HOMEWORK ASSIGNMENT 1

MATH-GA 2210.001 ELEMENTARY NUMBER THEORY

Each problem will be marked out of 5 points.

Exercise 1 ([1, II.1.1])**.** A p-adic number

$$a = \sum_{i=-m}^{\infty} a_i p^i \in \mathbb{Q}_p$$

is a rational number if and only if the sequence of digits is periodic.

`Solution.` Suppose that a is a rational number $\frac{m}{n}$. Let us show that its p-adic expansion is periodic. We may assume that m and n are coprime. Similarly, we may assume that p divides neither m nor n. Then

$$a = a_0 + a_1 p + a_2 p^2 + \cdots$$

where $a_0 \neq 0$ and each $a_i \in \{0, \dots, p-1\}$. Solving

$$a_0 n \equiv m \bmod p,$$

we find $a_0 \in \{1, \dots, p-1\}$ that satisfies this congruence equation. Then

$$\frac{\frac{m-na_0}{p}}{n} = a_1 + a_2 p + a_3 p^2 + \cdots$$

in $\mathbb{Q}_p$. Note that $\frac{m-na_0}{p}$ is an integer. Applying the previous step to $\frac{m-na_0}{np}$, we find a_1 and get

$$\frac{\frac{m-na_0-na_1p}{p^2}}{n} = a_2 + a_3 p + a_4 p^2 + \cdots$$

in $\mathbb{Q}_p$. Similarly, $\frac{m-na_0-na_1p}{p^2}$ is an integer. Keep doing this, we get $a_0, a_1, \dots, a_r$ such that

$$\frac{\frac{m-na_0-na_1p-na_2p^2-\cdots-na_rp^r}{p^{r+1}}}{n} = a_{r+1} + a_{r+2} p + a_{r+3} p^2 + \cdots$$

in $\mathbb{Q}_p$ for every $r \geqslant 0$. On the other hand, the absolute value of the integers

$$\frac{m-na_0}{p}, \frac{m-na_0-na_1p}{p^2}, \dots, \frac{m-na_0-na_1p-na_2p^2-\cdots-na_rp^r}{p^{r+1}}$$

are bounded. Indeed, we have

$$\Big|\frac{m-na_0-na_1p-na_2p^2-\cdots-na_rp^r}{p^{r+1}}\Big| \leqslant \frac{|m|+|n|a_0+|n|a_1p+|n|a_2p^2+\cdots+|n|a_rp^r}{p^{r+1}} \leqslant$$

$$\leqslant \frac{|m|+|n|(p-1)(1+p+p^2+\cdots+p^r}{p^{r+1}} = \frac{|m|+|n|(p^{r+1}-1)}{p^{r+1}} =$$

$$= \frac{|m|}{p^{r+1}} + |n| - \frac{|n|}{p^{r+1}} \leqslant \frac{|m|}{p^{r+1}} + |n| \leqslant |m| + |n|.$$

Thus, they belongs to a finite set. So, for $r \gg 0$, two of them, say

$$\frac{m-na_0-na_1p-na_2p^2-\cdots-na_{r_1}p^{r_1}}{p^{r_1+1}}$$

This assignment is due on Wednesday 04 February 2015.

and

$$\frac{m - na_0 - na_1p - na_2p^2 - \cdots - na_{r_2}p^{r_2}}{p^{r_2+1}}$$

coincides (here $r_1 \neq r_2$). Thus, we have

$$a_{r_1+1} + a_{r_1+2}p + a_{r_1+3}p^2 + \cdots = \frac{m - na_0 - na_1p - na_2p^2 - \cdots - na_{r_1}p^{r_1}}{p^{r_1+1}} =$$
$$= \frac{m - na_0 - na_1p - na_2p^2 - \cdots - na_{r_2}p^{r_2}}{p^{r_2+1}} = a_{r_2+1} + a_{r_2+2}p + a_{r_2+3}p^2 + \cdots$$

in $\mathbb{Q}_p$. This means that

$$a_{r_1+i} = a_{r_2+i}$$

for every $i \geqslant 1$. This is exactly means that the p-adic expansion

$$a_0 + a_1p + a_2p^2 + \cdots$$

is periodic.

