Mathematics 4: Number Theory Problem Sheet 5

Workshop 23 Nov 2012

Working with p-adic numbers

Recall that the *standard form* of a nonzero p-adic number a is $a = p^k(a_0 + a_1p + \cdots + a_np^n + \dots)$, where $k \in \mathbb{Z}$ and all the a_i are in $\{0, 1, 2, \dots, p-1\}$, with $a_0 \neq 0$.

(1) (a) Write 5 as a p-adic number in standard form.
(You will need to do the cases $p = 2$, $p = 3$, $p = 5$ and $p > 5$ separately.)
(b) Write -5 as a p-adic number in standard form.

(2) Calculate 1/3 as a 5-adic number, and 1/5 as a 3-adic number.

(3) In $\mathbb{Q}_p$, which rational number is represented by the sum

$$2 + 3p + 5p^2 + 2p^3 + 3p^4 + 5p^5 + 2p^6 + 3p^7 + 5p^8 + \dots?$$

[Note: While this will be a standard representation of a p-adic number only for $p > 5$, it nevertheless gives a nonstandard representation of a p-adic number for $p = 2, 3$ and 5.]

(4) For $\sqrt{7} = a_0 + a_1 3 + a_2 3^2 + a_3 3^3 + a_4 3^4 + \dots$ in $\mathbb{Q}_3$, find $a_0, a_1, a_2, a_3, a_4 \in \{0, 1, 2\}$.

(5) *The field* $\mathbb{Q}_p(\sqrt{p})$
(a) Let p be prime. Show that there is no $x \in \mathbb{Q}_p$ with $x^2 = p$, and so $\mathbb{Q}_p(\sqrt{p})$ is a quadratic extension of $\mathbb{Q}_p$.
(b) Show how to extend $|\cdot|_p$ to $\mathbb{Q}_p(\sqrt{p})$ (i.e., to define $|\cdot|_p$ on $\mathbb{Q}_p(\sqrt{p})$ so that it still equals the original $|\cdot|_p$ on $\mathbb{Q}_p \subset \mathbb{Q}_p(\sqrt{p})$.)
(c) Show that every nonzero element of $\mathbb{Q}_p(\sqrt{p})$ can be written in standard form

$$p^k \left(a_0 + a_1p^1 + a_2p^2 + \cdots + a_ip^i + \cdots + \sqrt{p}(b_0 + b_1p^1 + b_2p^2 + \cdots + b_ip^i + \dots)\right),$$

where $k \in \mathbb{Z}$ and all the a_i are in $\{0, 1, 2, \dots, p-1\}$, with a_0 and b_0 not both 0.

Handin: due Friday, week 11, 30 Nov, before 12.10 lecture. Please hand it in at the lecture

The field $\mathbb{Q}_p(\sqrt{n})$

You are expected to write clearly and legibly, giving thought to the presentation of your answer as a document written in mathematical English.

(6) (a) Let p be an odd prime, and $n > 0$ be a fixed quadratic nonresidue mod p. Show that there is no $x \in \mathbb{Q}_p$ with $x^2 = n$, and so $\mathbb{Q}_p(\sqrt{n})$ is a quadratic extension of $\mathbb{Q}_p$.

(b) Show how to extend $|\cdot|_p$ to $\mathbb{Q}_p(\sqrt{n})$ (i.e., to define $|\cdot|_p$ on $\mathbb{Q}_p(\sqrt{n})$ so that it still equals the original $|\cdot|_p$ on $\mathbb{Q}_p \subset \mathbb{Q}_p(\sqrt{n})$.) To do this, apply the valuation axioms ZER, HOM and MAX to show successively that

- $|\sqrt{n}|_p = 1$;
- $|a + b\sqrt{n}|_p \leq 1$ for $a, b \in \mathbb{Z}_p$;
- For $a, b \in \mathbb{Z}_p$, we have $|a^2 - nb^2|_p = 1$ unless $|a|_p < 1$ and $|b|_p < 1$;
- For $a, b \in \mathbb{Z}_p$, we have $|a \pm b\sqrt{n}|_p = 1$ unless $|a|_p < 1$ and $|b|_p < 1$;
- For $a, b \in \mathbb{Z}_p$ not both divisible by p we have $|p^k(a + b\sqrt{n})|_p = p^{-k}$;

(c) Show that every nonzero number in $\mathbb{Q}_p(\sqrt{n})$ can be written in the form

$$p^k(A_0 + A_1 p + A_2 p^2 + \cdots + A_i p^i + \dots),$$

where $k \in \mathbb{Z}$, and all $A_i = a_i + b_i\sqrt{n}$, where $0 \leq a_i \leq p-1, 0 \leq b_i \leq p-1$, with $A_0 \neq 0$.

(d) Let n' be any other quadratic nonresidue of p. Show that $\sqrt{n'} \in \mathbb{Q}_p(\sqrt{n})$.

(e) Show that $\mathbb{Q}_p(\sqrt{n}) = \mathbb{Q}_p(\sqrt{n'})$.

