Exercise for "p-adic functions on $\mathbb{Z}_p$"

There will be four sets of exercises/problems for the CTNT 2020 lectures on p-adic functions. Some partial answers/hints are at the end of the file.

Problem 1.1 (Periodic power series expansion)**.**

(1) Solve $4x = 1$ in $\mathbb{Z}_7$, and write the solution as a "periodic" power series expression in powers of 7.
(2) Use the fact that 5 divides $7^4 - 1$ but not smaller powers of 7 minus to show that $1/5$ in $\mathbb{Z}_7$ admits a 7-adic power series expansion in powers of 7 with period 4.
(3) Recall that every number with a periodic decimal expansion is a rational number. Using the same argument to show that, a p-adic integer is a rational number if and only if it has a "periodic" power series expansion in powers of p.

Problem 1.2 (Proof of Hensel's lemma by example)**.** Consider $f(x) = (x-1)(x-2) - 5$ and let $p = 5$. Then $f(x)$ mod 5 has two simple zeros 1 and 2. Take $\alpha = 1$ as an example. Prove that there exists a unique $\tilde{\alpha} \in \mathbb{Z}_5$ such that $f(\tilde{\alpha}) = 0$ and $\tilde{\alpha} \equiv 1 \bmod 5$, as follows:

(1) First consider modulo 25, setting $x = 1 + 5a$. Solve $f(1 + 5a) \equiv 0 \bmod 25$.

(2) Now jump to the general case, suppose that we have solved $\alpha_n \bmod 5^n$ such that $f(\alpha_n) \equiv 0 \bmod 5^n$. We need to set $x = \alpha_n + 5^n b$ and try to solve $f(x) \equiv 0 \bmod 5^{n+1}$.

Explain why there exists a solution to b modulo 5?

(3) Compute the *formal derivative* $f'(x)$ of $f(x)$ (e.g. $(2x^2)' = 2 \cdot 2x = 4x$). Observe your computation for (2). What's the relation between the coefficient on b at your last step versus evaluation of $f'(x)$ at α mod 5?

Problem 2.1 (All triangles in $\mathbb{Q}_p$ are isoceles)**.** This is stated without proof. Show that given $x, y, z \in \mathbb{Q}_p$, at least two of the distances $|x-y|_p$, $|y-z|_p$, and $|z-x|_p$ are the same.

Problem 2.2 (p-adic powers)**.** Let $x \in p\mathbb{Z}_p$. Show that for every $n \in \mathbb{Z}_p$, the power $(1+x)^n$ makes sense.

(Method 1: viewing as a limit in n). Write out $n = a_0 + a_1 p + a_2 p^2 + \cdots$ and set $n_0 = a_0$, $n_1 = a_0 + a_1 p$, $n_2 = a_0 + a_1 p + a_2 p^2$, $\ldots$. Then we see that $n_i \equiv n_{i+1} \bmod p^n$.

Show that $(1+x)^{n_i} \equiv (1+x)^{n_{i+1}} \bmod p^{i+1}$.

(Method 2: Write out binomial expansion). Recall that when n is an integer, we have

$$(1+x)^n = \sum_{i \geq 0} \binom{n}{i} x^i.$$

Show that this series makes sense as well when $n \in \mathbb{Z}_p$, where $\binom{n}{i}$ is interpreted as $\frac{n(n-1)\cdots(n-i+1)}{i!}$. Show that $\binom{n}{i}$ belongs to $\mathbb{Z}_p$, and therefore the formal binomial expansion above converges when $x \in p\mathbb{Z}_p$.

(3) Show that the two definitions of $(1+x)^n$ above give the same answer.

