Math 581g, Fall 2011, Homework 2: SOLUTIONS

William Stein (wstein@uw.edu)

October 20, 2011

1. (Easy warm up) Suppose $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ is a lattice in $\mathbf{C}$. Prove that either ω_1/ω_2 or ω_2/ω_1 is in the complex upper half plane.

   Solution. We have $\omega_1/\omega_2 \notin \mathbf{R}$, since $\mathbf{R}L = \mathbf{C}$. If ω_1/ω_2 in the lower half plane, then its inverse is in the upper half plane, by basic algebra.

2. (Warm up) Let M_k denote the space of modular forms of weight k and level 1. Prove that if $k \geq 2$ and $f \in M_k$ is a constant function, then $f = 0$.

   Solution. Since $f \in M_k$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$, we have $f(-1/z) = z^{-k} f(z)$ for all $z \in \mathfrak{h}$. If $f \neq 0$ is constant, then $z^{-k} = 1$ for all $z \in \mathfrak{h}$, which is a contradiction since $k \geq 2$.

3. Let E be an elliptic curve over $\mathbf{C}$ given by a Weierstrass equation $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$. Prove that the differential $\omega = \frac{dx}{2y + a_1 x + a_3}$ has no poles. You may follow the proof presented in class in the special case when $a_1 = a_2 = a_3 = 0$. [Though you can read a complete proof of this in Silverman's book on elliptic curves, I encourage you not to.]

   Solution. First we consider the behavior of ω at ∞. The homogeneous equation is
$$Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3,$$
   and $x = X/Z$, $y = Y/Z$. Factoring out Z, we find that
$$X^3 = Z(Y^2 + a_1 XY + a_3 YZ - a_2 X^2 - a_4 XZ - a_6 Z^2) = Zu,$$
   where u is a unit in the local ring R_P corresponding to the point $P = (0:1:0)$. Thus $x = u_0 X^{-2}$, for a unit $u_0 \in R_P$, hence $\mathrm{ord}_\infty(x) = -2$ and $dx = -2u_0 X^{-3} dX$ has a pole of order 3 at infinity. Also, $\mathrm{ord}_\infty(y) = -3$, so using a basic property of ord, we find that $\mathrm{ord}_\infty(2y + a_1 x + a_3) = -3$, since $\mathrm{ord}_\infty(a_1 x) \geq -2$ and $\mathrm{ord}_\infty(a_3) \geq -2$. It follows that $\mathrm{ord}_\infty(\omega) = \mathrm{ord}_\infty(dx/(2y + a_1 x + a_3)) = 0$.

   Next, we consider the behavior at the affine points P where $2y + a_1 x + a_3 = 0$. Taking derivatives, we have
$$(2y + a_1 x + a_3)dy + a_1 y dx = (3x^2 + a_2 x + a_4)dx,$$
   so
$$\omega = \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + a_2 x + a_4 - a_1 y}, \tag{0.1}$$
   and
$$\frac{dx}{dy} = \frac{3x^2 + a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3}.$$

The zeros of $2y + a_1x + a_3$ are at the points where there is a vertical tangent, i.e., at the nontrivial 2-torsion points on E, so there are exactly 3 distinct zeros. Since $\mathrm{ord}_\infty(2y + a_1x + a_3) = -3$, these 3 distinct zeros occur with multiplicity 1. Also, since there are 3 distinct 2 torsion points (at which $\frac{dx}{dy} \to \infty$), the function $3x^2 + a_2x + a_4 - a_1y$ cannot vanish at any point where $2y + a_1x + a_3$ vanishes. Since dy has no poles on the affine plane, and the denominator in the right hand side of (0.1) does not vanish at the points P, we see that ω has no poles at the points P.

4. Let K be a number field and ℓ a prime number. Prove that

$$K \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \cong \prod_{\lambda \mid \ell} K_\lambda.$$

Here $\lambda \mid \ell$ are the prime ideals of the ring of integers of K that contain ℓ and K_λ is the completion of K at λ.

