Density of rational points on plane curves

Hugues Verdure

Institutt for Matematikk og Statistikk
Universitetet i Tromsø
9037 Tromsø
Norway
Hugues.Verdure@uit.no

Introduction

The study of Diophantine equations, that is finding integer solutions to a polynomial equation with integer coefficients, is a really old branch of mathematics. We can find examples on the subject in India (Baudhayana, 800 BC), in Alexandria (Diophantus, 250 AC), France (Fermat, 1637)...
While Diophantine equations are easy to formulate, solving them might be a different matter. The equations $3x + 8y = 7$ and $3x + 9y = 7$, while quite similar, have completely different sets of solutions. The first one has infinitely many (one of them is $x = -3$, $y = 2$), while the second one has none. Another example is the Pythagoras/Fermat equations $x^n + y^n = z^n$ for $n \geqslant 2$. It is known since Pythagoras that the equation for $n = 2$ has solutions ($x = 3$, $y = 4$, $z = 5$ is one of them), and actually infinitely many and all known. Fermat conjectured in 1637 that the other equations for $n \geqslant 3$ have no solutions, except the trivial ones, that is the one where x, y or z are 0. He even claimed to have a proof, but the margin was not large enough for the proof to fit in. The proof of the Taniyama-Shimura conjecture for semistable elliptic curves by Wiles and Taylor in the early nineties, together with works by Frey and Ribet implies that Fermat last theorem is now proved.
A very related topic is the study of rational points on algebraic curves. This is what we propose to look at. We will give answers to the following questions: given a plane algebraic curve, how many rational points may lie on the curve? And, in case of infinitely many points, are they dense on the curve (that is, given any point on the curve, does there exist a rational point on the curve infinitely near it)?
This paper is motivated by the reading of an article by Mazur [3] where he discusses a general conjecture on rational points on algebraic varieties, conjecture that he proves in the case of plane curves : if a plane curve has infinitely many rational points, then they are dense on some algebraic components of the curve.

The paper is organized as follows. In the first part, we look at curves of degree 1, that is lines, in the second part, we study curves of degree 2, or conics, while in the third part, we see the case of curves of degree 3. We always assume that the curves are irreducible.

The two first parts follow the same scheme. We find the number of rational points that is needed for the curve to have rational coefficients. Once we have such a curve with a rational point, we build a bijection, which is continuous both ways, between the curve and the real line, and that sends rational points to rational numbers. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, rational points are dense in the curve.
The third part involves more advanced mathematics. In this part, we take advantage of the fact that elliptic curves have a natural structure of abelian group. We use this to describe a mapping, from a neighbourhood of the identity element to a neighbourhood of $0 \in \mathbb{R}$, that is bijective, continuous both ways and that preserves in a way the group law. Then we show that the image of rational points by this mapping is dense round 0. In this part, we use results and notation from [4, 5].

Density of rational points on a line

In this section, we shall see that on a line in the real plane, there are either no rational points, or exactly one, or the rational points are dense on the line.

Assume that we have two rational points on a line $\mathcal{L}$, say $P = (x_P, y_P)$, and $Q = (x_Q, y_Q)$, with $P \neq Q$, and $x_P, x_q, y_P, y_Q \in \mathbb{Q}$. If $x_P = x_Q$, then $\mathcal{L}$ is the vertical line $\mathcal{L} : x = x_P$, and the rational points are (x_P, r), $r \in \mathbb{Q}$, and this is of course dense in $\mathcal{L}$. If $x_P \neq x_Q$, then the line $\mathcal{L}$ has equation

$$\mathcal{L} : y = \frac{y_P - y_Q}{x_P - x_Q} x + \frac{y_Q x_P - y_P x_Q}{x_P - x_Q}$$

and the coefficients are rationals. Then we have an homeomorphism between $\mathcal{L}$ and $\mathbb{R}$ given by $(x, y) \mapsto x$, and rational points in both $\mathcal{L}$ and $\mathbb{R}$ are in one-to-one correspondance, which proves that rational points are dense in $\mathcal{L}$.

