Math 702 Problem Set #5 Due Fri., March 26, 2004

1. (a) Determine whether or not there is a solution to the equation $x^2 - 43 = 0$ in $\mathbb{Z}_{97}$.

(b) Describe the behavior of the prime 97 in the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{43})$.

(c) Find an arithmetic progression $97 + jn$ ($j = 0, 1, 2, ...$) such that every prime in the progression has the same behavior in this extension as 97.

2. Let p be a prime number, and let $\beta \in \mathbb{Z}_p$.

(a) Show that if p is odd and $\beta \equiv 1 \pmod{p}$ then β is a square in $\mathbb{Z}_p$.

(b) Show that the conclusion of part (a) does not in general hold if instead $p = 2$, even if we assume that $\beta \equiv 1 \pmod{4}$.

(c) Show that if $p = 2$ and $\beta \equiv 1 \pmod{8}$, then β is a square in $\mathbb{Z}_2$. (Hint: P.S. 2 #6(b).)

3. Let K be a global field containing a primitive mth root of unity, for some $m > 1$. Let v be a non-archimedean prime of K that does not divide m, let π be a uniformizer for v, and consider the Hilbert norm residue symbol $(a, b)_v \in \mu_n$. Recall that

(i) $(aa', b)_v = (a, b)_v (a', b)_v$ and $(a, bb')_v = (a, b)_v (a, b')_v$;

(ii) $(a, b)_v = (\frac{a}{v})^{v(b)}$ if $v(a) = 0$, where $(\frac{a}{v})$ is the mth power residue symbol; and

(iii) $(a, b)_v = 1$ iff b is a norm from $K_v(\sqrt[m]{a}\,)$ to K_v.

Using the above, show the following:

(a) $(a, -a)_v = 1$ for all a. [Hint: What is the norm of $(-\sqrt[m]{a}\,)$?]

(b) $(a, b)_v (b, a)_v = 1$. [Hint: Apply (i) to $(ab, -ab)_v$ and use part (a).]

(c) $(\pi, \pi)_v = (\frac{-1}{v})$. [Hint: Apply (a) and (i) to $(\pi, -\pi)_v$. Then use (b) and (ii).]

(d) $(a, b)_v = (\frac{c}{v})$, where $c = (-1)^{v(a)v(b)} a^{v(b)} b^{-v(a)}$. [Hint: Write $a = \pi^{v(a)} a_0$ and $b = \pi^{v(b)} b_0$ and apply (i) and (ii).]

4. Let p be an odd prime number, let $R = \mathbb{F}_p[t]$, and let $K = \mathrm{frac}(R) = \mathbb{F}_p(t)$. Also, let K_∞ be the completion of K at the infinite prime, i.e. $K_\infty = \mathbb{F}_p((t^{-1}))$. Let $(K_\infty^*)^2$ denote the set of squares of elements of K_∞^*, and let $P = \{a \in R \,|\, a \in (K_\infty^*)^2\}$. Consider the quadratic residue symbol $(\frac{a}{I})$ for fractional ideals I of R, and for $b \in K^*$ consider the associated symbol $(\frac{a}{b}) := \prod_v (\frac{a}{v})^{v(b)}$, where v ranges over the places of K such that $v(a) = 0$.

(a) Show that for relatively prime $a, b \in R$ with $b \in P$, we have that $(\frac{a}{b}) = (\frac{a}{(b)})$. In the case that b is also a prime element (i.e. an irreducible polynomial), show that $(\frac{a}{b}) = 1$ if and only if a is a square modulo b. What can go wrong if instead $b \notin P$?

(b) Show that if $a, b \in P$ are relatively prime, then $(\frac{a}{b})(\frac{b}{a}) = 1$. [Hint: Following the situation for $\mathbb{Q}$, let $\langle a, b \rangle = (\frac{a}{b})(\frac{b}{a})$. Writing $b = a + c$, use the properties of the quadratic residue symbol to deduce that $(\frac{b}{a}) = (\frac{-a}{b})$ and hence $\langle a, b \rangle = (\frac{-1}{b})$. Redoing this with a replaced by 1, show that $\langle a, b \rangle = 1$.]

(c) Show that for $a \in P$, there is an element $c \in P$ such that for all $b \in P$ relatively prime to a, the condition that a is a square modulo b depends only on $b \bmod c$. What is c?

(d) Show by example that the conclusion of part (c) is not necessarily true if b is not required to be in P (but only in R, and relatively prime to a).

(e) In the case that $p = 3$, use parts (a) and (b) to evaluate $(\frac{t^2+1}{t^6+t^4+t})$ and $(\frac{t^2+1}{t^4+t^2-t+1})$.

(f) Explain the parallel between this situation and the situation over the ring $\mathbb{Z}$.