Homework

Due: Friday, April 17

1. Let $E/\mathbb{Q}$ be an elliptic curve. Use the canonical height $\hat{h}$ (see HW 7) to (re)prove:

   (a) The torsion group of $E(\mathbb{Q})$ is finite.

   (b) Let $m \geqslant 2$ be an integer such that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite. Then $E(\mathbb{Q})$ is finitely generated. (HINT: *Let* $\{Q_1, \cdots, Q_r\} \in E(\mathbb{Q})$ *be representatives for* $E(\mathbb{Q})/mE(\mathbb{Q})$, *and let* $A = 2\max_i \hat{h}(Q_i)$. *Show there is a constant* $C < 1$ *such that if* $P, R \in E(\mathbb{Q})$, $\hat{h}(P) > A$, *and* $P - Q_i = mR$, *then*
   $$\hat{h}(R) \leqslant C\hat{h}(P).$$
)

2. The Néron-Tate pairing on $E(\mathbb{Q})$ is
$$E(\mathbb{Q}) \times E(\mathbb{Q}) \xrightarrow{\langle\cdot,\cdot\rangle} \mathbb{R}$$
$$(P, Q) \longmapsto \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

   (a) Show that $\langle\cdot,\cdot\rangle$ is a $\mathbb{Z}$-bilinear symmetric form.

   (b) Suppose $P_1, \cdots, P_r \in E(\mathbb{Q})$. Define a matrix A with entries
   $$A_{ij} = \langle P_i, P_j \rangle.$$
   Show that the points $P_1, \cdots, P_r$ are linearly independent in $E(\mathbb{Q})$ if and only if $\det(A) \neq 0$.

3. Let $G = \langle\sigma\rangle$ be a cyclic group of order r, let M be a G-module, and let $f : G \to M$ be a crossed homomorphism.

   Let $m = f(\sigma)$.

   (a) Explain how to calculate $f(\sigma^i)$ for each i.

   (b) Show that m must satisfy
   $$m + \sigma m + \sigma^2 m + \cdots + \sigma^{r-1} m = 0. \tag{1}$$

   (c) Conversely, let $n \in M$ be any element which satisfies (1). Show that there is a crossed homomorphism $g : G \to M$ such that $g(\sigma) = m$.

4. Let L/K be a cyclic extension of degree r, and let σ generate $\mathrm{Gal}(L/K)$.

   If $\alpha \in L^\times$, its norm is
   $$N_{L/K}(\alpha) = \prod_{i=0}^{r-1} \sigma^i(\alpha).$$

(Warmup: Show that $N_{L/K}(\alpha) \in K^\times$.)

Show that our cohomological version of Hilbert's Theorem 90 ($(H^1(\mathrm{Gal}(L/K), L^\times) = 1$) implies the following classical form:

Suppose $\alpha \in L^\times$ satisfies $N_{L/K}(\alpha) = 1$. Then there exists some $\beta \in L^\times$ such that $\alpha = \beta/\sigma(\beta)$.

(a) Show that there is a crossed homomorphism $f : G \to L^\times$ such that $f(\sigma) = \alpha$. (HINT: *Use the multiplicative version of Problem* (3).)

(b) What does Hilbert 90 say about this f?

5. Here is a somewhat modern treatment of Pythagorean triples. Let a, b and c be nonzero integers such that

$$a^2 + b^2 = c^2.$$

Use Hilbert 90 to show that

$$(a, b, c) \text{ is proportional to } (m^2 - n^2, 2mn, m^2 + n^2) \tag{2}$$

for certain integers m and n, as follows.

We will need the field $\mathbb{Q}(i)$; it is a quadratic (thus cyclic) extension of $\mathbb{Q}$, with Galois group $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ generated by $\sigma : x + iy \mapsto x - iy$.

(a) Consider the number

$$\alpha = \frac{a + bi}{c} \in \mathbb{Q}(i).$$

Show there exists $\beta \in \mathbb{Q}(i)^\times$ such that

$$\frac{\beta}{\sigma(\beta)} = \alpha.$$

(HINT: *What is* $N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha)$*?*)

(b) Choose some $r \in \mathbb{Z}$ such that $r\beta = m + in \in \mathbb{Z}[i]$. Show that

$$\alpha = \frac{(m^2 - n^2) + i(2mn)}{m^2 + n^2}.$$

(HINT: $\beta/\sigma(\beta) = r\beta/\sigma(r\beta)$.)

(c) Show that (2) holds.