2015-09-28 Problems

Introduction to Number Theory

References:
"Number Theory 1: Fermat's dream" Kato, Kurokawa, Saito, Chapter 2.
"p-adic numbers, p-adic analysis and zeta functions" Koblitz, Chapter 1.

1.1. Find $a, b \in \mathbb{Q}$ such that $\operatorname{ord}_p(a+b) \neq \operatorname{ord}_p(a)$ and $\operatorname{ord}_p(a+b) \neq \operatorname{ord}_p(b)$.
1.2. Let $a, b \in \mathbb{Q}$. Let p be a prime number. Prove the following statements:
1.2.1. $\operatorname{ord}_p(ab) = \operatorname{ord}_p(a) + \operatorname{ord}_p(b)$
1.2.2. $\operatorname{ord}_p(a+b) \leq \min\{\operatorname{ord}_p(a), \operatorname{ord}_p(b)\}$
1.2.3. $\operatorname{ord}_p(a+b) = \min\{\operatorname{ord}_p(a), \operatorname{ord}_p(b)\}$ if $\operatorname{ord}_p(a) \neq \operatorname{ord}_p(b)$.

2.1. Compute the p-adic expansion of $-1 \in \mathbb{Q}_7$.
2.2. Compute the p-adic expansion of -1 for general p.

3.1. Show that $(1 - 5 + 5^2 - 5^3 + \cdots + (-5)^{n-1}) \cdot 6 \equiv 1 (\operatorname{mod} 5^n)$.
3.2. Find the inverse of 4 in $\mathbb{Z}/3^4\mathbb{Z}$.
3.3. Compute the p-adic expansion of $(p+1)^{-1}$.

4. Compute the first 3 digits of the p-adic expansion of -2 in $\mathbb{Q}_5$

5.1. Show that there exist two square roots of 6 in $\mathbb{Q}_5$. Compute the first 4 digits of their 5-adic expansions.
5.2. Let $a \in \mathbb{Z}$ be an integer such that $a \equiv \pm 1 (\operatorname{mod} 5)$. Show that a square root of a exists in $\mathbb{Q}_5$.

6.1. Prove that there exists a square root of -1 in $\mathbb{Q}_p$ if and only if $p \equiv 1 (\operatorname{mod} 4)$.
6.2. Prove that there exists a square root of -2 in $\mathbb{Q}_p$ if and only if $p \equiv 1, 3 (\operatorname{mod} 8)$.

7.1. Find 3 quadratic extensions of $\mathbb{Q}_5$.
7.2. Show that there exist 3 quadratic extensions of $\mathbb{Q}_p$ when $p \neq 2$.

8. Let $n \in \mathbb{N}$.
8.1. Let $[x]$ denote the largest integer $\leq x$. Show that

$$\operatorname{ord}_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right].$$

8.2. Show that $\log_p n \geq \operatorname{ord}_p n$.

9. Let p be an odd prime. Find a sequence $(x_n)_{n \geq 1}$ of rational numbers that converges to 1 in $\mathbb{R}$ and to 0 in $\mathbb{Q}_p$.

10. Let p be prime. Let $m \geq 2$ if $p = 2$ and $m \geq 1$ if $p \neq 2$. We have maps

$$\log : 1 + p^m\mathbb{Z}_p \to p^m\mathbb{Z}_p, \quad \exp : p^m\mathbb{Z}_p \to 1 + p^m\mathbb{Z}_p.$$

Prove the following statements (may look at the proof for $\mathbb{R}$ or for $\mathbb{C}$):
10.1. $\exp(x + y) = \exp(x)\exp(y)$.
10.2. $\log(ts) = \log(t) + \log(s)$
10.3. $\log(\exp(t)) = t$
10.4. $\exp(\log(x)) = x$

11. Let $a \in \mathbb{Q}_p^\times$.
11.1 Let $(x_n)_{n\geq 1}$ be a Cauchy sequence of rational numbers that converges to a.
Show that the p-adic order becomes constant for large n, i.e., show that there exists N such that $\mathrm{ord}_p(x_N) = \mathrm{ord}_p(x_{N+1}) = \cdots$.
11.2. If $(y_n)_{n\geq 1}$ is another Cauchy sequence converging to a, show that the constant values are equal. That is, show that $\mathrm{ord}_p(x_n) = \mathrm{ord}_p(y_n)$ for n large.

12. We use the constant in Problem 11 and define $\mathrm{ord}_p(a)$ to be that constant for $a \in \mathbb{Q}_p$.
12.1. Suppose the p-adic expansion is given by $a = a_m p^m + a_{m+1}p^{m+1} + \cdots$ with $a_m \neq 0$. Show that $\mathrm{ord}_p(a) = m$.
12.2. Prove the statements 1.2.1-1.2.3 for $a, b \in \mathbb{Q}_p$.
12.3. Set $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid \mathrm{ord}_p\, a \geq 0\}$. Show that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. Give a nonzero noninvertible element.

13.1 Show that $\mathbb{Z}_p \subset \mathbb{Q}_p$ is open and closed.
13.2 Show that $p^m\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid \mathrm{ord}_p\, a \geq m\}$.
13.3 Show that $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$.
13.4 Show that $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$.
13.5 Show that the group homomorphisms

$$\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}_{(p)}/p^m\mathbb{Z}_{(p)} \to \mathbb{Z}_p/p^m\mathbb{Z}_p$$

induced by the inclusions $\mathbb{Z} \subset \mathbb{Z}_{(p)} \subset \mathbb{Z}_p$ are isomorphisms.
13.6. Show that the closure of $\mathbb{Z}_{(p)}$ in $\mathbb{Q}_p$ equals $\mathbb{Z}_p$.
13.7. Show that the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ equals $\mathbb{Z}_p$.