MATH 620: HOMEWORK #5

1. Strong approximation for SL_2.

In class we discussed how the Strong Approximation Theorem for $\mathrm{SL}_2(\mathbb{Z})$ implies that the natural homomorphism $r_N : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N)$ is surjective for all integers N. This exercise gives a direct proof of this statement.

1. Show that r_N is surjective if and only if whenever $A \in \mathrm{Mat}_2(\mathbb{Z})$ is a matrix such that $\det(A) \equiv 1 \bmod N$ there is a matrix $B \in \mathrm{SL}_2(\mathbb{Z})$ such that $A \equiv B \bmod N\mathbb{Z}$.
2. Let A be a matrix as in part (1). An elementary row (resp. column) operation on A consists of adding an integral multiple of a row (resp. column) to a different row (resp. column). Show that such an operation corresponds to multiplying A on the left (resp. right) by a matrix in $\mathrm{SL}_2(\mathbb{Z})$. Use this and the Euclidean algorithm to show that there are matrices $U, V \in \mathrm{SL}_2(\mathbb{Z})$ such that
$$UAV = \begin{pmatrix} n_1 & 0 \\ 0 & n_2 \end{pmatrix}$$
for some integers $n_1, n_2 \in \mathbb{Z}$.
3. Show that
$$\begin{pmatrix} n_2 & 1 \\ n_2 - 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} n_1 & 0 \\ 0 & n_2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -n_2 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 1 - n_1 & 1 \end{pmatrix} \mod N\mathrm{Mat}_2(\mathbb{Z}).$$
Use this and parts (1) and (2) to show that $r_N : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N)$ is surjective.
4. Explain why the above proof applies whenever $\mathbb{Z}$ is replaced by an arbitrary Euclidean domain R with respect to some norm function $\mathcal{N} : R \to \mathbb{Z}$ and $N\mathbb{Z}$ is replaced by an arbitrary non-zero ideal $\mathcal{I}$ of R.

Comment The Strong Approximation Theorem holds for SL_2 over an arbitrary number field K, which implies
$$\mathrm{SL}_2(O_K) \to \mathrm{SL}_2(O_K/J)$$
is surjective for all non-zero ideals J of the integers O_K. The method of proof of the latter fact given in this problem breaks down, though, if O_K is not Euclidean. For some interesting connections between this topic and hyperbolic geometry, see the paper "Generators and relations for certain special linear groups" by R. Swan, Advances in Math. 6, 1–77 (1971).

2. Hensel's Lemma

This problem is about a generalization of Hensel's Lemma to polynomials in two variables. Let K be a p-adic field with integers O_K and absolute value $|\ | : K \to \mathbb{R}$ normalized so that $|\pi_K| = q^{-1}$ when π_K is a uniformizer in O_K and $q = \#O_K/(\pi_K O_K)$. Suppose $f_1(x,y), f_2(x,y) \in O_K[x,y]$ are polynomials in two variables over O_K. We then have a polynomial map $K \times K \to K \times K$ defined by
$$(x,y) \to F(x,y) = (f_1(x,y), f_2(x,y)).$$
Suppose $(x_0, y_0) \in O_K \times O_K$ has the property that
$$F(x_0, y_0) \in (\pi_K O_K) \times (\pi_K O_K).$$

5. State and prove a generalization of the naive version of Hensel's Lemma which will provide a sufficient condition for there to exist $(x_1, y_1) \in O_K \times O_K$ such that
$$F(x_1, y_1) = (0,0) \quad \text{and} \quad (x_1, y_1) \equiv (x_0, y_0) \mod (\pi_K O_K) \times (\pi_K O_K).$$

6. Apply your criterion in (5) to the case in which $(x_0, y_0) = (0, 0)$, $f_1(x, y) = x^3 + xy + \pi_K$ and $f_2(x, y) = x^2 - y^2 - h - \pi_K$.
7. State and prove a generalization of the sophisticated form of Hensel's Lemma based on Newton's iteration.