Now let us show that p-adic numbers with periodic p-adic expansions are rational. Suppose that the p-adic expansion of a is periodic. Let us show that $a \in \mathbb{Q}$. Since adding/subtracting a rational and multiplying/dividing by a non-zero rational does not change the rationality and irrationality of the numbers in $\mathbb{Q}_p$, we may assume that

$$a = a_0+a_1p+a_2p^2+\cdots+a_Np^N+a_0p^{N+1}+a_1p^{N+2}+a_2p^{N+2}+\cdots+a_{2N}p^{2N}+a_0p^{2N+1}+\cdots .$$

Then

$$a = \Big(a_0 + a_1p + a_2p^2 + \cdots + a_Np^N\Big)\Big(1 + p^N + p^{2N} + p^{3N} + \cdots\Big)$$

in $\mathbb{Q}_p$. On the other hand, we have

$$\frac{1}{1-p^N} = 1 + p^N + p^{2N} + p^{3N} + \cdots$$

in $\mathbb{Q}_p$. Indeed, the proof of this equality is the same as of

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + \cdots$$

that is given in [1, II.1]. Thus, we have

$$a = \Big(a_0+a_1p+a_2p^2+\cdots+a_Np^N\Big)\Big(1+p^N+p^{2N}+p^{3N}+\cdots\Big) = \frac{a_0 + a_1p + a_2p^2 + \cdots + a_Np^N}{1-p^N},$$

so that a is rational.

Exercise 2 ([1, II.1.2]). A p-adic integer

$$a = a_0 + a_1p + a_2p^2 + \cdots$$

is a unit in the ring $\mathbb{Z}_p$ if and only if $a_0 \neq 0$.

`Solution.` For a, being a unit in $\mathbb{Z}_p$ means that there is

$$b = b_0 + b_1p + b_2p^2 + \cdots$$

with each $b_i \in \{0, \ldots, p-1\}$ such that $ab = 1$ in $\mathbb{Z}_p$. Keeping in mind the construction of $\mathbb{Q}_p$ in [1, II.1], we see that $ab = 1$ if and only if

$$\Big(a_0 + a_1p + a_2p^2 + \cdots + a_{n-1}p^{n-1}\Big)\Big(b_0 + b_1p + b_2p^2 + \cdots + b_{n-1}p^{n-1}\Big) \equiv 1 \bmod p^n$$

for every $n \geqslant 1$. On the other hand, if $a_0 = 0$, then we never find b_0 such that

$$a_0b_0 \equiv 1 \bmod p,$$

which implies that a is not a unit unless $a_0 \neq 0$.

Vice versa, suppose that $a_0 \neq 0$. Let us show that a is a unit. Solving the congruence equation

$$a_0 b_0 \equiv 1 \bmod p,$$

we find a unique $b_0 \in \{1, \ldots, p-1\}$. Similarly, we get $a_1 \in \{0, \ldots, p-1\}$ by solving

$$a_0 b_1 + a_1 b_0 \equiv \frac{1 - a_0 b_0}{p} \bmod p,$$

where $\frac{1-a_0 b_0}{p}$ is an integer by construction. In general, we may prove the existence of the required integers $b_0, b_1, \ldots, b_n$ for ever given n by induction. Indeed, the base of induction is already done (we found a_0). Thus, if we have $b_0, b_1, \ldots, b_{n-1}$ such that

$$\Big(a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}\Big)\Big(b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1}\Big) \equiv 1 \bmod p^n,$$

then

$$\frac{\Big(a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}\Big)\Big(b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1}\Big) - 1}{p^n}$$

is an integer, which implies that the congruence equation

$$\Big(a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n\Big)\Big(b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n\Big) \equiv 1 \bmod p^{n+1}$$

is equivalent to

$$\frac{\Big(a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}\Big)\Big(b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1}\Big) - 1}{p^n} + (a_0 b_n + b_0 a_n) \equiv 0 \bmod p,$$

which has a unique solution $b_n \{0, \ldots, p-1\}$. This proves the existence of $b \in \mathbb{Q}_p$ such that $ab = 1$.

Exercise 3 ([1, II.1.3])**.** Show that the equation

$$x^2 = 2$$

has a solution in $\mathbb{Z}_7$.

