Homework #6 Solutions

4.1.5. If a is an odd integer, then we may write $a = 2k + 1$ for some integer k. Thus $a^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$. Now, k^2 and k have the same parity (i.e. they are either both even or both odd), so in any case the integer $k^2 + k$ is even (as the sum of two integers of the same parity is always even). Thus $4(k^2 + k)$ is divisible by 8, so $a^2 = 4(k^2 + k) + 1 \equiv 1 \pmod 8$.

4.1.10. I refuse to look at LaTeX documentation or define a macro to duplicate the non-standard notation the textbook is using here. Instead, I will denote the two integers by r_1 and r_2 (i.e., r_1 is the remainder when m is divided into a, and r_2 is the remainder when m is divided into b). Without a loss of generality, we may assume that $r_1 \geq r_2$. Using the division algorithm, we may write $a = q_1 m + r_1$ and $b = q_2 m + r_2$ for integers q_1 and q_2. We therefore have $a - b = m(q_1 - q_2) + r_1 - r_2$. As $a \equiv b \pmod m$, m divides $a - b$, so this last equation implies that $r_1 - r_2 = a - b - m(q_1 - q_2)$ is divisible by m. Since $0 \leq r_2 \leq r_1 < m$, $0 \leq r_1 - r_2 < m$, which forces $r_1 - r_2 = 0$, i.e., $r_1 = r_2$.

4.1.20. Here is the addition table, in all its typeset glory.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

4.1.27. (We should assume $n \geq 2$ here since the assertion does not make sense for $n = 1$.) For any integer $n \geq 2$, $\sum_{k=1}^{n-1} k = n(n-1)/2$ by Exercise 1.3.6. If in addition n is odd, then $n - 1$ is even, so $(n-1)/2$ is an integer, and therefore $\sum_{k=1}^{n-1} k = n((n-1)/2)$ is divisible by n, i.e., $\sum_{k=1}^{n-1} k \equiv 0 \pmod n$. If n is even, then the sum in question is the product of the integers $n/2$ and $n - 1$. If n divides this product, then because $(n, n-1) = 1$, n divides $n/2$ by Lemma 3.4. But $0 < n/2 < n$, so this is impossible. Therefore the congruence never holds for n even.

4.1.30. When $n = 1$, both sides of the putative congruence are equal to 4, so the congruence is valid. Assume now that the congruence holds for some integer $k \geq 1$. We then have

$$4^{k+1} = 4 \cdot 4^k \equiv 4(1 + 3k) \equiv 4 + 12k \equiv 1 + 3 + 3k \equiv 1 + 3(k+1) \pmod 9.$$

So, by induction, the congruence holds for all $n \geq 1$.

4.1.33. If a is any integer, and r is the remainder when a is divided by 4, then $0 \leq r < 4$, and since $a \equiv r \pmod 4$, $a^2 \equiv r^2 \pmod 4$. We have $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 0 \pmod 4$,

Date: March 22, 2018.

and $3^2 = 9 \equiv 1 \pmod 4$. Thus the square of an integer is congruent to either 0 or 1 modulo 4. It follows that a sum of two squares is congruent to either 0, 1, or 2 modulo 4. Therefore, if $n \equiv 3 \pmod 4$, then n cannot be the sum of two squares.

4.1.34. If $x = 0$ or $x = 1$, then $x^2 = x$, so certainly $x^2 \equiv x \pmod p$. Conversely, suppose x is an integer satisfying $x^2 \equiv x \pmod p$. Then p divides $x^2 - x = x(x-1)$. As p is prime, it follows that p divides either x or $x - 1$. In the first case, $x \equiv 0 \pmod p$, while in the second case, $x \equiv 1 \pmod p$.