Problem 2.3 (Compute $\sqrt{2}$ in $\mathbb{Z}_7$ in a much cooler way)**.** We still need that $3^2 \equiv 2 \bmod 7$. Next, we consider the following:

$$\sqrt{2} = 3 \cdot \big(\frac{2}{9}\big)^{1/2} = 3 \cdot \big(1 - 7 \cdot \frac{1}{9}\big)^{1/2}.$$

We already know that $1/9$ exists in $\mathbb{Z}_7$. To show the square root exists, we recall the binomial expansion

$$(1-x)^n = \sum_{i \geq 0} (-1)^i \binom{n}{i} x^i.$$

"Plugging in $n = \frac{1}{2}$ and $x = 7 \cdot \frac{1}{9}$," we have

$$\sqrt{2} = 3 \cdot \sum_{i \geq 0} (-1)^i \binom{1/2}{i} \big(7 \cdot \frac{1}{9}\big)^i, \tag{2.3.1}$$

where $\binom{1/2}{i} = \dfrac{\frac{1}{2}(\frac{1}{2}-1)\cdots(\frac{1}{2}-i+1)}{i!}$ is the formal binomial number.

(1) Show that for every i, the formal binomial number $\binom{1/2}{i} = \dfrac{\frac{1}{2}(\frac{1}{2}-1)\cdots(\frac{1}{2}-i+1)}{i!}$ belongs to $\mathbb{Z}_7$.

(2) Show that (2.3.1) converges in $\mathbb{Z}_7$.

(3) Convince yourself that formally, if $x \in p\mathbb{Z}_p$ and $m, n \in \mathbb{Z}_p$,

$$\Big(\sum_{i \geq 0} (-1)^i \binom{n}{i} x^i\Big) \cdot \Big(\sum_{i \geq 0} (-1)^i \binom{m}{i} x^i\Big) = \Big(\sum_{i \geq 0} (-1)^i \binom{n+m}{i} x^i\Big).$$

Problem 3.1 (Finite dimensional Banach space)**.** Let V be a finite dimensional vector space over $\mathbb{Q}_p$. Fix a basis $e_1, \dots, e_n$ of V. One can define a *standard supnorm* $||\cdot||$ by

$$||a_1 e_1 + \cdots + a_n e_n|| := \max_{1 \le i \le n} \{|a_i|_p\}.$$

(1) Show that this standard supnorm is a Banach norm on V, that is, it satisfies (a) $||av|| = |a|_p \cdot ||v||$ for $a \in \mathbb{Q}_p$, $v \in V$; (b) $||v + w|| \le \max\{||v||, ||w||\}$; and (c) $||v|| = 0$ if and only if $v = 0$. Moreover, V is complete with respect to $||\cdot||$.

(2) Conversely, let $||\cdot||'$ be a norm satisfying conditions (a)(b)(c), and moreover that the values of $||\cdot||'$ belongs to $p^{\mathbb{Z}} \cup \{0\}$. Show that the subset $M := \{v \in V \; ; \; ||v||' \le 1\}$ is a $\mathbb{Z}_p$-submodule of V.

(3) Recall that $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$. Show that $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = V$.

(4) It is known that $\mathbb{Z}_p$ is a PID. Show that there exists an integer N such that

$$p^N \mathbb{Z}_p e_1 \oplus \cdots \oplus p^N \mathbb{Z}_p e_n \subseteq M.$$

(5) Use that $\mathbb{Z}_p$ and hence $\mathbb{Z}_p^n$ is compact to show that there exists an integer N such that

$$M \subseteq p^{-N} \mathbb{Z}_p e_1 \oplus \cdots \oplus p^{-N} \mathbb{Z}_p e_n.$$

From this deduce that there exists $C > 1$ such that, for every $v \in V$

$$C^{-1} \cdot ||v|| \le ||v||' \le C \cdot ||v||.$$

(6) Let $\mathbf{f}_1, \dots, \mathbf{f}_n$ denote a $\mathbb{Z}_p$-basis of M. Show that they form an orthonormal basis of V for the norm $||\cdot||'$.

Problem 3.2 (Another orthonormal basis of $\mathcal{C}(\mathbb{Z}_p; \mathbb{Q}_p)$)**.** This problem comes out from my personal research. Consider the following sequence of (polynomial) functions:

$$f_0(x) = x, \quad f_1(x) = \frac{x^p - x}{p}, \quad f_2(x) = \frac{\left(\frac{x^p - x}{p}\right)^p - \frac{x^p - x}{p}}{p}, \quad \dots \quad f_{n+1}(x) = \frac{f_n(x)^p - f_n(x)}{p}, \dots$$

on $\mathbb{Z}_p$.

