Exercise Set 8 – Arithmetic Geometry, Frank Thorne (thorne@math.sc.edu)

Due Monday, April 25, 2016

Do **one** of the two problems. (You are welcome to do both of course, but this is not required or expected.) The first problem is recommended for those interested in number theory; the second is recommended for anyone interested in algebraic geometry or commutative algebra.

(1) This exercise is adapted from Section 8.8 of Washington's book. **Please do not read the solution given there!**

Let E be the elliptic curve over $\mathbb{Q}$ given by $y^2 = x(x-2p)(x+2p)$, where p is a prime $\equiv 9 \pmod 1$6. Then one element of the 2-Selmer group of E is the curve

$$C = C_{1,p,p} \ : \ u^2 - pv^2 = 2p, \quad u^2 - pw^2 = -2p.$$

(Both equations together are the curve – it takes two equations to cut out a curve in $\mathbb{A}^3$; one equation only gives you a surface.) Prove that it has p-adic points for all primes $p \leq \infty$, but does not have any rational points – therefore implying that it represents a nontrivial element of the Shafarevich-Tate group.

One outline for such a proof (which you will probably follow, but feel free to deviate from it) is as follows.

(a) Suppose that (u, v, w) is a rational point on C. Prove that we can write

$$u = \frac{pr}{e}, \ v = \frac{s}{e}, \ w = \frac{t}{e}$$

where e, u, v, w are integers and e is coprime to $prst$.

(b) Substituting into the original equation, prove that $s^2 + 4e^2 = t^2$ and that s is coprime to $2e$. Recall that there are thus coprime integers m and n with

$$2e = 2mn, \ s = m^2 - n^2, \ t = m^2 + n^2.$$

(c) Prove that $pr^2 = m^4 + n^4$, that $m \not\equiv n \pmod 2$, and that any prime divisor q of r does not divide either m or n.

(d) With q as above, argue that $(m/n)^4 \equiv -1 \pmod q$. Conclude that $q \equiv 1 \pmod 8$, and then explain why r is.

(e) Explain why we can conclude that $m^4 + n^4 \equiv 9 \pmod{16}$, and why this is impossible. Conclude that $C(\mathbb{Q}) = \emptyset$.

(f) Prove that C has a real point.

(g) For $q = 2$, prove that there exists a solution in $\mathbb{Q}_2$ of the form

$$u = \frac{1}{2}, \ v = \frac{v_1}{2}, \ w = \frac{w_1}{2}.$$

You will use the fact that any integer $\equiv 1 \pmod 8$ has a square root in $\mathbb{Q}_2$. (This is all you need to know about $\mathbb{Q}_2$ to solve this part.)

(h) For $q = p$, a solution is given by

$$u = 0, \ v = \sqrt{-2}, \ w = \sqrt{2}.$$

If you know Hensel's lemma (or look it up), you can use it to give a proof that $\mathbb{Q}_p$ contains square roots of 2 and -2. Otherwise, take this for granted and go on to the next part.

(i) Finally, we prove that there are $\mathbb{Q}_q$-adic points for all $q \neq 2, p, \infty$. For any such q, we **assume** that there is a solution in $\mathbb{F}_q$, i.e. a solution modulo q. This follows from the Hasse bound (i.e., the Weil conjectures), except for small q which can be treated in an ad hoc manner.

Fix any such q, and solution (u_1, v_1, w_1) modulo q. Then (by construction of the q-adic numbers) there is a q-adic solution to C if and only if there are solutions (u_k, v_k, w_k) modulo q^k for each integer $k \geq 1$, with $(u_{k+1}, v_{k+1}, w_{k+1}) \equiv (u_k, v_k, w_k) \pmod{q}^k$.

Prove, by induction on k, that there are such solutions (u_k, v_k, w_k).

(2) Let A, B, C be abelian groups (with the operation written additively) together with the action of an abelian group G. Suppose that these fit into an exact sequence

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0.$$

Prove that this induces a long exact sequence

$$0 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, C) \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C).$$

(Note that the last map does not have to be surjective.)

A suggested outline for doing this is as follows:

(a) Recall that $H^0(G, M)$ just consists of the elements of M which are fixed by every element of G. Prove that we get an exact sequence

$$0 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, C).$$

(b) Recall that $H^1(G, M)$ consists of **cocycles** modulo **coboundaries**, where a cocycle is a map $f \ : G \to M$ with $f(g_1 g_2) = f(g_1) + g_1 f(g_2)$ for all $g_1, g_2 \in G$, and a coboundary is any map $G \to M$ of the form $f(g) = gm - m$ for some fixed $m \in M$.

Prove that a homomorphism $\alpha \ : \ M \to M'$ of G-modules induces a map

$$\phi_* \ : \ H^1(G, M) \to H^1(G, M'),$$

defined by $(\phi_*(f))(g) = \phi(f(g))$.

(c) Prove that the maps ϕ and ψ induce an exact sequence

$$H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C).$$

(Note that it is claimed only that the image of the first map is the kernel of the second.)

(d) Define a map

$$\delta \;:\; H^0(G,C) \longrightarrow H^1(G,A)$$

as follows. For any $c \in H^0(G,C)$, $c = \psi(b)$ for some b. Define $\delta(c)$ to be the map $g \to g \cdot b - b$. Prove that δ is well-defined: that this indeed is a map into A (and not just B); that is satisfies the cocycle condition, and that if a different preimage b of c is chosen, the two maps $\delta(c)$ differ only by a coboundary.

(e) Prove that the kernel of δ is the image of $H^0(G,B)$ in $H^0(G,C)$.

(f) Prove, finally, that the image of δ is the kernel of ϕ_*.

– For a proof, see any book on group cohomology. *L. Washington, Elliptic Curves*

– Everything follows from a straightforward, but tedious, diagram chase that we leave to the reader. *J. Silverman, The Arithmetic of Elliptic Curves*

– For by a basic theorem of homological algebra, the $H^q(G,A)$ so defined satisfy the exactness property... *Cassels and Frohlich, ed., Algebraic Number Theory* (which purports to give an introduction to the subject form scratch)

– The proof of the exactness is then routine, and consists in chasing around diagrams. It should be carried out in full by the reader who wishes to acquire a feeling for this type of triviality. *S. Lang, Algebra*

– Take any book on homological algebra, and prove all the theorems without looking at the proofs given in that book. *Exercise from the second edition of S. Lang, Algebra*

– We will not print the proof in these notes, because it is best done visually. *C. Weibel, An Introduction to Homological Algebra*

The only complete proof I have seen in print is in Hatcher's book on algebraic topology. But you can watch Jill Clayburne present a proof of the (closely related) Snake Lemma here:

`https://www.youtube.com/watch?v=etbcKWEKnvg`

Please don't be That Guy.