MATH 7230 Homework 11

Andrea Bourque

April 2021

1 Problem 9.4 1

Show that a rational number a/b is a p-adic integer iff p does not divide b.

Proof. a/b is a p-adic integer if and only if $v(a/b) = v(a) - v(b) \geq 0$, by definition. Since the fraction is in reduced terms, $v(a) = 0$ or $v(b) = 0$. $p \mid b$ if and only if $v(b) > 0$. Then $p \mid b$ if and only if $v(a) = 0$. Then $p \mid b$ if and only if $v(a/b) = v(a) - v(b) = -v(b) < 0$, which is true if and only if a/b is not a p-adic integer. $\square$

2 Problem 9.4 2

With $p = 3$, express the product of $(2+p+p^2)$ and $(2+p^2)$ as a p-adic integer.

Proof. $(2+p+p^2)(2+p^2) = 4+2p^2+2p+p^3+2p^2+p^4 = 4+2p+4p^2+p^3+p^4 = (1+p)+2p+(1+p)p^2+p^3+p^4 = 1+3p+p^2+p^3+p^3+p^4 = 1+p^2+p^2+2p^3+p^4 = 1+2p^2+2p^3+p^4$. □

3 Problem 9.4 3

Express the p-adic integer -1 as an infinite series.

Proof. $-1 = -1 + p - p + p^2 - p^2 + p^3 - ... = (p-1) + (p-1)p + (p-1)p^2 + ...$ Notice then that $0 = 1 - 1 = 1 + (p-1) + (p-1)p + (p-1)p^2 + ... = p + (p-1)p + (p-1)p^2 + ... = pp + (p-1)p^2 + ... = pp^2 + ...$ That is, adding one to both sides creates an infinite telescoping effect which results in a p-adic integer with arbitrarily high degree. □

4 Problem 9.4 4

Show that the sequence $a_n = n!$ of p-adic integers converges to 0.

Proof. We show equivalently that $b_n = v(a_n)$ diverges to $+\infty$. By the multiplicative property of the valuation, $b_n = \sum_{i=1}^{n} v(i)$. Then $b_{n+1} - b_n = v(n+1) \geq 0$. Since $v(pn) = v(p) + v(n) = 1 + v(n) \geq 1 > 0$, we have $b_{n+p} - b_n = v(n+1) + ... + v(n+p) > 0$, since one of the numbers $n+1, ..., n+p$ will be divisible by p. Therefore b_n is monotone increasing and not eventually constant. It follows that b_n diverges to ∞. $\square$

5 Problem 9.4 5

Does the sequence $a_n = n$ of p-adic integers converge?

Proof. No. For $p \nmid n$, $|a_n| = 1$, and for $p \mid n$, $|a_n| < 1$. This is regardless of how large n is. $\square$

6 Problem 9.4 6

Show that the p-adic power series for $\log(1+x)$, $\sum_{n=1}^{\infty}(-1)^{n+1}x^n/n$, converges in $\mathbb{Q}_p$ for $|x| < 1$ and diverges elsewhere.

Proof. Notice that $p^{v(n)}|n$, so $p^{v(n)} \leq n$, so $v(n) \leq \log n / \log p$. Thus $v(n)/n \leq \log n/(n \log p) \to 0$.

Writing $\log(1+x) = \sum_{n=1}^{\infty} a_n x^n$, we have $|a_n| = |1/n| = p^{v(n)}$. By the nth root test, we determine $\lim_{n\to\infty} |a_n|^{1/n} = \lim_{n\to\infty} p^{v(n)/n} = p^0 = 1$. Therefore the radius of convergence is 1. $\square$

7 Problem 9.4 7

Show that the p-adic valuation of $n!$ is at most $n/(p-1)$.

Proof. $v(n!) = \sum_{i=1}^{\infty} \lfloor n/p^i \rfloor \le \sum_{i=1}^{\infty} n/p^i = \frac{n}{p}\frac{1}{1-1/p} = n/(p-1)$. $\square$

8 Problem 9.4 8

Show that the p-adic valuation of $(p^m)!$ is $(p^m - 1)/(p - 1)$.

Proof. $v((p^m)!) = \sum_{i=1}^{\infty} \lfloor p^m/p^i \rfloor = \sum_{i=1}^{m} p^{m-i} = p^m(p^{-1}+...+p^{-m}) = p^m p^{-1} \frac{1-p^{-m}}{1-p^{-1}} = \frac{p^m-1}{p-1}$. $\square$

9 Problem 9.4 9

Show that $\sum_{n=0}^{\infty} x^n/n!$ converges for $|x| < p^{-1/(p-1)}$, and diverges elsewhere.

Proof. Let $a_n = 1/n!$. Then $|a_n| = p^{v(n!)} \leq p^{n/(p-1)}$ by Problem 7. Then $|a_n|^{1/n} \leq p^{1/(p-1)}$, which is a fixed bound. By considering prime powers as in Problem 8, we can get arbitrarily close to this bound. Thus the radius of convergence is $p^{-1/(p-1)}$. For $|x| = p^{-1/(p-1)}$, so $v(x) = 1/(p-1)$. Then $v(x^n/n!) = nv(x) - v(n!) = n/(p-1) - v(n!)$. In particular, for $n = p^m$, we have $p^m/(p-1) - (p^m - 1)/(p-1) = 1/(p-1)$. Thus, there are infinitely many terms with the same absolute value in the series, so it does not converge. It follows that $|x| < p^{-1/(p-1)}$ is the interval of convergence. $\square$

10 Problem 9.5 1

Show that for any prime p, there are $p-1$ distinct $(p-1)$th roots of unity in $\mathbb{Z}_p$.

Proof. By Corollary 9.5.3, the $(p-1)$ solutions to $X^{p-1}-1=0$ in $\mathbb{Z}/p\mathbb{Z}$ lift to unique solutions in $\mathbb{Z}_p$. $\square$

11 Problem 9.5 2

Let p be an odd prime not dividing m. Describe an effective procedure for determining whether m is a square in $\mathbb{Z}_p$.

Proof. Let $f(X) = X^2 - m$. Since $p > 2$, $f'(X) = 2X$ is relatively prime to $f(X)$, so there are no repeated roots. By corollary 9.5.3, m is a square in $\mathbb{Z}_p$ if and only if m is a square in $\mathbb{Z}/p\mathbb{Z}$. $\square$

12 Problem 9.5 3

Indicate how to find the series representation of $\sqrt{m}$ and illustrate with an example.

Proof. We first solve $a_0^2 = m \mod p$. Then, we solve $(a_0 + a_1 p)^2 = m \mod p^2$. And so on.

Let $p = 7$, $m = 11$. $a_0^2 = 11 \mod 7$ gives $a_0 = 2, 5$. We take $a_0 = 2$. Then $(2 + 7a_1)^2 = 11 \mod 7^2$ gives $4 + 28a_1 = 11 \mod 49$, so $a_1 = 2$. Then $(2 + 2 \cdot 7 + 49a_2)^2 = 11 \mod 7^3$ gives $256 + 2 \cdot 16 \cdot 49a_2 = 11 \mod 343$ gives $a_2 = 4$. $(2 + 2 \cdot 7 + 4 \cdot 49 + 343a_3)^2 = 11 \mod 7^4$ gives $a_3 = 4$.

It seems that each iteration gives $a_i = (a_0 + a_1 p + ... + a_{i-1} p^{i-1})^{-1} \mod 7$. $\square$