It is also easy to give examples of lines with no or just one rational point: $\mathcal{L}_0 : y = \sqrt{2}x + 1$ has obviously no rational point, while $\mathcal{L}_1 : y = \sqrt{2}x$ has exactly one, namely $(0, 0)$.

We have thus proved the following:

Proposition 1. *Let $\mathcal{L}$ be a line on the real plane. Then we have exactly one of the following:*

1. *There are no rational points on $\mathcal{L}$*
2. *There is exactly one rational point on $\mathcal{L}$*
3. *An equation of $\mathcal{L}$ can be written with rational coefficients, and the rational points are dense on $\mathcal{L}$.*

Density of rational points on a conic

A conic is an irreducible plane curve of degree 2, so it has equation

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0.$$

Such an equation could be reducible (we don't allow that here), in which case it is the product of two lines, and we have essentially seen this case in the previous section. We will also assume that it is not degenerate, that is, there are infinitely many points on the curve (we want to eliminate cases like the empty circle, or the circle reduced to just one point). When it is not reducible, then no 3 points on the curve lie on a line. This is a consequence of Bezout's theorem, but we give here a simple proof.

Lemma 0.1. *Let $\mathcal{C} : Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ be a plane conic such that there exists 3 different points on it which lie on a line. Then $\mathcal{C}$ is reducible.*

Proof. By translating one of the three points to the origin, we can assume that the three points are $(0,0)$, (x_0, y_0) and (tx_0, ty_0) for $t \neq 0, 1$. This also means that $F = 0$, $Ax_0^2+Bx_0y_0+Cy_0^2+Dx_0+Ey_0 = 0$ and $t^2(Ax_0^2+Bx_0y_0+Cy_0^2)+t(Dx_0+Ey_0) = 0$, and in turn, $(t^2-t)(Dx_0+Ey_0) = 0$. Since $t^2-t \neq 0$, this means that $Dx_0+Ey_0 = 0$, and also $Ax_0^2 + Bx_0y_0 + Cy_0^2 = 0$. It is then easy to see that any point of the form (sx_0, sy_0) is on the curve, that is, a line of the form $\alpha x + \beta y = 0$ is included in the curve. We can assume that $\alpha \neq 0$. Then as polynomials in the variable x, write

$$Ax^2 + Bxy + Cy^2 + Dx + Ey = (\alpha x + \beta y)Q(x, y) + R(y)$$

where $Q(x, y)$ is a polynomial in two variables, while $R(y)$ is a polynomial in just y (actually, a polynomial in two variables, but the euclidian division assures us that the degree in x is less or equal to 0). Then, for any y, let $x = -\frac{\beta}{\alpha}y$. It is a point on the line, thus on the curve, which means that $R(y) = 0$ for all y, and therefore R is zero, and we have proved that

$$Ax^2 + Bxy + Cy^2 + Dx + Ey = (\alpha x + \beta y)Q(x, y),$$

hence the curve is reducible. □

From now on, we assume that we are given an irreducible non-degenerate conic of the form $\mathcal{C} : Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$. Then the curve is entirely defined by 5 distinct points. Namely, we have the following lemma:

Lemma 0.2. *Given 5 distinct points on the plane, with the property that no 3 of them lie on a line, then there exists a unique conic that passes through those points.*

