Homework 1: Written Solutions

Written Part

5. Let $a, b, c \in \mathbb{Z}$.

   (a) Suppose $a|b$ and $b|c$. Prove $a|c$

   Proof. By assumption there are $k, l \in \mathbb{Z}$ such that $b = ak$ and $c = bl$. Substitution gives $c = akl$ whence $a|c$ $\square$

   (b) Suppose $a|b$ and $b|a$. Prove $a = \pm b$.

   Proof. By assumption there are $k, l \in \mathbb{Z}$ with $a = bk$ and $b = al$. Substitution give $a = alk$ so that $lk = 1$. Therefore either $l = k = 1$ or $l = k = -1$ and the result follows. $\square$

   (c) Suppose $a|b$ and $a|c$. Prove $a|(b + c)$ and $a|(b - c)$.

   Proof. By assumption there are $k, l \in \mathbb{Z}$ with $b = ka$ $c = la$. Thus $b \pm c = ka \pm la = (k \pm l)a$ whence $b|(b \pm c)$. $\square$

6. In this exercise we prove the existence and uniqueness of division with remainder. Let $a, b \in \mathbb{Z}$, and suppose that $b \neq 0$. We start with existence.

   (a) We begin by considering the set of numbers $a - bq$ as q varies over the integers. Prove that the set
   $$S = \{a - bq : q \in \mathbb{Z}\},$$
   has at least one nonnegative element.

   Proof. The goal is to show that there is some q with $a - bq \geq 0$. Solving for q gives $q \geq (a/b)$ if $b \geq 0$ or $q \leq (a/b)$ if $b \leq 0$. In each case we can find some $q \in \mathbb{Z}$ satisfying the inequality. $\square$

   (b) Let r be the minimal nonnegative element of S. Show that $0 \leq r < |b|$.

   Proof. By assumption $r \geq 0$ and $r = a - bq$ for some q. Suppose $r \geq |b|$. Then
   $$r - |b| = a - bq - |b| = a = b(q \pm 1)$$
   is another nonnegative element of S, and it is smaller than r, contradicting the minimality of r. So we cannot have $r \geq |b|$ completing the proof. $\square$

   (c) Use (b) to conclude that $a = bq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$. This proves existence.

   Proof. Letting $r = a - bq$ be the minimal element of the set, then $a = bq + r$ and by the previous exercise $0 \leq r < |b|$. $\square$

(d) Show that the division with remainder from part (c) is unique. That is, suppose there are $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$a = bq_1 + r_1 \quad \text{and} \quad a = bq_2 + r_2.$$

Suppose further that $0 \leq r_i < |b|$ for $i = 1, 2$. Then show $q_1 = q_2$ and $r_1 = r_2$.

Proof. Perhaps swapping 1 and 2 we may assume without loss of generality that $r_1 \geq r_2$. The equation $bq_1 + r_1 = bq_2 + r_2$ can be rewritten as

$$r_1 - r_2 = b(q_2 - q_1).$$

Therefore $r_1 - r_2$ is a multiple of b, and $0 \leq r_1 - r_2 < |b|$, so the only possibility is that $r_1 - r_2 = 0$ and we have $r_1 = r_2$. Subbing into the equation above gives:

$$0 = b(q_2 - q_1),$$

and since $b \neq 0$ we have $q_2 - q_1 = 0$ so that $q_2 = q_1$. □

7. Fix two integers a and b. The extended Euclidean algorithm shows the greatest common divisor of a and b is an integral linear combination of a and b. In this exercise we prove a partial converse to this statement.

(a) Show that $\gcd(a, b)$ divides $au + bv$ for any $u, v \in \mathbb{Z}$.

Proof. Let $g = \gcd(a, b)$. Then $g|a$ and $g|b$ so that $g|au$ and $g|bv$. By 5(c) then $g|(au + bv)$. □

(b) Using part (a), prove that a and b are coprime if and only if there are $u, v \in \mathbb{Z}$ such that $au + bv = 1$. Give an example to show that u and v need not be unique.

