Homework 1 Solutions

1. Suppose $n \in \mathbb{Z}$. Let r be the remainder when n^2 is divided by 8. What are the possible values of r? (You must prove both that your list contains all possible values and that it does not contain any impossible values – otherwise you could just say that the list $0, 1, \ldots, 7$ definitely contains all the possibilities!)

   Solution 1: First suppose n is odd. Then $n = 2k + 1$ for some integer k, so

   $$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

   Since k and $k + 1$ are consecutive integers, one of them is even. Therefore $k(k + 1) = 2j$ for some $j \in \mathbb{Z}$, so $n^2 = 8j + 1$. Thus $r = 1$.

   Now suppose n is even. When n is divided by 4, the remainder must be 0 or 2 (because $4q + 1$ and $4q + 3$ would be odd). If the remainder is 0, then $n = 4q$ for some $q \in \mathbb{Z}$, so $n^2 = 16q^2 \equiv 0 \pmod 8$ and $r = 0$. If the remainder is 2, then $n = 4q + 2$ for some $q \in \mathbb{Z}$, so

   $$n^2 = (4q + 2)^2 = 16q^2 + 16q + 4 \equiv 4 \pmod 8$$

   and $r = 4$.

   The above arguments shows that r must be 0, 1, or 4, and that all three of these possibilities actually occur as remainders.

   Solution 2: We know that n must be congruent modulo 8 to one of $-3, -2, -1, 0, 1, 2, 3,$ or 4, so we consider several cases separately:

   - If $n \equiv 0 \pmod 8$, then $n^2 \equiv 0 \pmod 8$, so $r = 0$.
   - If $n \equiv \pm 1 \pmod 8$, then $n^2 \equiv 1 \pmod 8$, so $r = 1$.
   - If $n \equiv \pm 2 \pmod 8$, then $n^2 \equiv 4 \pmod 8$, so $r = 4$.
   - If $n \equiv \pm 3 \pmod 8$, then $n^2 \equiv 9 \equiv 1 \pmod 8$ so $r = 1$.
   - If $n \equiv 4 \pmod 8$, then $n^2 \equiv 16 \equiv 0 \pmod 8$, so $r = 0$.

   This shows that r must be 0, 1, or 4, and that all three of these possibilities actually occur as remainders.

2. Suppose $a, b \in \mathbb{Z}$ with $b > 0$. Let r be the remainder when a is divided by b. Prove that $(a, b) = (b, r)$.

   Solution 1: By definition, $a = bq + r$ for some integer q.

   We will prove that the common divisors of a and b are precisely the common divisors of b and r; it follows immediately that $(a, b) = (b, r)$.

   Suppose d is a common divisor of a and b. Since $r = a - bq$ is a linear combination of a and b, it follows that d is also a divisor of r. Thus every common divisor of a and b is also a common divisor of b and r.

Now suppose e is a common divisor of b and r. Since $a = bq+r$, it follows that $e \mid a$. Thus every common divisor of b and r is also a common divisor of a and b, which completes the proof.

Solution 2: The argument in Solution 1 shows that (a, b) is a common divisor of b and r; hence $(a, b) \leq (b, r)$. Similarly, the argument in Solution 1 also shows that (b, r) is a common divisor of a and b; hence $(b, r) \leq (a, b)$. It follows that $(a, b) = (b, r)$.

Solution 3: By definition, $a = bq + r$ for some integer q.

Recall that (a, b) is the smallest positive linear combination of a and b, and (b, r) is the smallest positive linear combination of b and r. Hence, in order to prove that $(a, b) = (b, r)$, it suffices to prove that the linear combinations of a and b are precisely the linear combinations of b are r.

We first check that every linear combination of a and b is also a linear combination of b and r. For any $u, v \in \mathbb{Z}$,

$$au + bv = (bq + r)u + bv = b(qu + v) + ru,$$

which proves the claim.

Now we check that every linear combination of b and r is also a linear combination of a and b. For any $u, v \in \mathbb{Z}$,

$$bu + rv = bu + (a - bq)v = av + b(u - qv),$$

which proves the claim and completes the proof.

3. If a, b, c are nonzero integers, let (a, b, c) denote the greatest common divisor of a, b, and c. [That is, (a, b, c) is the greatest integer which divides all of a, b, and c.] Prove that $(a, b, c) = ((a, b), c)$.

   Note: This means that if we have an efficient algorithm to compute the gcd of two integers, then we can efficiently compute the gcd of three integers by using the algorithm twice. In fact, there is such an algorithm, as we'll see later.

   Solution: As in Solution 1 to Problem 2, it suffices to prove that the common divisors of a, b, and c are precisely the common divisors of (a, b) and c. We saw in lecture that the common divisors of a and b are precisely the divisors of (a, b), and the claim follows immediately.

4. Suppose $a, b, c \in \mathbb{Z}$ such that $a \mid c$ and $b \mid c$. Prove that $ab \mid c(a, b)$.

   Note: An especially important special case is when $(a, b) = 1$. In that case, the theorem says that if $a \mid c$, $b \mid c$, and $(a, b) = 1$, then $ab \mid c$.

   Solution 1: There exist $m, n \in \mathbb{Z}$ such that $c = am$ and $c = bn$. By Bézout's identity, there exist $u, v \in \mathbb{Z}$ such that $(a, b) = au + bv$. Hence

$$c(a, b) = c(au + bv) = cau + cbv = bnau + ambv = ab(nu + mv),$$

   which shows that $ab \mid c(a, b)$.

   Solution 2: This solution is based on Exercises 1.3.19 and 1.3.20 from the textbook.

   For any prime p, let a_p denote the exponent of p in the prime factorization of a; define b_p and c_p similarly. The fact that $a \mid c$ says that $a_p \leq c_p$ for each p; similarly, $b_p \leq c_p$. Therefore $\max(a_p, b_p) \leq c_p$. We also know that for any prime p, the exponent of p in the prime factorization of (a, b) is $\min(a_p, b_p)$.

   The exponent of p in the prime factorization of $c(a, b)$ is $c_p + \min(a_p, b_p)$, and the exponent of p in the prime factorization of ab is $a_p + b_p$. Note that[1]

$$a_p + b_p = \max(a_p, b_p) + \min(a_p, b_p) \leq c_p + \min(a_p, b_p)$$

   for any prime p, so $ab \mid c(a, b)$.

5. Suppose $a, b, c \in \mathbb{Z}$ such that $(a, c) = (b, c) = 1$. Prove that $(ab, c) = 1$.

   Solution 1: By Bézout's identity, there exist $s, t, u, v \in \mathbb{Z}$ such that

$$as + ct = 1 \qquad \text{and} \qquad bu + cv = 1.$$

   Therefore

$$1 = bu + cv = (as + ct)bu + cv = ab(su) + c(btu + v).$$

   Since 1 is a linear combination of ab and c, it follows that $(ab, c) = 1$. (Any common divisor of ab and c must divide every linear combination of ab and c, so the fact that 1 is a linear combination implies that $(a, b) \mid 1$. Since 1 is the only positive divisor of 1, it follows that $(a, b) = 1$.)

   Solution 2: Let p be any prime divisor of c. We are given that $(a, c) = (b, c) = 1$, so p is not a divisor of a or b. Since p is prime, it follows that $p \nmid ab$. This proves that ab and c have no common prime divisors. It follows that they have no common divisor $d > 1$; if they had a common divisor $d > 1$, then any prime divisor p of d would be a common prime divisor of ab and c. Thus $(ab, c) = 1$.

[1] To prove the identity $x + y = \max(x, y) + \min(x, y)$, consider separately the cases $x \leq y$ and $x > y$.