Homework 1

Due Friday, January 29

Homework policies

You are welcome to discuss homework assignments with others, but you must write the solutions by yourself, in your own words. Those words should be clear, grammatical, and (as far as possible without sacrificing rigor/clarity) concise.

On homework assignments (and tests), you are free to use any theorem that was discussed in class, in the textbook sections that we have covered, or on a homework assignment.

Late homework assignments decay with a half-life of one day, e.g., if your homework is one day late, you will receive half credit. If it is twelve hours late, you will receive about 71% credit.

Practice problems

You don't need to turn in solutions to the following textbook problems, but you should try all of them.

- Section 1.1: 2, 5, 7, 8, 9
- Section 1.2: 8, 11, 14, 18, 24, 27

Problems to turn in

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: For any $n \in \mathbb{Z}$ divided by 4, the possible remainders are 0,1,2,3.

   Case 1: $n = 4k$ for some $k \in \mathbb{Z}$. Then, $n^2 = (4k)^2 = 16k^2 = 8(2k^2) = 8m$ for $m = 2k^2, m \in \mathbb{Z}$. Hence, the remainder $r = 0$.

   Case 2: $n = 4k+1$ for some $k \in \mathbb{Z}$. Then, $n^2 = (4k+1)^2 = 16k^2+8k+1 = 8(2k^2+k)+1 = 8m+1$ for $m = 2k^2 + k, m \in \mathbb{Z}$. Hence, the remainder $r = 1$.

   Case 3: $n = 4k + 2$ for some $k \in \mathbb{Z}$. Then, $n^2 = (4k + 2)^2 = 16k^2 + 16k + 4 = 8(2k^2 + 2k) + 4 = 8m + 4$ for $m = 2k^2 + 2k, m \in \mathbb{Z}$. Hence, the remainder $r = 4$.

   Case 4: $n = 4k + 3$ for some $k \in \mathbb{Z}$. Then, $n^2 = (4k + 3)^2 = 16k^2 + 24k + 9 = 8(2k^2 + 3k + 1) + 1 = 8m + 1$ for $m = 2k^2 + 3k + 1, m \in \mathbb{Z}$. Hence, the remainder $r = 1$.

   Thus, for all the possible $n \in \mathbb{Z}$, the remainders of n^2 divided by 8 are 0,1,4. □

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

   Proof: Suppose $d = (a, b)$ for $d \in \mathbb{Z}$ and $d > 0$. By the Division Algorithm,$a = bq + r$ for $r, q \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$, $d \mid a - bq = r$. Hence, d is a common divisor of b and r.

Need to prove d is the greatest.

Take $c \in \mathbb{Z}, c > 0$ as an arbitrary common divisor of b and r. Then $c \mid b$ and $c \mid r$. Hence $c \mid bq + r$ or $c \mid a$. This implies c is also a common divisor of a and b. But, $d = (a, b)$, hence $c \leq d$. Thus $(b, r) = d$.

Therefore $(a, b) = (b, r)$. □

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.

   Proof: Let $d = ((a, b), c)$ and $k = (a, b)$. Then $d \mid k$. Also, since $k = (a, b)$, $k \mid a$ and $k \mid b$, which implies $d \mid a$ and $d \mid b$. Hence d is a common divisor of a, b and c.

   Need to prove d is the greatest.

   Let $t \in \mathbb{Z}, t > 0$ be an arbitrary common divisor of a, b and c. Hence, $t \leq k = (a, b)$. By Bézout's Identity, $k = au + bv$ for $u, v \in \mathbb{Z}$. Since $t \mid a$ and $t \mid b$, $t \mid k$. Now $t \mid k$ and $t \mid c$, this implies t is a common divisor of (a, b) and c. Hence $t \leq d$, which proves $d = (a, b, c)$.

   Therefore, $((a, b), c) = (a, b, c)$. □

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: Suppose $a \mid c$, $b \mid c$. Then $c = am$ and $c = bn$ for some $m, n \in \mathbb{Z}$. By Bézout's Identity, $(a, b) = au + bv$ for $u, v \in \mathbb{Z}$. Then:

$$\begin{aligned} c(a, b) &= c(au + bv) \\ &= cau + cbv \\ &= (bn)au + (am)bv \\ &= ab(un + vm). \end{aligned}$$

   Since $un + vm \in \mathbb{Z}$, $ab \mid c(a, b)$. □

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

   Solution: Let $d = (ab, c)$ for $d \in \mathbb{Z}$. Since $(b, c) = 1$, by Bézout's Identity, $1 = bu + cv$ for $u, v \in \mathbb{Z}$. Then, $a = abu + acv$.

   Since $d = (ab, c)$, $d \mid ab$ and $d \mid c$. Since $a = abu + acv$, this implies $d \mid a$. Also $d \mid c$, then d is a common divisor of a and c.

   But $(a, c) = 1$, it follows that $(ab, c) = 1$ as well. □