We have seen that integer solutions to $x^2 - dy^2 = 1$ can be found using continued fractions. Given an integer solution (x_1, y_1) one finds infinitely many other integer solutions (x_i, y_i) via $x_i + \sqrt{d}y_i = (x_1 + \sqrt{d}y_1)^i$.

Lemma 24.1. The $\mathbb{Q}$-solutions to $x^2 - dy^2 = 1$ are given by

$$\left(\pm\frac{1+dt^2}{1-dt^2}, \pm\frac{2t}{1-dt^2}\right)$$

where $t \in \mathbb{Q}$.

Example 24.2. Consider the curve $y^2 = x^3 + 1$. What happens when you take a line of slope $t \in \mathbb{Q}$ through $(-1, 0)$?

Idea: Let P_1 and P_2 be two $\mathbb{Q}$-solutions, then the line between them hits the curve at a third $\mathbb{Q}$ solution P_3. One can also take the tangent line at a $\mathbb{Q}$-point P_1 to get a $\mathbb{Q}$-point.

Example 24.3. Let $P_1 = (-1, 0)$ and $P_2 = (0, 1)$ on $y^2 = x^3 + 1$. The line between P_1 and P_2 also meets the curve at $P_3 = (2, 3)$. The tangent line to the curve at P_3 meets the curve at $P_4 = (0, -1)$. It can be shown that the set of all rational solutions to $y^2 = x^3 + 1$ is $\{(-1, 0), (0, \pm 1), (2, \pm 3)\}$.

Natural questions:

(1) How many $\mathbb{Q}$-points can there be on a curve of the form $y^2 = x^3 + Ax + B$?
(2) How many $\mathbb{Q}$-points do you need to start with, to generate all $\mathbb{Q}$-points using the geometric method?
(3) How many $\mathbb{Z}$-points can there be on such a curve?
(4) How does one compute the $\mathbb{Z}$-points?

Exercise 24.4. Let $\Bbbk$ be a field and $A, B \in \Bbbk$. Prove that $x^3 + Ax + B$ has a repeated root if and only if $4A^3 + 27B^2 = 0$.

Definition 24.5. An *elliptic curve* over a field $\Bbbk$ (of characteristic not equal to 2) is an equation $y^2 = x^3 + Ax + B$ with $A, B \in \Bbbk$ such that $4A^3 + 27B^2 \neq 0$.

Definition 24.6. (Projective geometry) Let $\Bbbk$ be a field and $x, y, z \in \Bbbk$. Define the equivalence relation $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for $\lambda \in \Bbbk^*$. A *projective point* is an equivalence class of (x, y, z) where $(x, y, z) \neq (0, 0, 0)$. The *projective plane* is the set $(\Bbbk^3 - (0, 0, 0))/\sim$.

Definition 24.7. A polynomial $f(x, y, z)$ is *homogeneous* of degree d if every monomial $x^i y^j z^k$ in f is such that $i + j + k = d$.

Lemma 24.8. If $f(x, y, z)$ is homogeneous and $P_1 \sim P_2$ then $f(P_1) = 0$ if and only if $f(P_2) = 0$. Hence it makes sense to say that a projective point is a solution to a homogeneous polynomial equation.

Lemma 24.9. Let $f(x,y) \in \Bbbk[x,y]$ is a polynomial of total degree d. define $f^*(x,y,z) = z^d f(x/z, y/z)$. Then f^* is homogeneous of degree d. If $f(x_0,y_0) = 0$ then $f^*((x_0,y_0,1)) = 0$. Solutions to $f^*(x,y,z) = 0$ having $z = 0$ are called *points at infinity*.

Lemma 24.10. There is a single point at infinity on $E : y^2 = x^3 + Ax + B$, namely $(0,1,0)$. We sometimes call this point ∞.

Definition 24.11. A *line* in the projective plane is the set of solutions to $ax + by + cz = 0$ for some $a, b, c \in \Bbbk$.

Bézout's theorem: (Special case) Every line hits $E : y^2z = x^3 + Axz^2 + Bz^3$ at exactly three points counting multiplicities.

Example 24.12. The line at infinity is $z = 0$. The point at infinity on E is an *inflexion*.

Definition 24.13. Define

$$E(\Bbbk) = \{(x,y,z) \in \Bbbk^3 - (0,0,0) : y^2z = x^3 + Ax^2z + Bz^3 = 0\}/\sim .$$

Equivalently,

$$E(\Bbbk) = \{(x,y) \in \Bbbk^2 : y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

We will explain next time that the set $E(\Bbbk)$ is endowed with a group operation $+$. The identity element is ∞. One has $P + Q + R = \infty$ if and only if P, Q and R lie on a line.