Hint for Problem 37.

Try a concrete approach .....

Here are some brief hints on the problem that Aven and Max asked me about. Comments on the difficulty of proof follow the statements of the lemma.

Ex 37: Let p be an odd prime, find representatives for the quotient group $\mathbb{Q}_p^*/(Q_p^*)^2$

Prove a series of lemmas.

Lemma 1. *Every class in $\mathbb{Q}_p^*/(Q_p^*)^2$ has a representative in $\mathbb{Z}_p$.*

(Easy.)

Lemma 2. *Prove that every element $x \in \mathbb{Z}_p^*$ satisfying $x \equiv 1 \pmod p$ is an square in $\mathbb{Z}_p^*$. That is, $x \in (\mathbb{Z}_p^*)^2 \subset (\mathbb{Q}_p^*)^2$.*

(Easy, if you take the right approach.)

Lemma 3. *Prove that every coset in $\mathbb{Q}_p^*/(Q_p^*)^2$ can be represented by an element $x \in \mathbb{Z}_p$ whose canonical expansion is of one of the following forms*

$$x = a_0 \quad \textit{OR} \quad x = a_1 p,$$

where $a_0, a_1 \neq 0$.

(Medium: This requires that you combine the results in the previous two lemmas. In particular, you need to apply Lemma 1 in a precise way.)

To continue, note first that, *a priori*, it looks like we have $2(p-1)$ equivalence classes for the group $\mathbb{Q}_p^*/(Q_p^*)^2$. However, it will turn out that there are exactly two equivalence classes represented by p-adic integers of the form a_0, and two by p-adic integers of the form $a_1 p$. Using the book's hint, we know that the four representative are 1, c, p, cp, where c is a quadratic non-residue $\pmod p$. Towards this end, note that any a_0 that is a quadratic residue $\pmod p$ is in the same equivalence class as 1. (Easy.) Then prove something like the following

Lemma 4. *Suppose c, c' are in the set $\{1, \ldots, p-1\}$ and both are quadratic non-residues $\pmod p$, then $c \sim c'$ in $\mathbb{Q}_p^*/(Q_p^*)^2$.*

(I can think about a few ways to do this, but they all boil down to proving that the map $\varphi : \mathbb{F}_p^* \to \{\pm 1\}$ given by $a_0 \mapsto \begin{cases} 1, & \text{if } a_0 \text{ is a quadratic residue} \pmod p \\ -1, & \text{if } a_0 \text{ is a quadratic non-residue} \pmod p \end{cases}$ is a surjective group homomorphism with kernel equal to ..... and then using Hensel's Lemma again.)

Now finish .....