KMB, 24/10/08

L-functions, Problem Sheet 1

Some of these exercises were already alluded to in the course. The sheet has 14 questions.

Analytic bits and bobs.

1) Check that the two versions of the functional equation for the Riemann zeta function are indeed equivalent, assuming Euler's reflection formula and Legendre's duplication formula.

2) Locate where $\Gamma(z)$ has poles, check they're all simple, and compute the residue at each pole.

3) Check from the definition that $\Gamma(1/2) = \sqrt{\pi}$.

Normed fields.

4) Fill in the details of the sketch-proof in the lectures that if we can take $C = 2$ in part (iii) of the definition of a norm, then the norm does indeed satisfy the triangle inequality.

5) (a) Check directly that the p-adic norm on $\mathbf{Q}$ satisfies $|x+y| = \max\{|x|, |y|\}$ if $|x| \neq |y|$.

(b) Check from the axioms that if $|.|$ is a non-arch norm on an arbitrary field then $|x + y| = \max\{|x|, |y|\}$ if $|x| \neq |y|$.

6) Check that the P-adic norm on a number field is a norm. Hint: you might need to use standard facts about factorisation of fractional ideals into primes.

Good exercises for getting a concrete understanding of $\mathbf{Q}_p$.

7) Let $|.|_p$ denote the p-adic norm on $\mathbf{Q}$. For each of the sets of p, m, r below, either find an $x \in \mathbf{Z}$ such that $|r - x|_p \leq p^{-m}$, or show that no such x exists.

(i) $p = 257$, $r = 1/2$, $m = 1$
(ii) $p = 3$, $r = 7/8$, $m = 2$
(iii) $p = 3$, $r = 7/8$, $m = 7$
(iv) $p = 3$, $r = 5/6$, $m = 9$
(v) $p = 5$, $r = 1/4$, $m = 4$
(vi) and invent some more until you feel you've got the hang of it.

8) For each of the sets of p, m, r below, either find an $x \in \mathbf{Z}$ such that $|r - x^2|_p \leq p^{-m}$, or show that no such x exists.

(i) $p = 3$, $r = -2$, $m = 4$
(ii) $p = 5$, $r = 10$, $m = 3$
(iii) $p = 13$, $r = -4$, $m = 3$
(iv) $p = 2$, $r = -7$, $m = 6$
(v) $p = 7$, $r = -14$, $m = 4$
vi) $p = 5$, $r = -25$, $m = 4$
(vii) $p = 5$, $r = 2/3$, $m = 3$
(viii) and so on.

9) In the lectures we shows that there exists $x \in \mathbf{Q}_3$ such that $x^2 = 7$. Prove, using the same technique, that there is $x \in \mathbf{Z}_7$ with $x^3 = 6$ (here $\mathbf{Z}_p$ denotes the integers of $\mathbf{Q}_p$).

10)

(a) Convince yourself that the same technique as in Q9 and the lectures shows that if $p > 2$ is prime and $n \in \mathbf{Z}$ is coprime to p and a square mod p, then $\sqrt{n} \in \mathbf{Z}_p$.

(b) Check that in fact this fails for $p = 2$ by showing that there is no $\ell \in \mathbf{Q}_2$ such that $\ell^2 = 3$. Can you see why the method fails??

(c) When you've done Q14, explain why Hensel's Lemma makes part (a) of this problem a triviality, but does not apply to part (b).

11) We showed/will show in lectures that any p-adic integer ℓ can be written as $\sum_{n\geq 0} a_n p^n$ with $a_n \in \{0, 1, 2, \ldots, p-1\}$. Now set $p = 3$. For each of the following 3-adic integers, compute a_n for all $n \geq 0$: $\ell = 10, -10, -1/2, 1/4, 1/5$.

12) Recall that a real number is rational if and only if its decimal expansion is ultimately periodic. Prove the same thing for the p-adic numbers, that is, prove that if $\ell \in \mathbf{Q}_p$ and we write $\ell = \sum_{n\geq M} a_n p^n$ then the a_n are ultimately periodic iff $\ell \in \mathbf{Q}$. Hint: if you can prove this for the reals then the same proof works for $\mathbf{Q}_p$.

13) If you're computer-savvy then compute lots of terms a_n in the 3-adic number $\ell = \sum_{n\geq 0} a_n 3^n$ such that $a_1 = 1$ and $\ell^2 = 7$. Can you see a pattern to the a_n? Do you expect to see a pattern?

14) Here's the correct generalisation of questions 9 and 10a. This is a fundamental and important result! Surprisingly, I don't think I'll actually need it in the course (famous last words...) so I'll relegate the proof to an exercise. Any book on local fields will contain a crib.

Theorem. (Hensel's Lemma). Let k be a complete non-arch normed field, let R denote its integers, say $f \in R[X]$ is a polynomial and assume that there exists $a_0 \in R$ with $|f(a_0)| < |f'(a_0)|^2$. Then there exists $a \in R$ with $f(a) = 0$. If we furthermore demand that $|a - a_0| < |f(a_0)|/|f'(a_0)|$ then a is unique.

The existence of a follows from the standard Newton-Raphson argument from numerical analysis, and the non-archimedean-ness of the norm guarantees that the algorithm converges. Fill in the details of the following sketch-proof!

(i) Check that one can write $f(X+Y) = f(X) + Y f_1(X) + Y^2 f_2(X) + \ldots$ (a finite sum) with $f_n(X) \in R[X]$ (hint: $n! f_n(X)$ is the nth derivative of f; check that no denominators are introduced) and $f_1(X) = f'(X)$.

(ii) As is usual in Newton-Raphson, choose b_0 with $f(a_0) + b_0 f'(a_0) = 0$ and set $a_1 = a_0 + b_0$. Check that $|f(a_1)| < |f(a_0)|$ and that $|f'(a_1)| = |f'(a_0)|$.

(iii) Repeat the process! Given a_n, choose b_n with $f(a_n) + b_n f'(a_n) = 0$ (checking on the way that $f'(a_n) \neq 0$) and set $a_{n+1} = a_n + b_n$. Check that (a_n) is Cauchy (hint: check that $|b_n| \to 0$) and that $f(a_n) \to 0$.

(iv) Check that f is continuous and hence that $f(a) = 0$ if a is the limit of the a_n.

(v) Check that the a constructed above satisfies $|a - a_0| < |f(a_0)|/|f'(a_0)|$.

(vi) Finally, check that if a' satisfies $f(a') = 0$ and $|a' - a_0| < |f(a_0)|/|f'(a_0)|$ then $a' = a + b$ and $f(a) = f(a+b) = 0$; expand out using the expansion of $f(X+Y)$ above and check that we get a contradiction unless $b = 0$.