Math 581g, Fall 2011, Homework 5

William Stein (wstein@uw.edu)

Due: Wednesday, November 16, 2011

There are 7 problems. Turn your solutions in Monday, November 11, 2011 in class (or via email). You may work with other people. You can find the LaTeX of this file at http://wstein.org/edu/2011/581g/hw/. I will have office hours 11:00am-3:15pm on Thursday, November 10 in Padelford C423.

1. (Warm up) Find an element of $\mathrm{SL}_2(\mathbf{Z})$ that reduces modulo 30 to
$$\begin{pmatrix} -3 & 4 \\ 14 & 21 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/30\mathbf{Z}).$$

2. (a) (Warm up) Suppose $\varphi : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ is a nonzero map of complex tori induced by a $\mathbf{C}$-linear map T. Prove that the kernel of φ is isomorphic to $\Lambda_2/T(\Lambda_1)$.
   (b) (Though it doesn't mention abelian varieties, the following exercise is useful for understanding them.) Let V_i be finite dimensional complex vector spaces and let $\Lambda_i \subset V_i$ be lattices (so $\mathrm{rank}_{\mathbf{Z}}(\Lambda_i) = 2\dim_{\mathbf{C}} V_i$ and $\mathbf{R}\Lambda_i = V_i$). Suppose $T : V_1 \to V_2$ is a *surjective* $\mathbf{C}$-linear map such that $T(\Lambda_1) \subset \Lambda_2$. Observe that T induces a homomorphism $\varphi : V_1/\Lambda_1 \to V_2/\Lambda_2$.
      i. If the kernel of φ is finite, prove that it is isomorphic to $\Lambda_2/T(\Lambda_1)$. [Hint: One approach to this problem is to use the "snake lemma", which you can look up in many places.]
      ii. How can you describe and compute $\ker(\varphi)$ when it is infinite?

3. Write down a definition of the Weil pairing that makes sense for an elliptic curve over any base field. You are allowed to copy the definition from a book such as Silverman's. You don't have to understand it; the point is just that you see a completely different definition than the one I gave in class.

4. Let E be the elliptic curve with Weierstrass equation $y^2 = x(x-1)(x+1)$, let $P = (0,0)$ and $Q = (1,0)$. Let C be the cyclic group of order 2 generated by P. [Remark: Writing a program to solve all problems like this one automatically would be a good contribution to Sage, and a good final project idea.]
   (a) Find (a numerical approximation to) τ in the upper half plane such that (E, C) is isomorphic to (E_τ, C_τ), where notation is as in class.
   (b) Find τ in the upper half plane such that (E, P) is isomorphic to (E_τ, P_τ).
   (c) Find τ in the upper half plane such that (E, P, Q) is isomorphic to (E_τ, P_τ, Q_τ).

5. Prove that when $\Gamma = \mathrm{SL}_2(\mathbf{Z})$ then $\Gamma\backslash\mathbf{P}^1(\mathbf{Q})$ has cardinality 1.

6. Fix a positive integer M, a prime q, and let $\alpha = \mathrm{ord}_q(M)$. Use the extended Euclidean algorithm to show that there exists integers x, y, z such that $q^{2\alpha}x - yMz = q^\alpha$. Are x, y, z necessarily unique? (This little exercise is relevant to defining Atkin-Lehner operators, which I hope we get to in this class.)

7. Write a paragraph (or more) about what you plan to do your final project about.