Proof. We are given the points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3)$, $P_4 = (x_4, y_4)$, and $P_5 = (x_5, y_5)$. By a translation, we may assume that $P_1 = (0, 0)$. Since P_1, P_2 and P_3 do not lie on a line, the quantity $x_3y_2 - x_2y_3 \neq 0$, and we can define $\alpha = \frac{-y_3}{x_3y_2-x_2y_3}$, $\beta = \frac{x_3}{x_3y_2-x_2y_3}$, $\gamma = \frac{y_2}{x_3y_2-x_2y_3}$ and $\delta = \frac{-x_2}{x_3y_2-x_2y_3}$, and consider the change of variables $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$. This is really a change of variables, since $\alpha\delta - \beta\gamma = -1 \neq 0$. Moreover, since the change of variables is linear, conics are transformed to conics, and lines into lines. Finally, this change of variables lets P_1 unchanged, and sends the points P_2 and P_3 to $(1, 0)$ and $(0, 1)$ respectively. So we might assume that the five given points are $P_1 = (0, 0)$, $P_2 = (1, 0)$, $P_3 = (0, 1)$, $P_4 = (x_4, y_4)$, and $P_5 = (x_5, y_5)$.

We have to find coefficients A, B, C, D, E, F that satisfy

$$\begin{aligned} F &= 0 \\ A + D + F &= 0 \\ C + E + F &= 0 \\ Ax_4^2 + Bx_4y_4 + Cy_4^2 + Dx_4 + Ey_4 + F &= 0 \\ Ax_5^2 + Bx_5y_5 + Cy_5^2 + Dx_5 + Ey_5 + F &= 0 \end{aligned}$$

This systems reduces to

$$\begin{aligned} A(x_4^2 - x_4) + Bx_4y_4 &= -C(y_4^2 - y_4) \\ A(x_5^2 - x_5) + Bx_5y_5 &= -C(y_5^2 - y_5) \end{aligned}$$

The determinant of the system is

$$(x_4^2 - x_4)x_5y_5 - (x_5^2 - x_5)x_4y_4 = x_4x_5\left(y_5(x_4 - 1) - y_4(x_5 - 1)\right).$$

This can't be 0, since it would then mean $x_4 = 0$, or $x_5 = 0$ or $y_5(x_4 - 1) - y_4(x_5 - 1) = 0$. But the first case is the same as saying that the points P_1, P_3, P_4 lie on the same line, the second, that the points P_1, P_3, P_5 lie on the same line, while the third that the points P_2, P_4, P_5 lie on the same line, namely the line $Y = \frac{y_4}{x_4 - 1}(X - 1)$ (or $Y = \frac{y_5}{x_5 - 1}(X - 1)$ if $x_4 = 1$.) Then all the solutions are

$$\begin{aligned} A &= \frac{x_4y_4(y_5^2 - y_5) - x_5y_5(y_4^2 - y_4)}{(x_4^2 - x_4)x_5y_5 - (x_5^2 - x_5)x_4y_4}C \\ B &= \frac{(x_5^2 - x_5)(y_4^2 - y_4) - (x_4^2 - x_4)(y_5^2 - y_5)}{(x_4^2 - x_4)x_5y_5 - (x_5^2 - x_5)x_4y_4}C \end{aligned}$$

We see that $C = 0$ leads $A = B = C = D = E = F = 0$ which is absurd. Then $C \neq 0$, and dividing the equation of the conic by C, we can assume that $C = 1$, and we have just proved that there exists a unique conic that passes through the 5 points. □

We will now prove the following:

Theorem 1. *Let $\mathcal{C} : Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ be a non-degenerate conic. If the curve has at least 5 distinct rational points on it, then there are infinitely many rational points on it, and they are dense on the curve.*

Proof. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3)$, $P_4 = (x_4, y_4)$, and $P_5 = (x_5, y_5)$ be the 5 rational points. Since it is a conic, one of the coefficients A, B, C is not zero, say A, and we may therefore assume that $A = 1$. Then we have to solve the system

$$\begin{aligned} Bx_1y_1 + Cy_1^2 + Dx_1 + Ey_1 + F &= -x_1^2 \\ Bx_2y_2 + Cy_2^2 + Dx_2 + Ey_2 + F &= -x_2^2 \\ Bx_3y_3 + Cy_3^2 + Dx_3 + Ey_3 + F &= -x_3^2 \\ Bx_4y_4 + Cy_4^2 + Dx_4 + Ey_4 + F &= -x_4^2 \\ Bx_5y_5 + Cy_5^2 + Dx_5 + Ey_5 + F &= -x_5^2 \end{aligned}$$

