Comments on HW 8.

Ex 33: Determine the sign of $r \in \mathbb{Q}$ by considering the canonical p-adic expansion of r.

Multiplying $r \in \mathbb{Q}$ by the appropriate power of p^k makes the product $r = p^k q$ a p-adic integer and does not change the sign of r since $p^k > 0$. Thus, we may assume $r \in \mathbb{Q} \cap \mathbb{Z}_p$.

It is not hard to show that you can assume that the non-repeated part b of a canonical p-adic expansion can be assumed to be the same length as the repeating part a. You can either consider cases (length $a =$ length b, or not) or consider the repeating pattern given by $a \cdot \dfrac{\operatorname{lcm}(a,b)}{a}$ and the non-repeating part $b \cdot \dfrac{\operatorname{lcm}(a,b)}{b}$. These both have the same length $\operatorname{lcm}(a,b)$.

By these observations, we may assume that r is a rational p-adic integer with the length of the repeating part a the same as the length of the non-repeating part b. Call this length ℓ. Then, using Σ-notation we have

$$x = b + \sum_{i=1}^{\infty} a \cdot (p^\ell)^i.$$

Summing the convergent infinite series,

$$x = b + a\frac{p^\ell}{1-p^\ell} = \frac{(a-b)p^\ell + b}{1-p^\ell}.$$

Note that the denominator $1 - p^\ell < 0$ and $b < p^\ell$ since b's p-adic expansion has ℓ digits in it. Thus, $x > 0$ if, and only if, the expression $a - b < 0$, or $b > a$ as needed.

Ex 37: Let p be an odd prime, find representatives for the quotient group $\mathbb{Q}_p^*/(Q_p^*)^2$ and show that this group is of order 4. We will show something additional: This group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

As the proof of this problem is rather complicated, we will prove a series of lemmas needed in the solution. The symbol p will denote an odd prime throughout.

Lemma 1. *If $\mathbb{F}_p^*$ denotes the multiplicative group of the finite field with p elements, then 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. Thus, $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2 \cong \{\pm 1\}$ as groups.

Proof. Since $\mathbb{F}_p^*$ is a multiplicative subgroup of a field, it is cyclic. Let ξ be a generator for the group, and note that the map φ sends $\xi^{2k} \mapsto 1$, and $\xi^{2k+1} \mapsto -1$. If $\xi^k, \xi^l \in \mathbb{F}_p^*$, then it is easy to see that $\varphi(\xi^k \xi^l) = \varphi(\xi^{k+l}) = \varphi(\xi^k)\varphi(\xi^l)$, by considering all the parities of k, l (both k, l even; both k, l odd; exactly one of k, l odd). The second statement follows from the First Isomorphism Theorem for groups. $\square$

Before continuing we make a few observations about the significance of Lemma 1. A first consequence is that the number of quadratic residues $\pmod p$ equals the number of quadratic non-residues $\pmod p = \frac{p-1}{2}$. Secondly, since φ is a homomorphism, we see that the product of two non-residues is a residue $\pmod p$, the product of a residue and a non-residue is a non-residue $\pmod p$, etc. Finally, *and this will be a key ingredient in our proof*, since every quadratic residue is in the identity coset in $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$, and every quadratic non-residue is in the non-trivial coset in $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$, it follows that if c, c' are both quadratic non-residues $\pmod p$, then $c \equiv c'u^2 \pmod p$ for some $u^2 \in (\mathbb{F}_p^*)^2$.

We now prove a series of lemmas that were outlined in office hours.

Lemma 2. *Every class in $\mathbb{Q}_p^*/(Q_p^*)^2$ has a representative a in $\mathbb{Z}_p$ whose canonical $p$adic expansion is of the form $a = a_0 + a_1 p + \cdots$ where $a_0 \neq 0$, or $a_0 = 0$ and $a_1 \neq 0$.*

Proof. Let $b \in \mathbb{Q}_p$ be a representative for a coset in $\mathbb{Q}_p^*/(Q_p^*)^2$. If $b = \ldots b_2 b_1 b 0_\wedge b_{-1} b_{-2} \ldots b_{-m}$ where $b_{-m} \neq 0$, then multiply b by p^m if m is even, or by p^{m+1} if m is odd to get $a \in \mathbb{Z}_p$. In the first case, the first non-zero digit in the canonical expansion of a is b_{-m} and is located in the units place (a_o). In the second case, the canonical expansion of a looks like $a = \cdots b_{-m+1} b_{-m} 0_\wedge$. To finish, note that a and b are in the same coset in $\mathbb{Q}_p^*/(Q_p^*)^2$ since they differ by multiplication by a square. ☐

Lemma 3. *Every element $x \in \mathbb{Z}_p^*$ satisfying $x \equiv 1 \pmod p$ is an square in $\mathbb{Z}_p^*$. That is, $x \in (\mathbb{Z}_p^*)^2 \subset (\mathbb{Q}_p^*)^2$.*

Proof. This is a straight-forward application of Hensel's Lemma, but you should give the details. ☐

Lemma 4. *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 $a_0, a_1 \neq 0$.

