# HOMEWORK ASSIGNMENT 2

MATH-GA 2210.001 ELEMENTARY NUMBER THEORY

*Each problem will be marked out of 5 points.*

**Exercise 1** ([1, II.2.2])**.** Let $n$ be a natural number,

$$n = a_0 + a_1 p + \cdots + a_{r-1} p^{r-1}$$

it's $p$-adic expansion, with $0 \leqslant a_i < p$, and $s_n = a_0 + a_1 + \cdots + a_{r-1}$. Show that

$$v_p(n!) = \frac{n - s_n}{p-1}.$$

`Solution.` Let us prove the required assertion by induction on $n$. When $n = 1$, we have $s_1 = 1$, so that

$$\frac{n - s_1}{p-1} = 0,$$

which is exactly $v_p(1)$ since $p$ does not divide 1.

Suppose that the required assertion holds for $n$, i.e. we have

$$v_p(n!) = \frac{n - s_n}{p-1}.$$

Let us show that it holds for $n+1$, i.e. let us show that we have

$$v_p\big((n+1)!\big) = \frac{n + 1 - s_{n+1}}{p-1}.$$

If $a_0 \neq p - 1$, then

$$n + 1 = (a_0 + 1) + a_1 p + \cdots + a_{r-1} p^{r-1}$$

is $p$-adic expansion of $n+1$, so that $s_{n+1} = s_n + 1$, which gives

$$v_p\big((n+1)!\big) = v_p(n+1) + v_p(n!) = v_p(n+1) + \frac{n - s_n}{p-1} = 0 + \frac{n - s_n}{p-1} = \frac{n + 1 - s_{n+1}}{p-1},$$

which is exactly what we want. If $a_0 = a_1 = \cdots = a_{r-1} = p - 1$, then

$$n + 1 = p^r$$

is $p$-adic expansion of $n+1$, so that $s_{n+1} = 1$ and $s_n = r(p-1)$, which gives

$$v_p\big((n+1)!\big) = v_p(n+1) + v_p(n!) = v_p(n+1) + \frac{n - s_n}{p-1} = r + \frac{n - s_n}{p-1} =$$
$$= \frac{r(p-1) + n - s_n}{p-1} = \frac{r(p-1) + n - r(p-1)}{p-1} = \frac{n}{p-1} = \frac{n + 1 - s_{n+1}}{p-1},$$

which is exactly what we want. Thus, we may assume that $a_0 = p-1$, but not all numbers $a_0, a_1, \ldots, a_{r-1}$ are equal to $p - 1$.

Let $m$ be the number in $\{1, \ldots, r-1\}$ such that

$$a_0 = a_1 = \cdots = a_{m-1} = p - 1$$

and $a_m \neq p - 1$. Then

$$s_n = m(p-1) + a_m + a_{m+1} + \cdots + a_{r-1}.$$

This assignment is due on Wednesday 11 February 2015.

Moreover, we have $v_p(n+1)=m$ and

$$n+1=(a_m+1)p^m+a_{m+1}p^{m+1}+\cdots+a_{r-1}p^{r-1}$$

is the $p$-adic expansion of $n+1$. This gives

$$s_{n+1}=(a_m+1)+a_{m+1}+\cdots+a_{r-1}=m(p-1)+s_n+1.$$

Thus, we have

$$v_p\big((n+1)!\big)=v_p(n+1)+v_p(n!)=v_p(n+1)+\frac{n-s_n}{p-1}=m+\frac{n-s_n}{p-1}=$$
$$=\frac{m(p-1)+n-s_n}{p-1}=\frac{m(p-1)+n-(s_{n+1}-1-m(p-1)}{p-1}=\frac{n}{p-1}=\frac{n+1-s_{n+1}}{p-1},$$

which is exactly what we want.

Let us give another solution. For every $m\in\{1,\ldots,r-1\}$, there are

$$\left\lfloor\frac{n}{p^m}\right\rfloor=a_m+a_{m+1}p+\cdots+a_{r-1}p^{r-1-m}$$

integers between 1 and $n$ that are divisible by $p^m$. Thus, for every $m\in\{1,\ldots,r-1\}$, there are exactly

$$\left\lfloor\frac{n}{p^m}\right\rfloor-\left\lfloor\frac{n}{p^{m-1}}\right\rfloor$$

integers between 1 and $n$ with exponential valuation $v_p=m$. Thus,

$$v_p(n!)=\sum_{m=1}^{r-1}\left(\left\lfloor\frac{n}{p^m}\right\rfloor-\left\lfloor\frac{n}{p^{m-1}}\right\rfloor\right)=\sum_{m=1}^{r-1}\left\lfloor\frac{n}{p^m}\right\rfloor=\sum_{m=1}^{r-1}\sum_{i=m}^{r-1-m}a_ip^{i-m}=$$
$$=a_1+a_2(p+1)+a_3(p^2+p+1)+\cdots+a_{r-1}(p^{r-2}+p^{r-3}+\cdots+1)=\frac{n-s_n}{p-1}.$$

**Exercise 2** ([1, II.2.3])**.** Prove that the sequence

$$1,\frac{1}{10},\frac{1}{10^2},\frac{1}{10^3},\frac{1}{10^4},\frac{1}{10^5},\cdots$$

does not converge in $\mathbb{Q}_p$ for any $p$.

