This is a file illustrating the mathematical background on the computation of $\mathbb{Q}$-rational points of an elliptic curve (or more generally a plane cubic curve) defined over $\mathbb{Q}$.

1 Abstract elliptic curves

In this section we list some general properties of elliptic curves that are necessary for the understanding of the algorithm. The main reference is [1, Chapter IV].

Definition 1.1. An elliptic curve is a nonsingular curve of genus 1, defined over a field k, together with a distinguished k-rational point.

Here, a curve is a one-dimensional algebraic variety. Abstractly speaking, a k-rational point of a variety X is a morphism of schemes $\operatorname{Spec} k \to X$ such that the composition with the structure morphism $\operatorname{Spec} k \to X \to \operatorname{Spec} k$ is identity. Geometrically, a k-rational point is just a classical geometric point.

Example 1.2. Consider the curve $(x^2 + y^2 - 1 = 0)$ defined over $\mathbb{R}^2$, which is geometrically a cycle. Every point $(\cos\alpha, \sin\alpha)$ is an R-rational point of the curve.
On the other hand, the curve $(x^2 + y^2 + 1 = 0)$ on $\mathbb{R}^2$ has no rational points. But if we consider it as a curve on $\mathbb{C}$, then it indeed has many $\mathbb{C}$-rational points.

The genus here stands for geometric genus, which is the dimension of $H^0(X, \omega_X)$ of a variety X. Geometrically speaking, a smooth curve defined over $\mathbb{C}$ can also be considered as a smooth surface over $\mathbb{R}$, and the geometric genus can be seen as the number of "holesöf the surface. For example, an elliptic curve over $\mathbb{C}$ looks like a torus, if we consider it as a real manifold.

Proposition 1.3. *An elliptic curve can be embedded as a smooth cubic curve in the projective plane $\mathbb{P}^2_k$, such that the distinguished point is mapped to* $[0:0:1]$.

Beweis. This is a consequence of Riemann-Roch theorem of curves, see [1, Theorem IV.1.3]. □

A smooth curve of degree d on $\mathbb{P}^2_k$ is defined by a single homogeneous equation $F(X, Y, Z) = 0$ of degree d.
There is a one-to-one correspondence between the k-rational points on $\mathbb{P}^2_k$ such that the Z-coordinate is non-zero, and the k-rational points on $\mathbb{A}^2_k$. The bijection is given by $[X : Y : Z] \mapsto (\frac{X}{Z}, \frac{Y}{Z})$ and $(x, y) \mapsto [X : Y : 1]$.
If a curve is defined over $\mathbb{P}^2_k$ by $F(X, Y, Z) = 0$, its points with $Z \neq 0$ can be described as the curve $F(x, y, 1) = 0$ on $\mathbb{A}^2_k$, using the identification above. Conversely, given a curve $f(x, y) = 0$ on $\mathbb{A}^2_k$, we can compactify the curve to a curve on $\mathbb{P}^2_k$, processing like follows:
Let $f = \sum_{i=0}^{d} f_i$ be the decomposition of f into homogeneous polynomials, where each f_i has degree i. Define the homogeneous polynomial $F(X, Y, Z) = \sum_{i=0}^{d} f_i(X, Y) \cdot Z^{d-i}$, which is homogeneous of degree d.
Due to the proposition, we will always consider an elliptic curve as a smooth cubic curve in $\mathbb{P}^2_k$. By abuse of notation, we sometimes also write a (not necessarily homogeneous) cubic polynomial in x, y and call it an elliptic curve. In this case we mean the compactification of the curve in $\mathbb{P}^2_k$.

2 Smoothness criterion

It is however not true that given any curve $F = 0$ on $\mathbb{P}^2$, it is smooth. The Jacobian criterion is very useful to determine whether there are non-smooth points on a curve.

Proposition 2.1 (Jacobian criterion)**.** *A point P on a plane curve $F = 0$ on $\mathbb{P}^2_k$ is non-smooth if and*

only if P is a solution of the following system:

$$\begin{aligned} F(P) &= 0, \\ \frac{\partial F}{\partial X}(P) &= 0, \\ \frac{\partial F}{\partial Y}(P) &= 0, \\ \frac{\partial F}{\partial Z}(P) &= 0. \end{aligned}$$

Note that we have defined a curve over an arbitrary field, so the partial derivative of a polynomial with coefficients in the field does not necessarily make sense in analysis. They are rather called "formal derivatives", which are done in the same way as one does to $\mathbb{R}$-polynomials, but have no meaning in differentials.
In the algorithm, when one gives a cubic polynomial, it will not be checked that the curve is smooth everywhere, since the computation of many quadric and cubic functions is too complicated.

3 Bézout's theorem

Theorem 3.1 (Bézout's theorem)**.** *Let k be an algebraically closed field. Let C, D be curves in $\mathbb{P}^2_k$ of degree d,e. Then they intersect at precisely de points, counting multiplicity.*

This is one of the fundamental tools we need to proceed the algorithm, so let us see some examples.

Example 3.2. $x = 0$ and $x + 1 = 0$ are two parallel lines in $\mathbb{A}^2_k$ and do not intersect in $\mathbb{A}^2_k$. However, if we compactify them to lines in $\mathbb{P}^2_k$, we obtain equations $X = 0$ and $X + Z = 0$. Namely, they are curves of degree 1. There is an intersection point $[0 : 1 : 0]$. And by Bézout, it is the unique intersection point.

Example 3.3. consider the quadric $y - x^2 = 0$ and $y = 0$ in $\mathbb{A}^2_k$. They intersect at a double point $(0, 0)$. After compactification, the equations in $\mathbb{P}^2_k$ are $YZ - X^2 = 0$ and $Y = 0$. By Bézout, they only intersect at $[0 : 0 : 1]$ with multiplicity 2.

