Homework 3: *1.4*: 2*, 3*, 5, 6, 7 *1.5*: 1*, 2*, 4*
*in back of book

Exercises 1.4

5. Note that $8n + 7 \equiv 7 (\text{mod } 8)$. But by direct checking we see that 7 is not the sum of three squares mod 8. ie: $0^2 \equiv 0(\text{mod } 8)$, $1^2 \equiv 1(\text{mod } 8)$, $2^2 \equiv 4(\text{mod } 8)$, $3^2 \equiv 1(\text{mod } 8)$, $4^2 \equiv 0(\text{mod } 8)$, $5^2 \equiv 1(\text{mod } 8)$, $6^2 \equiv 4(\text{mod } 8)$, $7^2 \equiv 1(\text{mod } 8)$. Thus any square is $0, 1,$ or 4 mod 8. Since we can't add three of these numbers to get 7, seven is not the sum of three squares mod 8, and therefore $8n + 7$ is not the sum of three squares, for any n.

6. Manipulating this equation, we see that $x^2 \equiv 1 \iff x^2 - 1 \equiv 0 \iff (x + 1)(x - 1) \equiv 0(\text{mod } p)$. But then we see that $p|(x + 1)(x - 1)$, which tells us by Theorem 1.3.1 that either $p|(x + 1)$ or $p|(x - 1)$. In the first case $x \equiv -1$, in the second case $x \equiv 1$. Thus $x^2 \equiv 1(\text{mod p})$ has just two solutions mod p, which are distinct if $p \neq 2$.

7. Expanding, we see that $(p - 1)! \equiv 1 \cdot 2 \cdots (p - 2) \cdot (p - 1)(\text{mod } p)$, which is a product of $p - 1$ factors. Assuming in general that $p \neq 2$, this is an odd number of factors. From number 6, we see that 1 and $p - 1$ are the only two numbers that are self-inverse mod p. Thus, all n such that $2 \leq n \leq p - 2$ have an inverse n^{-1}, which cannot be congruent to n, 1 or $p - 1$. If we pick such an n, we see that in addition to n, n^{-1} must also occur in the product $(p - 1)!$. Thus we can cancel n and n^{-1} in this product. If we now take a remaining factor that is not 1 or $p - 1$, we see that its inverse must by the uniqueness of inverses be distinct from n and n^{-1}, and so must occur in the remaining factors. In this way, any factor of $(p - 1)!$ that is not 1 or $p - 1$ is canceled by its inverse, and so $(p - 1)! \equiv 1 \cdot (p - 1) \equiv -1(\text{mod p})$.