Introduction to the p-adic numbers
Exercise Sheet 3

Ross Paterson

This exercise sheet is split into sections:

B theoretical questions which use only major results/definitions in the course;
C theoretical results requiring some thought.

Section B

1. Find the number of roots in $\mathbb{Q}_p$ of $f(X) = X^2 + 6X + 1$ for:
   (a) $p = 3$?
   (b) $p = 5$?
   (c) $p = 7$?
2. Find the number of roots in $\mathbb{Q}_p$ of $f(X) = X^2 + \frac{1}{2}X - \frac{1}{4}$ for
   (a) $p = 2$?
   (b) $p = 3$?
   (c) $p = 5$?
3. Is 2 a square in $\mathbb{Q}_p$ for
   (a) $p = 2$?
   (b) $p = 3$?
   (c) $p = 7$?
4. Assume that p is an odd prime number. Define the sequence $a_n := p^n + 1$ for $n \geq 1$.
   (a) Is the sequence $(a_n)_n$ Cauchy?
   (b) Show that for all $n \geq 1$ the element $a_n \in \mathbb{Q}_p$ is a square, and that there exists a unique square root $\sqrt{a_n} \in \mathbb{Z}_p$ such that $\sqrt{a_n} \equiv 1 \mod p$.
   (c) Is the sequence of these square roots $(\sqrt{a_n})_n$ Cauchy?

Section C

5. Show that -1 is a square in $\mathbb{Q}_p$ if and only if $p \equiv 1 \mod 4$
6. Let $\mathbb{Z}_p^\times := \left\{ x \in \mathbb{Q}_p \ : \ |x|_p = 1 \right\}$ be the unit circle in $\mathbb{Q}_p$, and recall that $\mathbb{Q}_p^\times := \mathbb{Q}_p \setminus \{0\}$. Assume that p is an odd prime.
   (a) Show that $\mathbb{Z}_p^\times$ is a group under multiplication, and the reduction map $\mathbb{Z}_p^\times \to \mathbb{Z}/p\mathbb{Z}^\times$ is a surjective group homomorphism.
   (b) Show that $x \in \mathbb{Z}_p^\times$ is a square if and only if x is a square modulo p.
   (c) Show that
   $$\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

[Note how different this is to the situation for the rationals: $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is infinite!]

7. Fermat's Last theorem, a celebrated result of Andrew Wiles from 1995, states that for $n \geq 3$ the only solutions $x, y, z \in \mathbb{Q}$ to
$$x^n + y^n = z^n,$$
are the ones whose product satisfies $xyz = 0$. Assuming that $p \nmid n$, show that there exist solutions $x, y, z \in \mathbb{Q}_p$ such that $xyz \neq 0$ (i.e. Fermat's last theorem is false in $\mathbb{Q}_p$).

8. Show that y is a simple root of a polynomial $f(X)$ over $\mathbb{Q}_p$ if and only if $f(X) = (X - y)G(X)$ for some polynomial $G(X)$ such that $G(y) \neq 0$.