ELLIPTIC CURVES PROBLEM SET V.
(B. CONRAD, LISBON SUMMER SCHOOL, 2011)

Let $\mathscr{F}$ denote the set of triples (X, Y, Z) of nonzero integers such that $\gcd(X, Y, Z) = 1$ and $X^4 + Y^4 = Z^2$. Fermat proved $\mathscr{F} = \emptyset$ by "infinite descent", and the exercises below interpret his method in terms of the Mordell–Weil Theorem on an elliptic curve over $\mathbf{Q}$.

V.1. Let $\mathscr{F}^+$ denote the set of triples $(x, y, z) \in \mathscr{F}$ with $x, y, z > 0$, so $\mathscr{F} = \emptyset$ if and only if $\mathscr{F}^+ = \emptyset$ (why?). Assume $\mathscr{F} \neq \emptyset$, and choose $(x_0, y_0, z_0) \in \mathscr{F}^+$. Fermat applied the Pythagorean parameterization to the triple (x_0^2, y_0^2, z_0) (and used artful manipulations) to construct $(x_1, y_1, z_1) \in \mathscr{F}^+$ so that

$$(x_0, y_0, z_0) = (x_1^4 - y_1^4, 2x_1y_1z_1, z_1^4 + 4x_1^4y_1^4).$$

(In particular, $1 \leqslant z_1 < z_0$, so by iterating ad infinitum we reach a contradiction.)

Check that the incredible expression on the right side defines a map $f : \mathscr{F} \to \mathscr{F}$ (so Fermat really proved that $f(\mathscr{F}^+)$ contains $\mathscr{F}^+$).

V.2. Let $C = \{(u, v) \in \mathbf{C}^2 \mid v^2 = u^4 + 1\}$, and let E be the elliptic curve $\{w^2 = t^3 - 4t\}$.

(i) Check that $(X, Y, Z) \mapsto (X/Y, Z/Y^2)$ defines a bijection between $\mathscr{F}$ and the set of the $\mathbf{Q}$-points $(u, v) \in C(\mathbf{Q})$ with $v \neq 1$ (i.e., $C(\mathbf{Q}) - \{(0, 1)\}$).

(ii) Check that $(u, v) \mapsto (2u^2/(v-1), 4u/(v-1))$ and $(t, w) \mapsto (2t/w, 1 + 8t/w^2)$ define inverse bijections $E(\mathbf{Q}) - E[2] \leftrightarrow C(\mathbf{Q}) - \{(0, 1)\}$.

(iii) Using the bijections from $\mathscr{F}$ to $C(\mathbf{Q}) - \{(0, 1)\}$ to $E(\mathbf{Q}) - E[2]$, show that Fermat's map $\mathscr{F} \to \mathscr{F}$ is *exactly* the map $P \mapsto (2, 0) \oplus [2](P)$ on $E(\mathbf{Q}) - E[2]$. (This latter map "makes sense" a priori because $E(\mathbf{Q}) - E[2]$ is the set of points of infinite order in $E(\mathbf{Q})$, due to our determination that $E(\mathbf{Q})_{\mathrm{tors}} = E[2]$, but that is not logically relevant here.)

V.3. Now we finally interpret Fermat's infinite descent in terms of the Mordell–Weil Theorem. Let $E(\mathbf{Q})^+$ be the subset of $E(\mathbf{Q}) - E[2]$ that corresponds to $\mathscr{F}^+$. (Beware that this is *not* a subgroup; e.g. it does not contain 0.) It suffices to assume there exists $P_0 \in E(\mathbf{Q})^+$ and to deduce a contradiction.

(i) Show via Exercise V.2(iii) that Fermat's argument constructs $P_1 \in E(\mathbf{Q})^+$ satisfying $P_0 = (2, 0) \oplus [2](P_1)$. Using that $(2, 0)$ is 2-torsion, iterate the procedure to find $P_2 \in E(\mathbf{Q})^+$ so that $P_0 = (2, 0) \oplus [4](P_2)$.

(ii) By iteration (the "infinite descent"), deduce that the difference $P_0 - (2, 0) \in E(\mathbf{Q})$ is infinitely 2-divisible: it lies in $2^n E(\mathbf{Q})$ for all $n \geqslant 1$.

(iii) Use the Mordell–Weil Theorem (!) to show that for any elliptic curve $\mathscr{E}$ over $\mathbf{Q}$ and any prime p, the infinitely p-divisible elements of $\mathscr{E}(\mathbf{Q})$ are exactly the prime-to-p elements in $\mathscr{E}(\mathbf{Q})_{\mathrm{tors}}$ (i.e., the d-torsion elements for d not divisible by p).

(iv) Use that $E(\mathbf{Q})_{\mathrm{tors}} = E[2]$ to deduce a contradiction, so no such P_0 exists!