(1) Show that for every n and every $x \in \mathbb{Z}_p$, $f_n(x) \in \mathbb{Z}_p$.

(2) For an integer n, we write it as $n_0 + n_1 p + n_2 p^2 + \cdots + n_r p^r$ with $a_i \in \{0, 1, \dots, p-1\}$, we set

$$\mathbf{e}_n(x) := f_0(x)^{n_0} f_1(x)^{n_1} \cdots f_r(x)^{n_r},$$

again, as a (polynomial) function on $\mathbb{Z}_p$. Show that as a polynomial, $\mathbf{e}_n(x)$ has degree n, and if e_n denote the leading coefficient of $\mathbf{e}_n(x)$, then $v_p(e_n) = -v_p(n!)$.

(3) Show (in a completely abstract way) that if we write the Mahler expansion of $\mathbf{e}_n(x)$, all coefficients belong to $\mathbb{Z}_p$. And show (using (2)) that the Mahler coefficient on $\binom{x}{n}$ belongs to $\mathbb{Z}_p^\times$. From this, deduce that $||\mathbf{e}_n(x)|| = 1$.

(4) (Somehow using a completely abstract argument,) show that every $\binom{x}{n}$ is in turn a $\mathbb{Z}_p$- (as opposed to $\mathbb{Q}_p$-) linear combination of $\mathbf{e}_0(x), \dots, \mathbf{e}_n(x)$. And use this to deduce that $\mathbf{e}_0(x)$, $\mathbf{e}_1(x)$, $\dots$ also give an orthonormal basis of $\mathcal{C}(\mathbb{Z}_p; \mathbb{Q}_p)$.

Problem 4.1 (Convolution product)**.** Note that the set of formal power series $\mathbb{Z}_p[\![T]\!]$ is a ring. We now explain what the product structure corresponds to in terms of p-adic measures.

Let μ_1 and μ_2 denote two measures on $\mathbb{Z}_p$ (with values in $\mathbb{Q}_p$). Then we can define a convolution measure $\mu_1 \star \mu_2$ as follows: for every $f(z) \in \mathcal{C}(\mathbb{Z}_p; \mathbb{Q}_p)$, we have

$$\int_{\mathbb{Z}_p} f(z)\mu_1 \star \mu_2(z) := \int_{\mathbb{Z}_p \times \mathbb{Z}_p} f(x+y)\mu_1(x)\mu_2(y).$$

Show that under the Amice transform $A_{\mu_1 \star \mu_2}(T) \in \mathbb{Z}_p[\![T]\!]$ is given by

$$A_{\mu_1 \star \mu_2}(T) = A_{\mu_1}(T) \cdot A_{\mu_2}(T).$$

Problem 4.2 (p-adic L-functions for Dirichlet L-functions)**.** Let N be an integer relatively prime to p, and let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Q}_p^\times$ be a *non-trivial* character. Extend χ to a function on $\mathbb{Z}$ so that

$$\chi(n) := \begin{cases} \chi(n \bmod N) & \text{if } \gcd(n, N) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

The Dirichlet L-function is defined to be

$$L(\chi, s) := \sum_{n \geq 1} \frac{\chi(n)}{n^s}.$$

Consider the measure $\mu_\chi \in \mathcal{D}(\mathbb{Z}_p; \mathbb{Q}_p)$ whose Amice transform is

$$A_{\mu_\chi}(T) := \sum_{i=0}^{N-1} \frac{\chi(i)(1+T)^{N-i}}{(1+T)^N - 1}$$

Show that $A_{\mu_\chi}(T)$ belongs to $\mathbb{Z}_p[\![T]\!]$.