3. The Minkowski bound and computations of units

7. Show that the cubic field $K = \mathbb{Q}(\theta)$ generated by a root θ of $x^3 - x - 1 = 0$ has class number 1 and unit group $\{\pm\theta^n\}_{n=1}^{\infty}$.
8. Show that $K = \mathbb{Q}(\sqrt{30})$ has class number two and unit group $O_K^* = \{\pm(11 + 2\sqrt{30})^n\}_{n\in\mathbb{Z}}$. (Hint: Compute some norms.) Find the continued fraction for $\sqrt{30}$ and verify that this gives rise to a fundamental unit in O_K^* in the way discussed in class.

4. Elliptic curves and class groups

Suppose k is a field of characteristic different from 2 and that $g(t) \in k[t]$ is a monic separable polynomial of degree 3. The polynomial $Y^2 - g(t) \in k(t)[Y]$ is separable and irreducible as a polynomial in Y. The field $L = k(t)[Y]/(Y^2 - g(t))$ is an elliptic function field; it is isomorphic to the extension of $k(t)$ by the roots y and $-y$ of $Y^2 = g(t)$ in an algebraic closure of $k(t)$. A problem on an earlier problem set showed that the integral closure of $k[t]$ in L is $A = k[t] + k[t]y$; this is not difficult to check using the action of $\mathrm{Gal}(L/k(t)) = \{e, \sigma\}$ on L. Let C_F^0 be the set of discrete valuations of L which are trivial on k. Define v_∞ to be element of C_F^0 such that $v_\infty(g(t)) = -\deg(g(t))$ for $0 \neq g(t) \in k[t]$.

9. Show that v_∞ ramifies in L. Let $w_\infty : L - 0 \to \mathbb{Z}$ be the unique element of C_F^0 over v_∞. Explain why $w_\infty(a(t) + b(t)y) = \max(-2\deg(a(t)), -2\deg(b(t)) - 3)$ if $a(t)$ and $b(t)$ are elements of $k[t]$ which are not both zero. Finally explain why the non-zero elements of A are exactly those for which $w(\alpha) \geq 0$ for all $w \in C_F^0$ different from w_∞.
10. The Riemann Roch Theorem says that if D is a divisor of L, then
$$\dim_k H^0(D) - \dim_k H^0(\kappa - D) = \deg(D) + 1 - g(L)$$
when $g(L)$ is the genus of L and κ is a canonical divisor on L. Recall that $H^0(T) = 0$ if T is a divisor of negative degree, since principal divisors have degree 0 and effective divisors have non-negative degrees. Use problem 9 along with the Riemann-Roch formula for $D = cw_\infty$ and c a large positive integer to show that $g(L) = 1$.
11. Let E_2 be the divisor w_∞. Explain why the argument discussed in class shows that every non-zero element of $\mathrm{Pic}^0(L)$ is represented by a difference $E_1 - E_2$ in which $E_1 \neq E_2$ is an effective divisor of degree 1. Show that such E_1 correspond to solutions (t_0, y_0) of $y_0^2 = g(t_0)$ in which $t_0, y_0 \in k$. Define the set of such solutions to be the set of points $\mathcal{E}(k)$ of the affine curve $\mathcal{E} : Y^2 = g(t)$ over k. (Hint: If w is a valuation of L of degree 1, consider the restriction of w to $k[t]$.)
12. Show that if E_1 and E_2 are as in problem 11, then $E_1 - E_2$ is not a principal divisor. To do this, suppose that $E_1 - E_2 = \mathrm{div}(f)$ for some $f \in L$. Show that $f \in A$ and that $\mathrm{Norm}_{L/k(t)}(f)$ must be a polynomial in t which is either linear constant or linear. Write $f = a(t) + b(t)y$ for some $a(t), b(t) \in k[t]$, and show that no such f exists.
13. Conclude from problems 11 and 12 that $\mathrm{Pic}^0(L)$ is identified with the union of $\mathcal{E}(k)$ with one point $\{\infty\}$ corresponding to the class of the trivial divisor. This union is the set of points over k of the projective smooth curve associated to L. Show that $\mathrm{Pic}^0(L)$ is naturally isomorphic to the ideal class group of A.