Solution. Let R be the ring of integers of K. We prove that $R \otimes \mathbf{Z}_\ell \cong \bigoplus_{\lambda \mid \ell} R_\lambda$. Using that R is a Dedekind domain, we can write (uniquely) $\ell R = \prod_{\lambda_i \mid \ell} \lambda_i^{e_i}$, and for each positive integer n, we have $\ell^n R = \prod_{\lambda_i \mid \ell} \lambda_i^{e_i n}$. Using the Chinese remainder theorem and various compatibilities between finite direct sums and limits, we have

$$\begin{aligned} R \otimes \mathbf{Z}_\ell &\cong R \otimes \varprojlim_n \mathbf{Z}/\ell^n\mathbf{Z} \cong \varprojlim_n R \otimes \mathbf{Z}/\ell^n\mathbf{Z} \cong \varprojlim_n R/\ell^n R \\ &\cong \varprojlim_n \bigoplus_{\lambda_i \mid \ell} R/\lambda_i^{e_i n} \cong \bigoplus_{\lambda_i \mid \ell} \varprojlim_n R/\lambda_i^{e_i n} \cong \bigoplus_{\lambda \mid \ell} R_\lambda. \end{aligned}$$

The result then follows by tensoring both sides of the above isomorphism by $\mathbf{Q}$.

5. Let E be the elliptic curve $y^2 = x(x-1)(x+1)$. Show that the representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_2)$ that gives the action of the Galois group on $E[2]$ is reducible, i.e., has an invariant subspace of dimension 1.

Solution. The representation sends each element $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ to the identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Thus any nonzero proper subspace is invariant.

6. In the section of the textbook called *Modular forms as functions on lattices* we define maps between the set $\mathcal{R}$ of lattices in $\mathbf{C}$ and the set $\mathcal{E}$ of isomorphism classes of pairs (E, ω), where E is an elliptic curve over $\mathbf{C}$ and $\omega \in \Omega_E^1$ is a nonzero holomorphic differential 1-form on E. Prove that the maps in each direction defined in the book are bijections. (See Appendix A1.1 of Katz's *p-adic properties of modular schemes and modular forms.*)

Solution. If you understand Section 5 of Chapter VI of [Silverman, *The Arithmetic of Elliptic Curves*] then you can do this problem. In particular, given an elliptic curve E over $\mathbf{C}$ and a nonzero differential ω on E, we can use algebra to find a Weierstrass equation of the form $y^2 = 4x^3 + ax + b$ with $\omega = dx/y$. The *proof* of [Prop. 5.2(a), loc. cit.] implies that if $\Lambda = \{\int_\gamma \omega : \gamma \in \mathrm{H}_1(E(\mathbf{C}), \mathbf{Z})\}$, then $\mathbf{C}/\Lambda \cong E(\mathbf{C})$ via the analytic isomorphism induced by the Weierstrass function $\wp_\Lambda$ associated to Λ. This implies surjectivity of $\mathcal{R} \to \mathcal{E}$ and that the composition of the two maps is the identity on $\mathcal{E}$. The other key fact you need is [Cor. 5.1.1, loc. cit.], which ensures that $\mathcal{R} \to \mathcal{E}$ is injective. (Silverman does not give a complete proof, but gives four references for the key fact that he omits.)

7. Prove that the number of subgroups of $\mathbf{Z}^2$ of index n is equal to the sum of the positive divisors of n. [Hint: first do the case $n = p$ is prime first as a warm up, then reduce to the prime power case.]

   Solution. First we reduce to the prime power case by applying the structure theorem for finite abelian groups to the abelian group $\mathbf{Z}^2/L$ of order n. We may thus assume that the index of L in $\mathbf{Z}^2$ is a prime power p^m. The lattices L of index p^m in $\mathbf{Z}^2$ are in bijection with the Hermite normal form matrices of determinant p^m, which are easy to count. They are the one matrix $\left(\begin{smallmatrix} p^m & 0 \\ 0 & 1 \end{smallmatrix}\right)$, the p matrices $\left(\begin{smallmatrix} p^{m-1} & b \\ 0 & p \end{smallmatrix}\right)$ with $0 \leq b < p$, the p^2 matrices $\left(\begin{smallmatrix} p^{m-2} & b \\ 0 & p^2 \end{smallmatrix}\right)$ with $0 \leq b < p^2$, etc., up through the p^m matrices $\left(\begin{smallmatrix} 1 & b \\ 0 & p^m \end{smallmatrix}\right)$ with $0 \leq b < p^m$. Summing, we find $1 + p + p^2 + \cdots + p^m$ matrices, as claimed.