Further p-adic problems

(7) *The field $\mathbb{Q}_p(\sqrt{np})$.*

(a) Let p be an odd prime, and $n > 0$ be a fixed quadratic nonresidue mod p. Show that there is no $x \in \mathbb{Q}_p$ with $x^2 = np$, and so $\mathbb{Q}_p(\sqrt{np})$ is a quadratic extension of $\mathbb{Q}_p$.

(b) Show how to extend $|\cdot|_p$ to $\mathbb{Q}_p(\sqrt{np})$.

(c) Show that every nonzero element of $\mathbb{Q}_p(\sqrt{np})$ can be written in standard form

$$p^k \left(a_0 + a_1 p + a_2 p^2 + \cdots + \sqrt{np}(b_0 + b_1 p + b_2 p^2 + \dots)\right),$$

where $k \in \mathbb{Z}$ and all the a_i and b_i are in $\{0, 1, 2, \dots, p-1\}$, with a_0 and b_0 not both 0.

(8) *$\mathbb{Q}_p$ has only three quadratic extensions.*

Let p be an odd prime. Recall from lectures that a p-adic integer $\beta = a_0 + a_1 p + a_2 p^2 + \dots$ not divisible by p^2 (ie with β/p^2 not a p-adic integer) is a square iff a_0 is nonzero and a quadratic residue $\pmod{p}$.

(a) Let $n \in \{1, 2, \ldots, p-1\}$ be a fixed quadratic nonresidue $\pmod p$. Show that $x^2 = \beta$ has a solution in one of the fields $\mathbb{Q}_p, \mathbb{Q}_p(\sqrt{n}), \mathbb{Q}_p(\sqrt{p})$ or $\mathbb{Q}_p(\sqrt{np})$.

(b) Deduce that there are at most 3 quadratic extensions of $\mathbb{Q}_p$.

(c) Prove that the fields in (a) are distinct, so that $\mathbb{Q}_p$ has *exactly* 3 quadratic extensions.

(9) *$\mathbb{Q}_2$ has 7 quadratic extensions.*

[Recall from lectures that a 2-adic integer not divisible by 4 is a square iff it is congruent to 1 (mod 8).]

(a) Show that every unit in the 2-adic integers $\mathbb{Z}_2$ is congruent $\pmod 8$ to some $u \in \{1, -1, 3 - 3\}$.

(b) Show that every number in $\mathbb{Q}_2$ can be written in the form $2^\nu u s^2$ for some u as in (a), $\nu \in \mathbb{Z}$ and some unit $s \in \mathbb{Z}_2$.

(c) Deduce that there are exactly 7 quadratic extensions of $\mathbb{Q}_2$, namely $\mathbb{Q}_2(\sqrt{k})$ for $k = 2, -1, -2, 3, 6, -3$ or -6.

(10) Given $c \in \mathbb{Q}_p$, $c \neq 0$, show that every $c' \in \mathbb{Q}_p$ sufficiently close to c (in fact, with $|c - c'|_p < |c|_p$) has $|c'|_p = |c|_p$.

(11) Show that in $\mathbb{Q}_p$ every ball $B(a, r) := \{x \in \mathbb{Q}_p : |x - a|_p \leq r\}$ is both open (contains a ball of positive radius around each point) and closed (contains all its limit points).

(12) *Series in $\mathbb{Q}_p$ whose terms tend to zero always converge!*

Suppose that $c_1, c_2, \ldots, c_n, \cdots \in \mathbb{Q}_p$ with $|c_n|_p \to 0$ as $n \to \infty$. Show that the partial sums $s_n = c_1 + \cdots + c_n$ form a p-Cauchy sequence. Deduce that $\sum_n c_n$ converges in $\mathbb{Q}_p$.

Conversely, show that the condition $|c_n|_p \to 0$ $(n \to \infty)$ is necessary for convergence of the series. [The proof of this last part is the same as for the real case.]

(13) *$\mathbb{Q}_p$ contains all the $(p-1)$-th roots of unity.*

Let p be an odd prime.

(a) Let $g \in \{1, 2, \ldots, p-1\}$ be a primitive root $\pmod p$. Show that there is a p-adic number $\omega = g + a_1 p + a_2 p^2 + \cdots$ such that $\omega^{p-1} = 1$.

(b) (easy!) Deduce the fact that $\mathbb{Q}_p$ contains $p - 1$ $(p-1)$-th roots of unity.

(c) Show that every number in $\mathbb{Q}_p$ has an alternative representation $\sum_{i=-k}^{\infty} a_i p^i$ for some $k \in \mathbb{Z}$, where $a_i \in \{0, 1, \omega, \omega^2, \ldots, \omega^{p-2}\}$.

(14) *The 6-adic numbers.*

Define the ring $\mathbb{Q}_6$ of 6-adic numbers as for the p-adic numbers but with 6 replacing p. Show that $\mathbb{Q}_6$ not a field by finding a 6-adic number $\alpha \neq 0, -1$ satisfying $\alpha(\alpha+1) = 0$.

[Suggestion: put $\alpha = 2+a_1.6+a_2.6^2+\cdots$, and show that you can solve $\alpha(\alpha+1) = 0 \pmod{6^k}$ for $k = 2, 3, \ldots$. (This shows too that the 6-adic integers don't form an integral domain.)]