`Solution.` Keeping in mind the construction of $\mathbb{Q}_p$ in [1, II.1], we must find an infinite sequence of integers

$$a_0, a_1, a_2, a_3 \ldots,$$

in $\{0, 1, 2, 3, 4, 5, 6\}$ such that

$$\Big(a_0 + a_1 7 + a_2 7^2 + \cdots + a_{n-1} 7^{n-1}\Big)^2 \equiv 2 \bmod 7^n$$

for every $n \geqslant 1$. For $n = 1$ this congruence equation gives

$$a_0^2 \equiv 2 \bmod 7,$$

which gives that either $a_0 = 3$ or $a_0 = 4$.

Let us fix $a_0 = 3$ (the case when $a_0 = 4$ is similar). Then the above equation for $n = 2$ gives

$$a_0^2 + 2a_1 7 \equiv 2 \bmod 7^2,$$

which is equivalent to

$$\frac{a_0^2 - 2}{7} + a_1 \equiv 0 \bmod 7,$$

which has a unique solution $a_1 \in \{0, 1, 2, 3, 4, 5, 6\}$. Note that

$$\frac{a_0^2 - 2}{7}$$

is an integer by construction. Once we found, $a_0, a_1, \dots, a_n$, we use

$$\Big(a_0 + a_1 7 + a_2 7^2 + \cdots + a_n 7^n\Big)^2 \equiv 2 \bmod 7^{n+1}$$

to get

$$\frac{\Big(a_0 + a_1 7 + a_2 7^2 + \cdots + a_{n-1} 7^{n-1}\Big)^2 - 2}{7} + 2a_n \equiv 0 \bmod 7,$$

which gives us unique $a_n \in \{0, 1, 2, 3, 4, 5, 6\}$. Here

$$\frac{\Big(a_0 + a_1 7 + a_2 7^2 + \cdots + a_{n-1} 7^{n-1}\Big)^2 - 2}{7}$$

is an integer. This proves the existence of the solution $x^2 = 2$ in $\mathbb{Q}_p$. In fact, it proves that there are exactly two such solutions.

Exercise 4 ([1, II.1.4])**.** Write the numbers $\frac{2}{3}$ and $-\frac{2}{3}$ as 5-adic numbers.

`Solution.` Let us find the 5-adic expansion of $\frac{2}{3}$ first. We must find an infinite sequence of integers

$$a_0, a_1, a_2, a_3 \dots,$$

in $\{0, 1, 2, 3, 4\}$ such that

$$2 \equiv 3\Big(a_0 + a_1 5 + a_2 5^2 + \cdots + a_{n-1} 5^{n-1}\Big) \bmod 5^n$$

for every $n \geqslant 1$. For $n = 1$, we get

$$3a_0 \equiv 2 \bmod 5,$$

which gives $a_0 = 4$. For $n = 2$ this gives

$$3a_0 + 3a_1 5 \equiv 2 \bmod 5^2,$$

which is equivalent to

$$3a_1 \equiv \frac{2 - 3a_0}{5} \bmod 5,$$

which gives us $a_1 = 1$, because $\frac{2-3a_0}{5} = -2$. Similarly, for $n = 3$, we have

$$3a_2 \equiv \frac{2 - 3a_0 - 15a_1}{5^2} \bmod 5,$$

which gives us $a_1 = 3$, because $\frac{2-3a_0-15a_1}{5^2} = -1$. For $n = 4$, we have

$$3a_3 \equiv \frac{2 - 3a_0 - 15a_1 - 75a_2}{5^3} \bmod 5,$$

which gives us $a_3 = 1$, because $\frac{2-3a_0-15a_1-75a_2}{5^3} = -2$. Note that the computation of a_3 is identical to that of a_1. Arguing as in the solution of Problem 1, we see that

$$a_1 + a_2 5 + a_3 5^3 + \cdots = a_3 + a_4 5 + a_4 5^3 + \cdots$$

in $\mathbb{Q}_p$. This means that

$$\frac{2}{3} = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots = 4\overline{13}.$$

Similarly, we can the 5-adic expansion of

$$-\frac{2}{3} = 1 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \cdots = \overline{31}.$$

References

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