From the lemma, we know that this system has a unique solution, and since the coefficients are rationals, then B, C, D, E, F have to be rational too.
If we have a rational point $P = (x, y)$ on the conic, with $x \neq x_1$ (which is always the case except for at most 2 points), then the slope of the line passing through P_1 and P is rational of course, being equal to $\frac{y-x_1}{x-x_1}$. This gives a map between rational points on $\mathcal{C}$ except at most 2 points, and rational numbers. We show now that this map has an inverse, namely, take a (almost any) rational number t, and consider the line $\mathcal{L}_t$ passing through the point P_1, and with slope t. Then this line will cross $\mathcal{C}$ in another rational point. This will show that the number of rational points on the conic is infinite, but we will have to work a bit more to prove density.
The line $\mathcal{L}_t$ has equation

$$\mathcal{L}_t : y = tx + (y_1 - tx_1).$$

We replace y in the equation of $\mathcal{C}$ by this expression to find the x-coordinate of the intersection points. This gives us

$$\begin{aligned}\left(A + Bt + Ct^2\right) x^2 + \left(By_1 - Btx_1 + 2Cty_1 - 2Ct^2x_1 + D + Et\right) x \\ + \left(Cy_1^2 + Ct^2x_1^2 - 2Cty_1x_1 + Ey_1 - Etx_1 + F\right) \quad = \quad 0\end{aligned}$$

If $A + Bt + Ct^2 = 0$, then we just have one intersection point, namely P_1, but this happens for at most 2 values of t. But if $A + Bt + Ct^2 \neq 0$, we know that this equation has two solutions. We know one of them, namely x_1, and the other, say α verifies

$$\begin{aligned}-x_1 - \alpha &= \frac{By_1 - Btx_1 + 2Cty_1 - 2Ct^2x_1 + D + Et}{A + Bt + Ct^2} \\ x_1\alpha &= \frac{Cy_1^2 + Ct^2x_1^2 - 2Cty_1x_1 + Ey_1 - Etx_1 + F}{A + Bt + Ct^2}\end{aligned}$$

This shows that the other intersection point is $P = (\alpha, \beta)$ with

$$\alpha = -x_1 - \frac{By_1 - Btx_1 + 2Cty_1 - 2Ct^2x_1 + D + Et}{A + Bt + Ct^2}$$

and

$$\beta = t\alpha + y_1 - tx_1.$$

The good thing is that since we assume that $t, x_1, y_1 \in \mathbb{Q}$, and we have proved that $A, B, C, D, E, F \in \mathbb{Q}$, then necessarily P is a rational point. It is not difficult to show that the two maps are inverse of each other, so that we have a bijection between the set

$$\mathcal{C}(\mathbb{Q}) - \{(x, y) | x = x_1\}$$

and the set

$$\mathbb{Q} - \left\{t | A + Bt + Ct^2 = 0\right\}.$$

Since the second one is infinite, the first one has to be infinite too, and there are infinitely many rational points on $\mathcal{C}$. As for density, since the map going from the second set to the first set is obviously continuous, density of the rational numbers in $\mathbb{R}$ implies that $\mathcal{C}(\mathbb{Q})$ is dense in $\mathcal{C}(\mathbb{R})$. □

Corollary 1.1. *There are infinitely many Pythagorean triples.*

Proof. The circle $x^2+y^2=1$ has at least 5 rationals points, namely $(1,0)$, $(-1,0)$, $(0,1)$, $(0,-1)$ and $(\frac{3}{5},\frac{4}{5})$, the last one coming from the Pythagorean triple $(3,4,5)$. We know therefore that there are infinitely many rational points on this circle. Now, given any such rational point, of the form $(\frac{a}{c},\frac{b}{c})$, with a,b,c positive, and relatively prime, then $a^2+b^2=c^2$, that is (a,b,c) is a Pythagorean triple, and there are therefore infinitely many. □

A natural question to ask is: what happens with less than 5 points? The answer is: there exists conics with exactly 0, 1, 2, 3 or 4 rational points. We shall give an example of each of them.

