Exercise 1. Let $a, b, n \in \mathbb{N}$. Prove that if $a^n = b^n$, then $a = b$. [*Suggestion:* You can avoid using the FTA by observing that $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.]

Exercise 2. Let $m \in \mathbb{R}$. Prove that

$$\left(\frac{-2m}{m^2+1}, \frac{1-m^2}{m^2+1}\right)$$

is a rational point if and only if $m \in \mathbb{Q}$.

Exercise 3. Let

$$C(\mathbb{Q}) = \{(X, Y) \mid X, Y \in \mathbb{Q}, X^2 + Y^2 = 1\}.$$

Prove that the function $\pi : \mathbb{Q} \to C(\mathbb{Q})$ given by

$$\pi(m) = \left(\frac{-2m}{m^2+1}, \frac{1-m^2}{m^2+1}\right)$$

is a bijection. [*Suggestion:* Show that, away from $(0, 1)$, the inverse is given by $(X, Y) \mapsto \frac{Y-1}{X}$.]

Exercise 4. Let $r, s \in \mathbb{Z}$ with $(r, s) = 1$, $s \neq 0$, and $r \equiv s \equiv 1 \pmod 2$. Write $r = 2k + 1$ and $s = 2\ell + 1$. Let $u = k + \ell + 1$ and $v = \ell - k$.

$$\left(\frac{-2rs}{r^2+s^2}, \frac{s^2-r^2}{r^2+s^2}\right) = \left(\frac{v^2-u^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right),$$

that the coordinates on the right hand side are reduced, and that $\gcd(u, v) = 1$ and $u \not\equiv v \pmod 2$.