Proof. Using Lemma 2, suppose first that a represents a class in $\mathbb{Q}_p^*/(Q_p^*)^2$ where a has canonical p-adic expansion $a = \cdots a_2 a_1 a_{0\wedge}$, where $a_0 \neq 0$. Then a_0 has an inverse $\pmod p$ (or if you prefer, it has an inverse in $\mathbb{Z}_p^*$) and

$$\begin{aligned} a &= a_0\,(1 + a_0^{-1} a_1 p + a_0^{-1} a_2 p^2 + \cdots) \\ &= a_0\;\, u^2 \end{aligned}$$

by Lemma 3.

Now suppose a has canonical p-adic expansion of the form $a = \sum_{i=1}^{\infty} a_i p^i$ for $a_1 \neq 0$, then

$$a = a_1 p\,(1 + a_0^{-1} a_2 p + a_0^{-1} a_3 p^2 + \cdots) = a_1 p\; u^2,$$

again by Lemma 3. This shows that every class in $\mathbb{Q}_p^*/(Q_p^*)^2$ has a representative of the form a_0 or $a_1 p$ where $a_0, a_1 \neq 0$. ☐

We next show that any two quadratic non-residues represent the same element in $\mathbb{Q}_p^*/(Q_p^*)^2$.

Lemma 5. *Suppose c, c' are in the set $\{1, \ldots, p-1\}$ and both are quadratic non-residues $\pmod p$, then c and c' are in the same coset in $\mathbb{Q}_p^*/(Q_p^*)^2$. That is, any two quadratic non-residues $\pmod p$ represent the same element in $\mathbb{Q}_p^*/(Q_p^*)^2$.*

Proof. Since $(c, p) = 1$, c has an inverse in $\mathbb{Z}_p^*$. Consider the polynomial $F(x) = x^2 - c'c^{-1} \in \mathbb{Z}_p[x]$. Using Hensel's Lemma, note that $F(x)$ has a root $(\text{mod } p)$ by Lemma 1 and that $F'(x) \equiv 0 \,(\text{mod } p)$ from which it follows that $F(x)$ has a unique root $u \in Z_p$. Thus, $c'c^{-1} = u^2$ and $c' = c'u^2$. □

Now .....

Theorem 6. *The group* $\mathbb{Q}_p^*/(Q_p^*)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}2\mathbb{Z}$ *and has elements* $\{\mathbb{Q}_p^2,\ c\mathbb{Q}_p^2,\ p\mathbb{Q}_p^2,\ cp\mathbb{Q}_p^2\}$ *where* c *is a quadratic non-residue* $(\text{mod } p)$.

Proof. For simplicity, we work with representatives of the cosets, and $a \sim b$ means $a\mathbb{Q}_p^2 = b\mathbb{Q}_p^2$. It is clear that any two quadratic residues $(\text{mod } p)$ are represented by 1, and by Lemma 5 that $c \sim c'$ for any two quadratic non-residues $(\text{mod } p)$. Combining this with Lemma 4, the set $\{1, c, p, cp\}$ must contain a complete set of representatives for $\mathbb{Q}_p^*/(Q_p^*)^2$. Clearly, $1 \nsim c$, and $1 \nsim p$ since both c and p are not squares in $\mathbb{Q}_p^*$. It is also the case that $c \nsim p$, since $|c|_p = 1$ and $|p|_p = \frac{1}{p}$ and if c and p were to differ by a square, then their norms would differ by an *even* power of $\frac{1}{p}$. (Stated otherwise, $c = u^2p^{2k}p$ which is impossible.) Since $\mathbb{Q}_p^*/(Q_p^*)^2$ is a group, the product cp is also in $\mathbb{Q}_p^*/(Q_p^*)^2$.

A moments's thought yields that we have actually shown that the cosets represented by c, p generate $\mathbb{Q}_p^*/(Q_p^*)^2$. Since $c^2 \sim 1$, and $p^2 \sim 1$ in $\mathbb{Q}_p^*/(Q_p^*)^2$, this group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Ex 40: The statement of the stronger version of Hensel's Lemma had two typos in it. **Correct** these if you have not already done so.