Solutions to Homework 10

§6.3 #2. *Use Corollary 3.6 to give another proof of Fermat's little theorem, Proposition 3.3 of Chapter 1.*

Let p be a prime number, and let $a \in \mathbb{Z}_p$. We want to prove that $a^p = a$. If $a = 0$ then this is clear, so we focus on the case where $a \neq 0$.

Because p is prime, $\mathbb{Z}_p$ is a field, so the group of units $\mathbb{Z}_p^\times$ is just $\mathbb{Z}_p \setminus \{0\}$, which has order $p - 1$. Thus for all $a \in \mathbb{Z}_p^\times$ we have $a^{p-1} = 1$ by Corollary 3.6. Multiplying through by a we get $a^p = a$, as desired.

§6.3 #25. *Let p be an odd prime. Prove that x^2+1 has a root in $\mathbb{Z}_p$ if and only if $\mathbb{Z}_p^\times$ contains an element of order 4. Now infer that $p \equiv 1 \pmod 4$.*

First suppose that $a \in \mathbb{Z}_p$ satisfies $a^2 + 1 = 0$. Then $a^2 = -1$, so $a^4 = 1$, so a has order 1, 2, or 4. (It cannot have order 3: if $a^3 = 1$ and $a^4 = 1$ then we can divide to get $A = 1$, so a had order 1.) If a has order 1 or 2 then $a^2 = 1$, so $1 = -1$, so $p = 2$, but we assumed that p was odd. Thus a has order 4 as an element of $\mathbb{Z}_p^\times$.

Conversely, suppose that $\mathbb{Z}_p^\times$ contains an element a of order 4. Then $a^4 = 1$, so $a^2 = \pm 1$. But we've assumed that a does not have order 2, so $a^2 \neq 1$, so $a^2 = -1$. Thus a is a root of $x^2 + 1$.

By Corollary 3.4, the order of an element divides the order of the group, so if $\mathbb{Z}_p^\times$ has an element of order 4 then 4 divides $|\mathbb{Z}_p^\times| = p - 1$, so $p \equiv 1 \pmod 4$.