Prove that we have

$$\int_{\mathbb{Z}_p} x^n d\mu_\chi(x) = L(\chi, -n).$$

Hint on Problem 1.1: (2) and (3). Let us explain the idea by examples. When we compute the decimal expansions of a rational number, we can recast the process as follows: (e.g. using $999 = 27 \times 37$)

$$\frac{2}{37} = \frac{54}{999} = 0.054054054054054\cdots$$

Let us elaborate on the last step further:

$$\frac{54}{999} = \frac{54}{1000-1} = \frac{54 \cdot 10^{-3}}{1-10^{-3}} = 54 \cdot 10^{-3}\big(1 + 10^{-3} + 10^{-6} + \cdots\big) = 0.054054054054054\cdots$$

The same argument works for p-adic numbers. For example, we consider $\frac{3}{13}$ in $\mathbb{Z}_5$. For a technical reason, it is more convenient to consider $\frac{3}{13}$ as $1 - \frac{10}{13}$ instead (as we will see). Noting that $5^4 - 1 = 26 \times 24 = 13 \times 48$. Thus

$$-\frac{10}{13} = \frac{-480}{5^4-1} = \frac{480}{1-5^4} = 480 + 480 \times 5^4 + 480 \times 5^8 + \cdots$$

We know that $480 = 5 + 4 \cdot 5^2 + 3 \times 5^3$; so

$$\frac{3}{13} = 1 - \frac{10}{13} = 1 + \big(5 + 4 \cdot 5^2 + 3 \times 5^3\big) + 5^4 \times \big(5 + 4 \cdot 5^2 + 3 \times 5^3\big) + 5^8 \times \big(5 + 4 \cdot 5^2 + 3 \times 5^3\big) + \cdots$$

It is not hard to imitate this to solve (2). For (3), the only essential question is: say we have a rational number $\frac{a}{b}$ with $p \nmid b$, does there exist an integer N such that b divides $p^N - 1$? The answer is yes, because we can turn the table and look at modulo b. The needed number N is precisely the order of the element $p \bmod b$ in the group $(\mathbb{Z}/b\mathbb{Z})^\times$.

Hint on Problem 1.2: (2) Plugging in $x = \alpha_n + 5^n b$, we try to solve

$$(\alpha_n + 5^n b - 1)(\alpha_n + 5^n b - 2) \equiv 5 \bmod 5^{n+1}$$

$$(\alpha_n - 1)(\alpha_n - 2) + 5^n b\big(\alpha_n - 2 + \alpha_n - 1\big) + 5^{2n} b^2 \equiv 5 \bmod 5^{n+1}$$

As 5^{2n} is divisible by 5^{n+1}, we can drop the b^2-term and get

$$(\alpha_n - 1)(\alpha_n - 2) + 5^n b\big(\alpha_n - 2 + \alpha_n - 1\big) \equiv 5 \bmod 5^{n+1}$$

By how α_n is taken, we know that $(\alpha_n - 1)(\alpha_n - 2) - 5$ is divisible by 5^n. So we have

$$\frac{(\alpha_n - 1)(\alpha_n - 2) - 5}{5^n} + b\big(\alpha_n - 2 + \alpha_n - 1\big) \equiv 0 \bmod 5. \tag{4.2.1}$$

The upshot is that $\alpha_n \equiv 1 \bmod 5$, so $\alpha_n - 2 + \alpha_n - 1 \equiv -1 \bmod 5$. So we can always solve for a unique $b \bmod 5$.

(3) Note that $f'(x) = (x-1) + (x-2)$. The coefficients on b in (4.2.1) is precisely $f'(x)|_{x=\alpha_n}$. As we always need α to be a simple zero in Hensel's lemma, $f'(x)|_{x=\alpha_n} \neq 0$ in $\mathbb{F}_p$. This is how Hensel's lemma is proved.

Hint on Problem 2.2: (1) One can, for example, prove inductively that $(1+x)^{p^i}-1$ is divisible by p^{i+1} when $x \in p\mathbb{Z}_p$.

(2) To see that $\binom{n}{i}$ belongs to $\mathbb{Z}_p$, one can observe that when $n \in \mathbb{N}$, this is true. As $\mathbb{N}$ is dense in $\mathbb{Z}_p$, the same holds for $n \in \mathbb{Z}_p$.

