Math 444
Newberger

Tips and Remarks for Homework 1

#7 page 6 Let n be a positive integer. Prove that a and c leave the same remainder when dividing by n if and only if $a - c = nk$ for some integer k.

Since this is an if and only if statement, you must write two proofs:
"$\Rightarrow$" If a and c leave the same remainder when dividing by n, then $a - c = nk$ for some integer k.
and
"$\Leftarrow$" If $a - c = nk$ for some integer k, then a and c leave the same remainder when dividing by n.

Here's how to start for "$\Rightarrow$":

- Write out your assumptions (the if part): Let a and c have the same remainder when dividing by n. To make use of this information, you'll use the Division Algorithm to divide a and c by n. The Division Algorithm says there exists $q_1, r_1 \in \mathbb{Z}$ such that $a = q_1 n + r_1$, and there exists $q_2, r_2 \in \mathbb{Z}$ such that $c = q_2 n + r_2$. Since a and c have the same remainder when dividing by n, we have $r_1 = r_2$. So from your assumptions, you have two equations to work with (replacing r_2 by r_1 since they are equal): $a = q_1 n + r_1$ and $c = q_2 n + r_1$.
- Now explain what you want to prove (the then part): We want to show that $a - c = nk$ for some integer k. This means we want to find an integer k such that $a - c = nk$.
- Next, you will use the if to get the then. Use the assumptions to write $a - c$ in terms of n to determine what k should be.

Here's how to start for "$\Leftarrow$" (this one is tricky):

- Write out your assumptions (the if part): Let $k \in \mathbb{Z}$ such that $a - c = nk$.
- Now explain what you want to prove (the then part): We want to show that a and c have the same remainder when dividing by n. Use the division algorithm, as you did above. The Division Algorithm says there exists $q_1, r_1 \in \mathbb{Z}$ such that $a = q_1 n + r_1$, and there exists $q_2, r_2 \in \mathbb{Z}$ such that $c = q_2 n + r_2$. Furthermore, the Division Algorithm says $0 \le r_1, r_2 < n$. We want to show that $r_1 = r_2$.
- Next, you will use the if to get the then. You now have three equations to work with: $a = q_1 n + r_1$, $c = q_2 n + r_2$ and $a - c = nk$. Here's the idea: We want to show $r_1 = r_2$; this is the same as $r_1 - r_2 = 0$ and as $r_2 - r_1 = 0$. We know that the numbers r_1 and r_2 are either equal or one is bigger than the other. So either $r_1 - r_2 \ge 0$ or $r_2 - r_1 \ge 0$. Technically, the statement would have to be proved in both cases, but the proofs are identical, so you can write, "without loss of generality, assume that $r_1 - r_2 \ge 0$." Now $0 \le r_2 \le r_1 < n$, so $r_1 - r_2$ (which is the distance between r_1 and r_2 on the numberline) also satisfies $0 \le r_1 - r_2 < n$. Use your three equations to prove that $n | r_1 - r_2$, and argue that the only divisor of n that is greater than or equal to 0 and less than n is 0. Thus $r_1 - r_2$ must equal zero.

Problem #8 page 7

b. Make a conjecture about the remainder when the square of an odd integer is divided by 8.

When the square of an odd integer is divided by 8, the remainder is 1.

It will be easier to prove your conjecture if you write it as an if/then statement.

If x is odd, then x^2 has remainder 1 when dividing by 8.

c. Prove your conjecture.

- Write out your assumptions (the if part). Let x be odd. Then there exists $n \in \mathbb{Z}$ such that $x = 2n + 1$.
- Now explain what you want to prove (the then part). We want to show that x^2 has remainder 1 when dividing by 8. This means we want to find a number k such that $x^2 = 8k + 1$.
- Next you will use the if to get the then. Prove the statement in two cases: case 1 when n is even, and case 2 when k is odd.
  Case 1. n is even. Then there exists $m \in \mathbb{Z}$ such that $n = 2m$. Calculate x^2 in this case. Say what k should be to make $x^2 = 8k + 1$.
  Case 2. n is odd. Then there exists $m \in \mathbb{Z}$ such that $n = 2m + 1$. Calculate x^2 in this case. Say what k should be to make $x^2 = 8k + 1$.