Consider the circle $\mathcal{C}_0 : (x-\sqrt{2})^2+y^2=1$. If we expand this expression, we get $-2x\sqrt{2}+(x^2+1+y^2)=0$. If (x,y) is a rational point on the circle with $x\neq 0$, then $\sqrt{2}=\frac{x^2+y^2+1}{2x}\in\mathbb{Q}$ which is absurd. Then x has to be 0, but then $y^2=-1$ which is also absurd. Thus the circle $\mathcal{C}_0$ has no rational point.

Consider now the circle $\mathcal{C}_1 : (x-\sqrt{2})^2+y^2=2$. As we just did, we still can show that if (x,y) is a rational point on $\mathcal{C}_1$, then necessarily $x=0$. But this time, if $x=0$, there is a rational solution for y, namely, $y=0$, and so $\mathcal{C}_1$ has exactly one rational point, $(0,0)$.

Consider now the circle $\mathcal{C}_2 : (x-\sqrt{2})^2+y^2=3$. Again, there are no rational point (x,y) on the curve with $x\neq 0$. But when $x=0$, we easily find two rational points, namely $(0,1)$ and $(0,-1)$, which are therefore the only two rational points on $\mathcal{C}_2$.

If we want to have examples of conics with exactly 3 or 4 rational points, then we have to move away from circles. The reason is that with 3 rational points on a circle, then the center is also rational (as the intersection of the midperpendiculars), the square of the radius also is, and this shows that the coefficients of the conic can all be chosen rational, and we can continue the proof of the theorem from here.

Consider then the ellipse $\mathcal{C}_3 : x^2+(\sqrt{2}+1)y^2+\sqrt{2}y=0$. Since $\sqrt{2}$ is not rational, the only way to satisfy this equation with $x,y\in\mathbb{Q}$ is when $y^2-y=0$. But if $y=0$, then $x=0$, while if $y=1$, then $x=\pm 1$, which shows that there are exactly 3 rational points on $\mathcal{C}_3$, namely $(0,0)$, $(1,-1)$ and $(1,1)$.

Consider finally the ellipse $\mathcal{C}_4 : x^2+(\sqrt{2}-1)y^2=\sqrt{2}$. Since $\sqrt{2}$ is not rational, the only way to satisfy the equation with $x,y\in\mathbb{Q}$ is when $y^2=1$, and then in turn, $x^2=1$. This gives that there are exactly 4 rational points on $\mathcal{C}_4$, namely $(1,1)$, $(-1,1)$, $(1,-1)$ and $(-1,-1)$.

Density of rational points on irreducible smooth cubics

We will now look at the case of plane curves of degree 3, that is, cubics.

Essentially, we needed 2 distinct points to define a line, 5 to define a conic, and here, since we have 10 coefficients, 9 points should be sufficient to define a cubic. In the case of lines anc conics, 2 and 5 rational points implied an infinity of such points, and moreover, those points were dense on the curve. Can we expect that 9

rational points on a cubic curve implies infinity and density of such points? The answer is no. Take for example the elliptic curve

$$y^2 + 17xy - 120y = x^3 - 60x^2.$$

This curve has exactly 15 rational points (16 if we work in the projective plane): $(0,0)$, $(60,-900)$, $(-30,180)$, $(24,-144)$, $(-30,450)$, $(60,0)$, $(0,120)$, $(-12,288)$, $(240,1800)$, $(\frac{15}{4},\frac{225}{8})$, $(240,-5760)$, $(-12,36)$, $(30,-300)$, $(-40,400)$ and $(30,-90)$. This comes from theorems of Mordell (this curve over $\mathbb{Q}$ is of rank 0 as an abelian group), and Nagell-Lutz (that describe the rational points of finite order). Actually, Mazur proved in [2] that the structure of the torsion subgroup of the rational points on an elliptic curve is one of few types. As a consequence, if an elliptic curve has 17 rational points, it has infinitely many.

