  $\square$

**Problem 3.** Let  $a, m, n \in \mathbb{Z}$  with  $m, n > 0$ , and denote by  $[a]_n$  and  $[a]_m$  the equivalence classes of  $a$  modulo  $n$  and modulo  $m$ , respectively. If  $m \mid n$ , determine which of  $[a]_n$  and  $[a]_m$  is contained in the other. Prove your claim.

*Claim:* If  $m \mid n$ , then  $[a]_n \subseteq [a]_m$ .

*Proof.* Let  $x \in [a]_n$ . Then  $x \equiv a \pmod{n}$ , so  $n \mid x - a$  by definition. By hypothesis,  $m \mid n$ . By transitivity of the relation  $\mid$  (from Problem 2),  $m \mid x - a$ . Thus,  $x \equiv a \pmod{m}$ . By definition, this means that  $x \in [a]_m$ . So  $[a]_n \subseteq [a]_m$ .  $\square$