Topics in Number Theory - 6th exercise sheet

Alex Bartel

November 21, 2012

Please submit solutions to the questions 1,2,4,5 for credit. The submission deadlines for the exercise sheet are Nov 12, Nov 19, and Nov 26, always at 3 pm. Each answer will attract full marks if it is perfect, and 0 otherwise.

1. This is going to be easy if you have done question 4 on the previous exercise sheet:

   (a) Show that the following continued fraction converges in $\mathbb{Q}_5$ and determine its value:
   $$-2-\cfrac{5}{4-\cfrac{5}{4-\cfrac{5}{4-\dots}}}$$

   (b) Recall that Hensel's lemma implies that $\sqrt{2} \in \mathbb{Q}_7$. Find a continued fraction expression for a square root of 2 in $\mathbb{Q}_7$, similar to the above.

2. This is an alternative description of the Teichmüller lift, which does not use Hensel's lemma.

   (a) Let $a \in \mathbb{Z}_p$ be any element. Show (e.g. by induction) that the sequence $(a^{p^n})_n$ converges in $\mathbb{Z}_p$.

   (b) For each $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, choose any element $x_a \in \mathbb{Z}_p^\times$ that satisfies $x_a \equiv a \pmod{p}$. Show that the map
   $$[\cdot] : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times, \quad [a] = \lim_{n\to\infty} (x_a)^{p^n}$$
   is an injective group homomorphism that does not depend on the choice of x_a.

   (c) Deduce that $\mathbb{Q}_p$ contains the $(p-1)^{st}$ roots of unity.

3. Show that a p-adic number
   $$a = \sum_{n=k}^{\infty} a_n p^n, \quad a_n \in \{0, \dots, p-1\}$$
   is contained in $\mathbb{Q} \subset \mathbb{Q}_p$ if and only if the sequence $(a_n)_{n\geq k}$ is periodic, i.e. if and only if there exists $m \geq k$ and $l \in \mathbb{N}$ such that $a_n = a_{n+l}$ for all $n \geq m$. (Hint: Given $a \in \mathbb{Q}$ non-zero, write $a = p^o \frac{t}{s}$ with $p \nmid ts$ and show that there is some $r > 0$ such that $1 - p^r \equiv 0 \pmod{s}$.)

4. Using a geometry of numbers argument, show that an odd prime number p can be written as $p = x^2 + 2y^2$, $x, y \in \mathbb{Z}$, if and only if $\left(\frac{-2}{p}\right) = 1$. Since this is not a calculus course, you may use any formula for a volume of anything sensible without proving it.

5. (a) Let $p \equiv 1 \pmod 3$ be a prime. Show that there exists $f \in \mathbb{Z}$ such that $f^2 + f + 1 \equiv 0 \pmod p$.

   (b) Using a geometry of numbers argument, show that there are $x, y \in \mathbb{Z}$ such that $p = x^2 + xy + y^2$. The same remark as in the previous question applies.