(3) Again, one can first observe that this is true when $n \in \mathbb{N}$, and use that $\mathbb{N}$ is dense in $\mathbb{Z}_p$.

Hint on Problem 2.3: (3) To show the equality, one can proceed as follows: we know that the equality $(1-x)^n(1-x)^m = (1-x)^{n+m}$ holds whenever $n, m \in \mathbb{N}$, and the same holds for the power series version, as the power series really converges. Now in general, for $m, n \in \mathbb{Z}_p$, we can choose sequences of natural numbers $m_1, m_2, \ldots$ and $n_1, n_2, \ldots$ to converge to m and n in $\mathbb{Z}_p$, respectively. Taking limit (using the previous problem) of the equality $(1-x)^{n_i}(1-x)^{m_i} = (1-x)^{n_i+m_i}$ gives what we need.

<u>Hint on Problem 3.1:</u> (3) comes from that for every nonzero vector $v \in V$, there exists $a \in \mathbb{Q}_p^\times$ such that $||av||' \leq 1$.

(4) Take N sufficiently large so that $||e_i||' \leq p^N$ for every i.

(5) Suppose that such N does not exists. Then we have a sequence of integers $c_1, c_2, \cdots \to \infty$ and vectors

$$a_1^{(i)} e_1 + \cdots + a_n^{(i)} e_n$$

with $\max_{1 \leq j \leq n} |a_j^{(i)}|_p = p^{-c_i}$ and $|| \cdot ||'$-norm 1. Modify this by setting $b_j^{(i)} := p^{c_i} a_j^{(i)}$. Then we have a sequence of vectors

$$b_1^{(i)} e_1 + \cdots + b_n^{(i)} e_n \in V$$

with $|| \cdot ||'$-norm going to zero, yet $\max_{1 \leq j \leq n} |b_j^{(i)}|_p = 1$.

As $\mathbb{Z}_p^n$ is compact, the tuples $(b_1^{(i)}, \ldots, b_n^{(i)})_{i \in \mathbb{N}}$ admits a converging subsequence, which limit $(b_1, \ldots, b_n)$. Now, on the one hand, as $|| \cdot ||'$ is bounded by the $|| \cdot ||$, we must have $||b_1 e_1 + \cdots + b_n e_n||' = 0$ through the limit. On the other hand, in the subsequence, $\max_{1 \leq j \leq n} |b_j^{(i)}|_p = 1$ continues to hold, so $\max_{1 \leq j \leq n} |b_j|_p = 1$; in particular not all b_j are zero. This gives a vector $v = b_1 e_1 + \cdots + b_n e_n$ whose $|| \cdot ||'$-norm is zero, yet $v \neq 0$, contradicting condition (c).

Problem 4.1:
We directly apply the definition of Amice transform

$$\begin{aligned} A_{\mu_1\star\mu_2}(T) &= \int_{\mathbb{Z}_p} (1+T)^z \mu_1 \star \mu_2(z) \\ &= \int_{\mathbb{Z}_p} (1+T)^z \mu_1 \star \mu_2(z) \\ &= \int_{\mathbb{Z}_p\times\mathbb{Z}_p} (1+T)^{x+y} \mu_1(x)\mu_2(y) \\ &= \Big(\int_{\mathbb{Z}_p} (1+T)^x \mu_1(x) \Big) \cdot \Big(\int_{\mathbb{Z}_p} (1+T)^y \mu_2(y) \Big) \\ &= A_{\mu_1}(T) \cdot A_{\mu_2}(T). \end{aligned}$$

Problem 4.2: Use exactly the same argument with new functions:

$$f(t) = \frac{\sum_{i=1}^{N-1} \chi(i) e^{(N-i)t}}{e^{Nt}-1}$$

and

$$A_{\mu_\chi}(T) = \frac{\sum_{i=1}^{N-1} \chi(i)(1+T)^{N-i}}{(1+T)^N - 1}.$$