Definition 28.1. Let E_1, E_2 be elliptic curves over a field $\Bbbk$. An *isogeny* is a function $\phi : E_1 \to E_2$ given by polynomials or rational functions in the variables of E_1, which is a group homomorphism.

A general theorem in algebraic geometry states that any rational map from $\phi : E_1 \to E_2$ such that $\phi(\infty_1) = \infty_2$ is an isogeny.

Example 28.2. Let $E : y^2 = x^3 + 1$ over $\Bbbk$. Let $\zeta_3 \in \Bbbk$ satisfy $\zeta_3^2 + \zeta_3 + 1 = 0$. Define $\phi(x, y) = (\zeta_3 x, y)$ and $\phi(\infty) = \infty$. Then ϕ is an isogeny.

Exercise 28.3. Let $p \equiv 1 \mod 3$ be prime and $E : y^2 = x^3 + 1$ over $\mathbb{F}_p$. Let $r > 3$ be a prime dividing $\#E(\mathbb{F}_p)$ such that $r^2 \nmid \#E(\mathbb{F}_p)$. Let ϕ be as above. Show that $\phi(P) = [\lambda]P$ where $\lambda \in \mathbb{Z}_r$ satisfies $\lambda^2 + \lambda + 1 \equiv 0 \mod r$.

Example 28.4. Let $E_1 : y^2 = x(x^2 + ax + b)$ over $\Bbbk$ where $b \neq 0$ and $a^2 - 4b \neq 0$. The function

$$\phi(x, y) = (b/x, -by/x^2)$$

is an isogeny from E_1 to $E_2 : Y^2 = X(X^2 - 2aX + (a^2 - 4b))$ with kernel equal to $\{\infty, (0, 0)\}$.

Mordell-Weil Theorem: Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated.

Case $n = 4$ of Fermat's Last Theorem

Theorem: The equation $x^4 + y^4 = z^4$ has no solution $x, y, z \in \mathbb{N}$ (i.e., $x, y, z > 0$).

Theorem 28.5. The equation $x^4 + y^4 = z^2$ has no solution $x, y, z \in \mathbb{N}$.

Proof:

- Let $x, y, z \in \mathbb{N}$ be a solution with $z > 0$ minimal.
- Can assume $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$, x, z odd and y even.
- (x^2, y^2, z) is a primitive Pythagorean triple so $x^2 = r^2 - s^2, y^2 = 2rs, z = r^2 + s^2$ for coprime integers r, s with r odd and s even.
- $r = c^2, s = 2b^2$ for some coprime $b, c \in \mathbb{N}$, c odd.
- Then
$$a^2 = c^4 - 4b^4$$
and $c < z$.
- Again, may assume $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$, a, c odd and b even.
- $(a, 2b^2, c^2)$ is a primitive Pythagorean triple, so $a = r_1^2 - s_1^2, 2b^2 = 2r_1 s_1, c^2 = r_1^2 + s_1^2$ for some integers r_1, s_1 such that $\gcd(r_1, s_1) = 1$.
- Then $r_1 = x_1^2, s_1 = y_1^2$, $z_1 = c$ satisfy
$$x_1^4 + y_1^4 = z_1^2$$
and $z_1 < z$.