MA 453
Homework b

1. Suppose that $a, b \in U(p)$

   then $sq(ab) = (ab)^2 = a^2b^2 = sq(a)sq(b)$

   Hence group morphism

   Next, define $ker = \{a \in U(p) : a^2 \equiv 1(mod\,\text{p})\}$

   so if $a^2 \equiv 1 \text{ mod } p \Rightarrow a^2 - 1 \equiv 0 \text{ mod } p \Rightarrow (a-1)(a+1) \equiv 0 \text{ mod } p$

   so p is prime we are in a field and one of the factors is 0 mod p

   so, $a \equiv 1 \text{ mod } p$ or $a \equiv -1 \text{ mod } p$

   Since $p > 3 \Rightarrow 1 \neq -1$, so there are only two distinct elements.

   $Ker(sq) = \{1, -1\}$

   $$|U^2(p)| = |im(sq)| = \frac{|U(p)|}{|Ker(sq)|} = \frac{p-1}{2}$$

2. Suppose that $a, b \in U(p)$ and that $a, b \notin U^2(p)$

   By problem 1 $\Rightarrow U^2(p)$ is a subgroup of index 2

   so $U(p)$ splits into two cosets

   $U(p) = U^2(p) \cup cU^2(p)$

   so for fixed $c \notin U^2(p)$, all elements not in $U^2(p)$ are in $cU^2(p)$

   so for a, b, there are some $h_1, h_2 \in U^2(p)$ such that

   $a = ch_1$ and $b = ch_2$

   $ab = ch_1 \cdot ch_2 = c^2 h_1 h_2$

   and $c^2 \in U^2(p)$ and $h_1 h_2 \in U^2(p)$ because it is a subgroup

   Therefore, $ab \in U(p)U(p) = U^2(p)$

   What this means is that non-square times non-square gives a square

3. Suppose that $k \in U(p)$ such that $k^2 = -1 \bmod p$

   then $x^4 + 1 = x^4 - (-1) \equiv x^4 - k^2$

   so, $x^4 + 1 \equiv (x^2 - k)(x^2 + k)$ factors into two quadratics

4. Suppose that there is $k \in U(p)$

   such that $k^2 \equiv -2 \bmod p$

   $x^4 + 1 = x^4 - 2x^2 + 1 - (-2)x^2 = (x^2 - 1)^2 - (-2)x^2$

   $\equiv (x^2 - 1)^2 - (k^2)x^2$

   $= ((x^2 - 1) + (kx))((x^2 - 1) - (kx))$

   $= (x^2 - 1 + kx)(x^2 - 1 - kx)$

5. Suppose that $k \in U(p)$ such that k^2 mod p

   $x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2 + 1)^2 - 2x^2$

   $\equiv (x^2 + 1)^2 - (k^2)x^2$

   $= ((x^2 + 1) + (kx))((x^2 + 1) - (kx))$

   $= (x^2 + 1 + kx)(x^2 + 1 - kx)$