The previous example also shows that even if the coefficients are rationals and there exists a rational point, then there might be just a finite number of rational points, and of course density is even further away. The method that we used for conics doesn't work any longer. Of course, given a fixed rational point P_1, then (almost) any other rational point P on the curve defines a line $\mathcal{L}$ through P and P_1 with rational slope, as for the conics, and we have therefore a well defined map

$$\begin{array}{ccc} \mathcal{C}(\mathbb{Q}) - \{\text{few points}\} & \longrightarrow & \mathbb{Q} \\ P & \mapsto & \text{slope of } (PP_1) \end{array}$$

But, contrary to the conics, this map has no inverse: given $t \in \mathbb{Q}$, we can of course define the line $\mathcal{L}_t$ going through P_1 and slope t. This line intersects $\mathcal{C}$ at least in P_1. For the conics, we found exactly one other rational intersection point, found by solving a rational polynomial of second degree with a rational root. Here, we can't guarantee anything. We get indeed a rational polynomial of degree 3, with a rational root. The polynomial might have no other real root (the line has no intersection point other than P_1), or two real roots (the line intersects the cubic in two other points), but these roots are generally not rational.

What happens if we have an infinity of rational points? Are they then dense on the curve? The answer is again no, as an example will later show.

Irreducible smooth cubic with a rational point have another name, elliptic curves (by smooth, we mean also smooth at infinity). It can be shown that by a change of variables, they have a particular form. As mentionned earlier, the "right" way to study these curves is to define them over the projective plane. As we will work in different affine charts, we give the general definition. We refer to [4] for the theory on elliptic curves.

Definition 1. *An elliptic curve E over a field $\mathbb{K}$ of characteristic zero is a curve in $\mathbb{P}^2(\mathbb{K})$ given by an equation*

$$E : Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$$

with $-4a_4^3 - 27a_6^2 \neq 0$.

One point here is "special", the only point not lying in the affine plane $Z = 1$, namely the point $\mathcal{O} = [0, 1, 0]$, usually called the point at infinity. Given a field $\mathbb{K}$, define

$$E(\mathbb{K}) = \left\{ P = [x, y, z] \in \mathbb{P}^2(\mathbb{K}), y^2 z = x^3 + a_4 x z^2 + a_6 z^3 \right\}.$$

We can define an abelian group structure on the set $E(\mathbb{R})$: given two points P, Q, draw a line (PQ) (or the tangent to the curve if $P = Q$). This line intersects $E(\mathbb{R})$ in exactly a third point R. Then draw a line $(\mathcal{O}R)$ (or the tangent if $\mathcal{O} = R$). This line intersects $E(\mathbb{Q})$ in a third point S. Then define $P + Q = S$. The group law is infinitely differentiable. Moreover, if $P, Q \in E(\mathbb{Q})$, then $P + Q \in E(\mathbb{Q})$ too, which makes $E(\mathbb{Q})$ a subgroup of $E(\mathbb{R})$. Finally, since $\mathbb{P}^2(\mathbb{R})$ is compact, and $E(\mathbb{R})$ is closed in $\mathbb{P}^2(\mathbb{R})$, then $E(\mathbb{R})$ is compact too.