`Solution.` If $p=2$ or $p=5$, then

$$\left|\frac{1}{10^m}\right|_p=2^m,$$

so the sequence

$$1,\frac{1}{10},\frac{1}{10^2},\frac{1}{10^3},\frac{1}{10^4},\frac{1}{10^5},\cdots$$

is not bounded, and, in particular, it does not converge in $\mathbb{Q}_p$. Thus, we may assume that either $p=3$ or $p\geqslant 7$.

For every $m>n$, we have

$$\left|\frac{1}{10^n}-\frac{1}{10^m}\right|_p=\left|\frac{10^{m-n}-1}{10^m}\right|_p=\left|10^{m-n}-1\right|_p\left|\frac{1}{10^m}\right|_p.$$

Thus, if $m=n+1$, we have

$$\left|\frac{1}{10^n}-\frac{1}{10^m}\right|_p=\left|\frac{9}{10^m}\right|_p=|9|_p\left|\frac{1}{10^m}\right|_p=|9|_p\geqslant\frac{1}{9},$$

which implies that the sequence

$$1,\frac{1}{10},\frac{1}{10^2},\frac{1}{10^3},\frac{1}{10^4},\frac{1}{10^5},\cdots$$

is not Cauchy, and, in particular, it does not converge in $\mathbb{Q}_p$.

**Exercise 3** ([1, II.2.5])**.** Show that for every $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$, the sequence

$$\left\{a^{p^n}\right\}_{n\in\mathbb{N}}$$

converges in $\mathbb{Q}_p$.

`Solution.` Let us show that this sequence is Cauchy, so it converges. First, observe that there are

$$\varphi(p^n) = p^n - p^{n-1}$$

integers less than $p^n$ that do not divide it (here $\varphi$ is the Euler function). Since $\gcd(a, p) = 1$, we have

$$a^{\varphi(p^n)} = a^{p^n - p^{n-1}} \equiv 1 \bmod p^n$$

by Euler's Theorem. Then

$$a^{p^n} \equiv a^{p^{n-1}} \bmod p^n.$$

Raising LHS and RHS of this congruence to the power of $p^k$ for every $k \in \mathbb{N}$, we get

$$a^{p^{n+k}} \equiv a^{p^{n+k-1}} \bmod p^n.$$

Thus, we have

$$a^{p^m} \equiv a^{p^{m-1}} \equiv \cdots \equiv a^{p^n} \equiv a^{p^{n-1}} \bmod p^n.$$

for every $m \geqslant n$. Thus, $p^{n+1}$ divides

$$a^{p^m} - a^{p^n}$$

for all $m > n$. Then

$$\left|a^{p^m} - a^{p^n}\right|_p \leqslant \frac{1}{p^{n+1}}$$

for all $m > n$. This implies that the sequence

$$\left\{a^{p^n}\right\}_{n\in\mathbb{N}}$$

is Cauchy, and thus it converges in $\mathbb{Q}_p$.

**Exercise 4** ([1, II.1.6])**.** Prove that $\mathbb{Q}_p$ is not isomorphic to $\mathbb{Q}_q$ if $p \neq q$.

`Solution.` Without loss of generality, we may assume that $q > p$. In particular, $q \neq 2$. Let $m$ be an integer such that the congruence equation

$$x^2 \equiv m \bmod q$$

does not have a solution. Note that such $m$ exists, because $q > 2$. On the other hand, it follows from the Chinese Remainder Theorem that to find an integers $n$ such that

$$n \equiv 1 \bmod p$$

and

$$n \equiv m \bmod q.$$

Then the equation $x^2 = n$ does not have solutions in $\mathbb{Q}_q$. This follows, for example, from [1, Proposition II.1.4]. On the other hand, the equation

$$x^2 = n$$

has a root in $\mathbb{Q}_p$. Indeed, the equation

$$x^2 = n$$

has a solution in $\mathbb{Q}_p$ if and only if the congruence equation

$$x^2 \equiv n \bmod p$$

has a solution. This was implicitly proved in the lectures (cf. [1, Exercise II.1.3]) and it follows, in particular, from Hensel's Lemma (see [1, Lemma II.4.6]). Since

$$n \equiv 1 \bmod p,$$

the congruence equation $x^2 \equiv n \bmod p$ has obvious solutions, so that the equation $x^2 = n$ has a solution in $\mathbb{Q}_p$ as well. Thus, the fields $\mathbb{Q}_p$ and $\mathbb{Q}_q$ cannot be isomorphic.

## References

[1] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.