Math 581g, Fall 2011, Homework 5: SOLUTIONS

William Stein (`wstein@uw.edu`)

November 30, 2011

1. (Warm up) Find an element of $\mathrm{SL}_2(\mathbf{Z})$ that reduces modulo 30 to
$$A = \begin{pmatrix} -3 & 4 \\ 14 & 21 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/30\mathbf{Z}).$$
Solution. Adding 30 to the lower left entry gives the equivalent matrix $\left(\begin{smallmatrix} -3 & 4 \\ 44 & 21 \end{smallmatrix}\right)$, whose bottom two entries are coprime. Using the Euclidean algorithm `xgcd(44,21)` then yields, e.g., that $1 = 10 \cdot 44 + 21 \cdot 21$, so $B = \left(\begin{smallmatrix} 21 & 10 \\ 44 & 21 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$. We have $A \cdot B^{-1} \equiv C = \left(\begin{smallmatrix} 1 & 24 \\ 0 & 1 \end{smallmatrix}\right)$, so $A \equiv CB \equiv \left(\begin{smallmatrix} 1077 & 514 \\ 44 & 21 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ is a choice of lift. There are of course many choices of lift.

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 $\Lambda_2/T(\Lambda_1)$.
Solution. See below.
(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 $\mathbf{C}$-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.]
   Solution. See below.
   ii. How can you describe and compute $\ker(\varphi)$ when it is infinite?
   Solution. See below.

   The image of φ is a complex torus since it the continuous image of a compact connected topological space. Thus for the purposes of describing $\ker(\varphi)$, we may replace V_2 by $T(V_1)$ and Λ_2 by $T(V_1)\cap\Lambda_2$, and hence assume $T : V_1 \to V_2$ is surjective. We answer the above questions by proving that $\ker(\varphi)$ sits in the exact sequence of abelian groups
$$0 \to \frac{\ker(T)}{\Lambda_1 \cap \ker(T)} \to \ker(\varphi) \to \left(\frac{\Lambda_2}{T(\Lambda_1)}\right) \to 0.$$
   The first term in the sequence is the connected component of the kernel, and the last term is the finite discrete group of components of the not-necessarily-

connected kernel. To obtain the exact sequence we use the snake lemma:

$$
\begin{tikzcd}
 & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[d] \arrow[dddll, rounded corners] & \\
 & \Lambda_1 \arrow[r, "f"] \arrow[d, "T"] & V_1 \arrow[r, "g"] \arrow[d, "T"] & V_1/\Lambda_1 \arrow[r] \arrow[d, "\varphi"] & 0 \\
0 \arrow[r] & \Lambda_2 \arrow[r, "f'"] \arrow[d] & V_2 \arrow[r, "g'"] \arrow[d] & V_2/\Lambda_2 \arrow[d] & \\
 & D \arrow[r] & E \arrow[r] & F &
\end{tikzcd}
$$

Noting that $T : V_1 \to V_2$ is surjective, so $E = 0$, the snake lemma yields an exact sequence $0 \to B/A \to C \to D \to 0$. Since $B/A \cong \ker(T)/(\Lambda_1 \cap \ker(T))$ and $C = \ker(\varphi)$ and $D = \Lambda_2/T(\Lambda_1)$, this completes the proof.

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.

   Solution. (Just look in a book.)

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.

   Solution. It turns out that E has CM (complex multiplication), so this problem can be done by "pure thought", without resorting to computer computations. First, some general observations on this problem. We have $j(E) = 1728$, so E happens to be a CM curve with CM by $\mathbf{Z}[i]$, so $E_{\mathbf{C}} \cong \mathbf{C}/(\mathbf{Z}i+\mathbf{Z})$. Also, $\mathrm{Aut}(E_{\mathbf{C}}) = \langle i \rangle$ has order 4. There are 3 nontrivial 2-torsion points in $\mathbf{C}/(\mathbf{Z}i+\mathbf{Z})$, namely $t_1 = [i/2], t_2 = [1/2], t_3 = [(i+1)/2]$. The automorphism given by multiplication by i swaps t_1 and t_2 and fixes t_3. That same automorphism (or its negative) on E is given by $(x, y) \mapsto (-x, iy)$; the three nontrivial 2-torsion points on E are $P = (0,0), Q = (1,0), R = P+Q = (-1,0)$, and the automorphism of order 4 acts on P, Q, R by fixing P and swapping Q and R.

   Recall that $E_\tau = \mathbf{C}/(\mathbf{Z}\tau + \mathbf{Z})$ and $P_\tau = [1/N]$ and $Q_\tau = [\tau/N]$, for $N = 2$. Since the point $P = (0,0)$ is fixed and t_3 is fixed, we must find τ so that there is an isomorphism $\mathbf{C}/(\mathbf{Z}\tau + \mathbf{Z}) \approx \mathbf{C}/(\mathbf{Z}i + \mathbf{Z})$ that sends $[1/2]$ to $[(i+1)/2]$. Taking the isomorphism to be given by multiplication by $(i+1)$, we see that $\tau = \frac{i}{i+1} = \frac{1+i}{2}$ works.

   (b) Find τ in the upper half plane such that (E, P) is isomorphic to (E_τ, P_τ).

Solution. Since P has order 2, the answer to the previous problem suffices: take $\tau = \frac{1+i}{2}$.

(c) Find τ in the upper half plane such that (E, P, Q) is isomorphic to (E_τ, P_τ, Q_τ).

Solution. Again, we take $\tau = \frac{1+i}{2}$, and fix a choice of isomorphism $E_\tau \to E$ that sends P_τ to P. Then Q_τ maps to either Q or R (using the notation of the solution to the first part of this problem). If Q_τ maps to R, simply compose the isomorphism with an automorphism of order 4, which works because that automorphism fixes P_τ and swaps Q and R.

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

   Solution. Let a/c be a rational number in lowest terms, and use the extended Euclidean algorithm to find integers b, d such that $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$. Then $\gamma(\infty) = a/c$, so $[\infty] = [a/c] \in \mathbf{P}^1(\mathbf{Q})$.

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 is relevant to defining Atkin-Lehner operators.)

   Solution. For the first part, use the Euclidean algorithm and that $\gcd(M, q^{2\alpha}) = q^\alpha$ to find integers A, B such that $Aq^{2\alpha} + BM = q^\alpha$, then take $x = A, y = -B, z = 1$. For the second, of course x, y, z are not unique, since e.g. you could also take $y = 1, z = -B$.