Comments on Problem 44.

Ex 44: Prove that $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and that representatives for the cosets are given by $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.

First note that by by Exercise 42, a unit u of $\mathbb{Z}_2$ is a square if, and only if $u \equiv 1 \pmod 8$. Moreover, by lemmas we developed for the solution to problem 37, we know that every coset in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ can be represented by an element in $\mathbb{Z}_2$ whose first non-zero digit is either in the 'units' place or in the '2's place. That is, the representative has canonical expansion beginning either as $10_\wedge$ or as $1_\wedge$. We will again use the symbol $\sim$, for example, $a \sim b$, to mean that a and b are in the same coset in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. To tackle finding a complete set of representatives, we consider first the case that the representative u is a unit in $\mathbb{Z}_2$.

Lemma 1. *Suppose $u \in \mathbb{Z}_2$ is a unit and $u = \ldots u_3 u_2 u_1 1_\wedge$, then $u \sim u_2 u_1 1_\wedge$ in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$.*

Proof. Suppose u is as given. We will show that $u = (u_2 u_1 1_\wedge)(\ldots a_4 a_3 001_\wedge)$ where the digits a_i are to be determined. Establishing this shows that $u \sim u_2 u_1 1_\wedge$ since $\ldots a_4 a_3 001_\wedge$ is a square in $\mathbb{Q}_2$ and completes the proof.

The proof is by induction; specifically we show that we can solve for a_{i+1} when $a_i, a_{i-1}, \ldots, a_3$ are known. We begin by illustrating the first few steps, from which the general pattern is clear. Consider the multiplication problem:

$$
\begin{array}{cccccccc}
\ldots & a_6 & a_5 & a_4 & a_3 & 0 & 0 & 1_\wedge \\
 & & & & & u_2 & u_1 & 1_\wedge \\
\hline
\ldots & a_6 & a_5 & a_4 & a_3 & 0 & 0 & 1_\wedge \\
\ldots & a_5u_1 & a_4u_1 & a_3u_1 & 0 & 0 & u_1 & \\
\ldots & a_4u_2 & a_3u_2 & 0 & 0 & u_2 & & \\
\hline
\ldots & u_6 & u_5 & u_4 & u_3 & u_2 & u_1 & 1_\wedge
\end{array}
$$

Clearly, we should take $a_3 = u_3$. Substituting this back into the multiplication problem, we solve for a_4 as the solution to the linear equation $a_4 + a_3 u_1 = u_4$. With a_3 and a_4 known, we solve for a_5 as the solution to $a_5 + a_4 u_1 + a_3 u_2 + a_4 a_3 u_1 = u_5$. Note that the product $a_4 a_3 u_1$ only equals 1 if both a_4 and $a_3 u_1$ are one. In this case, we need to 'carry' the 1. The general case is now clear. With a_j for $j = 3, \ldots, i$ known, set a_{i+1} to be the solution to $a_{i+1} + a_i u_1 + a_{i-1} u_2 + I(a_i + a_{i-1} u_1 + a_{i-2} u_2) = u_{i+1}$, where I denotes the indicator function for the sum. That is, I takes on the value 1 exactly when you need to carry a 1. ☐

Lemma 2. *Suppose $x = \ldots x_3 x_2 10_\wedge \in \mathbb{Z}_2$ is $2u$ for $u \in \mathbb{Z}_2^*$, then $x \sim x_3 x_2 10_\wedge$ in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$.*

Proof. Multiply x by 2^{-1} and apply the last lemma. ☐

Combining Lemmas 1 and 2, a complete set of representatives is found among the set

$$\{u_2 u_1 1_\wedge,\ u_3 u_2 10_\wedge \mid u_i = 0, 1\}, \tag{1}$$

which is a set with **eight** elements.

Proof of Exercise 44. Note that by Exercise 42, we know that the squares in $\mathbb{Q}_2$ are **exactly** those numbers congruent to $1 \pmod 8$, so no two elements in the set in (1) are equivalent in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. (If you don't see this immediately $a \sim b$ only if the three right-most non-zero digits in the canonical expansions of a and b agree, and that the units place also agrees. This is what it 'means' to agree up to a square of the form $\ldots 001_\wedge$.)

Working out the values of the elements in (1), the units are 1, 3, 5, 7, and the non-units are 2, 6, 10, 14. See if you can match these up with Katok's suggestions for generators of $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. If you follow this proof, you should be able to do this. If you can't, ...

Finally, since the square of every class in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ is the identity element, by the Fundamental Theorem of Finite Abelian groups $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ is isomorphic to three copies of $\mathbb{Z}/2\mathbb{Z}$. $\square$