5. The Minkowski bound over function fields.

Suppose q is a prime power, and let $\mathbb{F}_q$ be a finite field of order q. Let $L = \mathbb{F}_q(t)$ be the rational function field in one variable t over $\mathbb{F}_q$. Define v_∞ to be the discrete valuation on L such that $v_\infty(g(t)) = -\deg(g(t))$ for $0 \neq g(t) \in \mathbb{F}_q[t]$. Suppose F is a finite separable extension of L. For

simplicity, we will assume that v_∞ splits completely in F; such F are analogs of finite totally real extensions of $\mathbb{Q}$. This problem is about a variation on the Minkowski method for bounding the class number of the integral closure A of $\mathbb{F}_q[t]$ in F.

14. Define $n = [F : L]$, and let $w_1, \ldots, w_n$ be discrete valuations of F which extend v_∞. Show that the inclusion $L \subset F$ gives rise to an isomorphism of completions $L_{v_\infty} \to F_{w_i}$ for all $i = 1, \ldots, n$. This identifies F_{w_i} with the formal power series field $L_{v_\infty} = \mathbb{F}_q((t^{-1}))$. The valuation ring O_{w_i} of F_{w_i} is thus identified with $\mathbb{F}_q[[t^{-1}]]$.
15. Define a Haar measure μ_∞ on $L_{v_\infty} = \mathbb{F}_q((t^{-1}))$ by the requirement that $\mu_\infty(\mathbb{F}_q[[t^{-1}]]) = 1$. Thus $\mu(a + t^{-b}\mathbb{F}_q[[t^{-1}]]) = q^{-b}$ for $a \in L_{v_\infty}$ and $b \in \mathbb{Z}$, since μ is invariant under translation and additive over unions of disjoint open subsets. Define μ to be the Haar measure on $\prod_{i=1}^n F_{w_i}$ which is the product of μ_∞ on each factor $L_{w_i} \equiv \mathbb{F}_q((t^{-1}))$. Suppose $C = (c_{i,j})$ is an invertible $n \times n$ matrix whose entries $c_{i,j}$ lie in $\mathbb{F}_q((t^{-1}))$. Show that if $U = \prod_{i=1}^n O_{w_i}$ then $\mu(O_{w_i}) = 1$. Using the identifications in problem 9, show that the image $C \cdot U$ of U under left multiplication by C is a compact open subset of $\prod_{i=1}^n F_{w_i}$ with