4 Derivation of the computation in the algorithm

We now give a complete description on the mathematical details in the algorithm.
Let $f = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$ be the equation of the cubic curve over $\mathbb{Q}$. (We again use the abuse of notations between affine equations and projective equations here.) The tangent line at (x_0, y_0) is then given by

$$\frac{\partial f}{\partial x}(x_0, y_0) \cdot x + \frac{\partial f}{\partial y}(x_0, y_0) \cdot y + k = 0,$$

where k is a constant. We pick k correctly such that (x_0, y_0) is indeed on the line. Denote $\frac{\partial f}{\partial x}(x_0, y_0) = u$, $\frac{\partial f}{\partial y}(x_0, y_0) = v$. The tangent equation can be then written as $ux + vy + k = 0$. Now by Bézout, the tangent line will intersect with the cubic at three point, but we know they intersect each other at (x_0, y_0) with multiplicity two, so there is at most one extra intersection point.
However, there are two obstructions. The first one is that Bézout only works over an algebraically closed field but not necessarily over $\mathbb{Q}$. The second one is that Bézout only works over projective plane, but we only consider the affine plane where $Z \neq 0$. We will see that the first obstruction actually will not happen, but the second one may indeed be a problem.
Let us try to compute the equation system given by the cubic and the tangent.

$$\begin{aligned} ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j &= 0, \\ ux + vy + k &= 0. \end{aligned}$$

The first problem is, if the point (x_0, y_0) we have is a non-smooth point, then $u = v = 0$. The tangent line will be in this case a tangent plane. (This indeed makes sense in algebraic geometry!). Then, the tangent plane will not intersect with the cubic at finitely many points. In fact, over $\mathbb{P}^2_{\mathbb{Q}}$, the intersection is just the whole cubic curve. So if we encounter a non-smooth point, the iteration has to be stopped. You might wonder how we derive that u=v=0 from the Jacobian criterion. The fact is, if we take a polynomial $f(x, y)$ and consider its compactification $F(X, Y, Z)$, then $\frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial X}(x_0, y_0, 1)$. And we have the Euler formula $d \cdot F = \frac{\partial F}{\partial X} + \frac{\partial F}{\partial Y} + \frac{\partial F}{\partial Z}$, where d is the degree of the polynomial. So the partial derivates of X and Y being zero already implies the partial derivative of Z being zero.
Now assume (x_0, y_0) is smooth and $v \neq 0$. Indeed, if $v = 0$, then $u \neq 0$, then we can swap the x, y coordinate, which is also realized in the code. By dividing the tangent line equation with v, we get $\frac{u}{v}x + y + \frac{k}{v} = 0$. Replacing u with $\frac{u}{v}$ and k with $\frac{k}{v}$, we may write the line equation as $ux + y + k = 0$. Hence $y = -ux - k$. We substitute all y in the cubic equation with this expression:

$$
\begin{aligned}
&ax^3 + bx^2(-ux - k) + cx(-ux - k)^2 + d(-ux - k)^3 + ex^2 \\
&+ fx(-ux - k) + g(-ux - k)^2 + hx + i(-ux - k) + j = 0. \\
&\Downarrow \\
&ax^3 - bux^3 - bkx^2 + cu^2x^3 + 2cukx^2 + ck^2x - du^3x^3 - 3du^2kx^2 - 3duk^2x - dk^3 \\
&+ ex^2 - fux^2 - fkx + gu^2x^2 + 2gukx + 2gk^2 + hx - iux - ik + j = 0. \\
&\Downarrow \\
&(a - bu + cu^2 - du^3)x^3 + (-bk + 2cuk - 3du^2k + e - fu + gu^2)x^2 \\
&+ \text{lower degree terms} = 0. \\
&\Downarrow \\
&x^3 + \frac{-bk + 2cuk - 3du^2k + e - fu + gu^2}{a - bu + cu^2 - du^3} \cdot x^2 + \text{lower degree terms} = 0.
\end{aligned}
$$

We do not care what the lower degree terms are. We already know two solutions of the cubic equation, namely x_0 and x_0. We know the third solution exists on $\mathbb{C}$. But by Vieta's lemma, the sum of all solutions is precisely the negation of the coefficient of x^2. So the sum is a rational number, and two of the summands are rational, hence the last solution has to be rational! In particular, the tangent line has to intersect with the cubic at a third $\mathbb{Q}$-rational point! The problem is, however, we do not know whether the division in the last step is legal. In other words, we do not know whether $a - bu + cu^2 - du^3$ is non-zero or not. Indeed, if it is zero, it means that the third intersection point in $\mathbb{P}^2_{\mathbb{Q}}$ has actually coordinate of the form $[X : Y : 0]$. So it is not in the $\mathbb{A}^2_{\mathbb{Q}}$ over which we work. (We work under the assumption $Z \neq 0$.) We have to stop the iteration in this situation. An alternative way to to this is to write down the last rational point we get, homogenize the equation f, and pick another affine plane, e.g. $Y \neq 0$. And start the iteration in that affine coordinate again.
If we are lucky enough that we avoid all the obstructions, then the algorithm really gives a third point. However, sometimes the third point coincides with the tangent point. Namely, the tangent line intersects with the cubic at the tangent point with multiplicity three. In this case, the iteration will fall into a cycle. It might be also possible that we have already visited the new point several iterations before, which also means a cycle.
Luckily, the probabilities that the obstructions above only happen in very little possibility. In most cases, we can get an infinite sequence of rational points on the curve by applying the same computation to the new point we get.

Literatur

[1] Hartshorne, Robin. Algebraic geometry. Vol. 52. Springer Science & Business Media, 2013.