Proof. If a and b are coprime then we can find such a u and v using the extended Euclidean algorithm. Conversely, suppose $au + bv = 1$. Then by part (a) we know that $\gcd(a, b)$ divides 1, so it must be equal to 1.

For a counterexample, consider 2 and 3 which are coprime. Than $u = -1$ and $v = 1$ gives $-1(2) + 1(3) = 1$. But on could also take $u = 5$ and $v = -3$ to get $5(2) - 3(3) = 1$ as well. □

(c) Suppose (u_1, v_1) and (u_2, v_2) are two solutions to $au + bv = 1$. Show that a divides $v_2 - v_1$ and that b divides $u_2 - u_1$. Even stronger, show that there is in fact some $k \in \mathbb{Z}$ so that $v_2 = v_1 - ka$ and $u_2 = u_1 + kb$ (for the same k).

Proof. We begin by making the following observation:

Lemma 1. *Suppose* $\gcd x, y = 1$ *and* $x|yz$. *Then* $x|z$.

Proof. Notice that there are some u, v such that $xu + yv = 1$. Multipying through by z we get $xzu + yzv = z$. Certainly $x|xzu$, and by assumption $x|yzv$, so that by 5(a) it must divide their sum which is z. □

With this in hand, we use the equation$au_1 + bv_1 = 1 = au_2 + bv_2$, and rearrange to get

$$a(u_1 - u_2) = b(v_2 - v_1). \tag{1}$$

In particular, a divides $b(v_2 - v_1)$, so that by Lemma 1 we may conclude that $a|v_2 - v_1$. Similarly we deduce that $b|u_1 - u_2$, and therefore it divides $u_2 - u_1$, giving the first result. In particular, we know that $ak_1 = (v_2 - v_1)$ and $bk_2 = (u_2 - u_1)$. To prove the remaining statement we must show that $k_1 = -k_2$. But plugging into Equation 1 gives $-abk_2 = abk_1$ and cancelling ab finishes the proof. □

8. In this exercise we prove the algebraic consistency of modular arithmetic. Let m be a positive integer, and fix integers a, a', b, b' satisfying

$$\begin{aligned} a &\equiv a' \mod m \\ b &\equiv b' \mod m. \end{aligned}$$

Prove that the following congruences hold.
We will assume throughout that $a = a' + km$ and $b = b' + lm$.

(a) $a + b \equiv a' + b' \mod m$.

Proof.

$$a + b = a' + km + b' + lm = a' + b' + (k + l)m \equiv a' + b' \mod m.$$

□

(b) $a - b \equiv a' - b' \mod m$.

Proof.

$$a + b = a' + km - (b' + lm) = a' - b' + (k - l)m \equiv a' - b' \mod m.$$

□

(c) $ab \equiv a'b' \mod m$.

Proof.

$$ab = (a+km)(b+lm) = ab+kmb+alm+kmlm = ab+m(kb+al+klm) \equiv ab \mod m.$$

□

9. Let's get a little practice with modular algebra. You're welcome to make use of a Jupyter notebook to help you in these calculations.

(a) What is 4^{-1} modulo 15?
Since $4 \cdot 4 = 16 \equiv 1 \mod 15$ we have $4^{-1} = 4$.

(b) Solve $4x = 11 \mod 15$ for x. Give a value of x that lives in $\mathbb{Z}/15\mathbb{Z}$.
We multiple both sides of the equation by 4^{-1}, which by part (a) is 4. This gives $x = 44 \equiv 14 \mod 15$.

(c) What is 35^{-1} modulo 573?
We use the extended Euclidean algorithm which gives $35u + 573v = 1$ for $u = 131$ and $v = -8$. In particular $35^{-1} \equiv 131 \mod 573$.

(d) Solve $35x + 112 = 375 \mod 573$ for x. Give a value of x that lives in $\mathbb{Z}/573\mathbb{Z}$.
Subtracting 112 from both sides gives $35x \equiv 263 \mod 573$. By part (c) dividing through by 35 is the same as multiplying by 131 so we get $x = 263 * 131 = 34453 \equiv 533 \mod 573$.