$$\mu(C \cdot U) = q^{-v_\infty(\det(C))}$$

Hints: U and $C \cdot U$ are finitely generated free modules of rank n for the discrete valuation ring $\mathbb{F}_q[[t^{-1}]] = B$. By multiplying C by a non-zero scalar which is close to 0 in B show that it is enough to consider the case in which C has entries in B and $C \cdot U \subset U$. Show that the map $U \to U$ given by $u \to Cu$ induces multiplication by $\det(C)$ on the top exterior power $\Lambda^n U$ of U over B. Then compute $\det(C)B$ a different way by applying the fundamental theorem about finitely generated modules over a P.I.D. to the inclusion of free B-modules of rank n given by $C \cdot U \subset U$.
16. Identify each F_{w_i} with $\mathbb{F}_q((t^{-1}))$ as in problem 9. Show that with this identification, $X = \oplus_{i=1}^n \mathbb{F}_q[t]$ is a discrete subgroup of $Y = \oplus_{i=1}^n F_{w_i}$, in the sense that there is an open neighborhood of each element of X which contains no other element of X. Show that if U is as in problem 10, then $t^{-1}U = \oplus_{i=1}^n t^{-1}O_{w_i}$ is a fundamental domain for X, in the sense that the inclusion $t^{-1}U \to Y$ gives a topological isomorphism $t^{-1}U \to Y/X$. Conclude that $\mu(Y/X) = \mu(t^{-1}U) = q^{-n}$, i.e. X has covolume q^{-n} in Y.
17. Explain why the integral closure A of $\mathbb{F}_q[t]$ in F is a finitely generated free $\mathbb{F}_q[t]$ module of rank n. Let $a_1, \ldots, a_n$ be generators for this module. Let $\psi : F \to \oplus_{i=1}^n F_{w_i}$ be the natural homomorphism. Define C to be the $n \times n$ matrix $(c_{i,j})$ such that the j^{th} column is the vector $\psi(a_j)$ considered as a column vector when we identify each F_{w_i} with $\mathbb{F}_q((t^{-1}))$. Explain why the elements of $\psi(A)$, considered as column vectors, consists of all $\mathbb{F}_q[t]$-linear combinations of the columns of C. Thus $\psi(A) = C \cdot X$ when X is as in problem 11. Show that when $t^{-1}U$ is the open subset as in problem 11, then $C \cdot t^{-1}U$ is a fundamental domain for $\psi(A)$ in $Y = \oplus_{i=1}^n F_{w_i}$. Conclude from this and problems 10 and 11 that $\mu(Y/\psi(A)) = q^{-v_\infty(\det(C))-n}$.
18. For C as in problem 12, show that $-v_\infty(\det(C)) = \deg(\mathrm{Disc}(A/\mathbb{F}_q[t]))/2$, where the degree of the disciminant ideal $\mathrm{Disc}(A/\mathbb{F}_q[t])$ of $\mathbb{F}_q[t]$ is defined to be the degree of a monic generator of this ideal. The formula at the end of problem 12 then becomes

$$\mu(Y/\psi(A)) = q^{\deg(\mathrm{Disc}(A/\mathbb{F}_q[t]))/2-n}.$$

If you have seen the Hurwitz formula for covers of curves, try checking that the right hand side of this formula gives

$$\mu(Y/\psi(A)) = q^{(2g(F)-2)/2} \tag{5.1}$$

when $g(F)$ is the genus of the smooth projective curve over $\mathbb{F}_q$ with function field F. The constant $q^{2g(F)-2}$ is the function field counterpart of the absolute value of the disciminant of the ring of integers of a number field. The equation (5.1) is the counterpart of the corresponding formula for totally real number fields.

19. Suppose S is an open compact subgroup of $Y = \oplus_{i=1}^{n} F_{w_i}$. Let T be a finitely generated $\mathbb{F}_q[t]$-submodule of Y which is co-compact. Show that if $\mu(S) > \mu(Y/T)$, then there is a non-zero element $s \in S \cap T$. Thus S is a function field counterpart of the convex symmetric subsets which come up in the classical theory of geometry of numbers, and there is no power of 2 needed in the function field case.
20. Use problems 14 and 15 to show the following counterpart of the classical Minkowski bound for the ideal classgroup of A. Suppose $\mathcal{C}$ is a non-zero integral ideal of A. Prove that there is a non-zero element $x \in \mathcal{C}$ such that

$$[A : Ax] \leq q \cdot q^{(2g(F)-2)/2}[A : \mathcal{C}] \tag{5.2}$$

Here the index $[A : \mathcal{C}]$ is the counterpart of the norm of an integral ideal of the ring of integers of a number field, $q^{(2g(F)-2)/2}$ is the counterpart of the square root of the discriminant of the field, and the Minkowski constant in the "totally real" function field case becomes simply q. Compare this result to what you can prove using Riemann-Roch.
Hints: Let w_1 be a fixed choice of a valuation of F over v_∞. Try using a compact open subset of $Y = \oplus_{i=1}^{n} F_{w_i}$ of the form

$$S = (t^c O_{w_1}) \times \prod_{i=2}^{n} O_{w_i}$$

for a well chosen integer c.