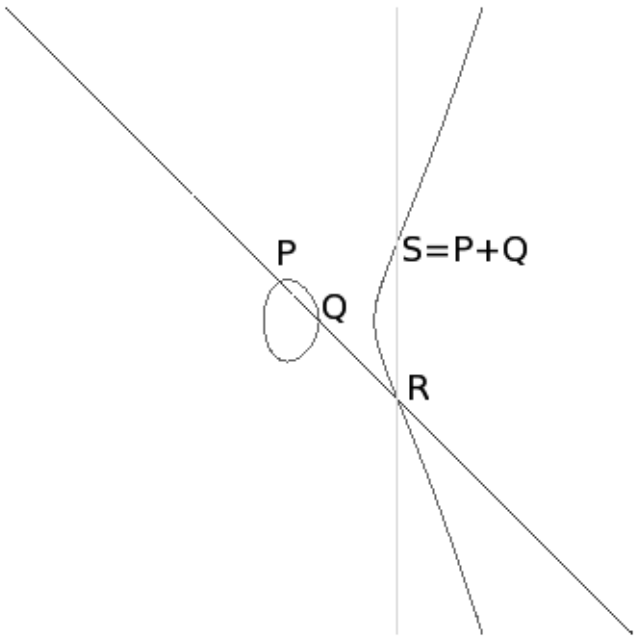

Figure 1: Addition in the affine plane

There are two types of elliptic curves defined over $\mathbb{R}$: $E(\mathbb{R})$ has either 1 or 2 connected components, depending on the number of real roots of $X^3 + a_4 X + a_6$ (or equivalently, the number of points of order 2).

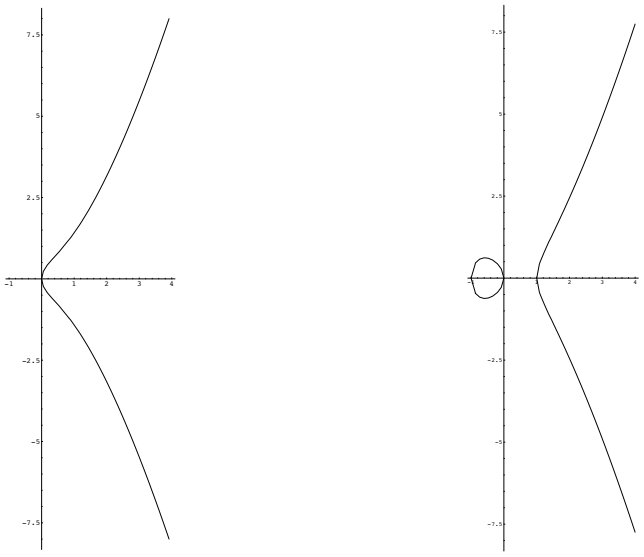

Figure 2: $E : y^2 = x^3 + x$ and $E : y^2 = x^3 - x$ with one and two components

We shall denote by $E(\mathbb{R})_{\mathcal{O}}$ the component that contains the point at infinity, called the identity component. We shall now prove the following:

Theorem 2. *Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve over $\mathbb{Q}$ with an infinite number of rational points. Then $E(\mathbb{Q}) \cap E(\mathbb{R})_{\mathcal{O}}$ is dense in $E(\mathbb{R})_{\mathcal{O}}$. Moreover, in the case of a second connected component, then $E(\mathbb{Q})$ is dense in $E(\mathbb{R})$ if and only if there exists a rational point on it.*

We shall need a few lemmas to prove this result.

Lemma 2.1. *Let V be any open neighborhood of $\mathcal{O}$. Then there exists an open neighborhood W of $\mathcal{O}$ shuch that for all $P, Q \in W$, $-P \in W$ and $P + Q \in V$.*

Proof. Since we are interested in what happens round $\mathcal{O}$, we will work in the affine plane $Y = 1$. There, the curve has equation

$$E : z = x^3 + a_4xz^2 + a_6z^3$$

and $\mathcal{O} = (0, 0)$. Note that we have $-(x, z) = (-x, -z)$. Let $f(x, z) = x^3 + a_4xz^2 + z^3 - z$. We have

$$\frac{\partial f}{\partial z} = 2a_4xz + 3a_6z^2 - 1,$$

and therefore $\frac{\partial f}{\partial z}(0, 0) = -1 \neq 0$. By the theorem of implicit functions, there exists $a > 0$ and $g : (-a, a) \longrightarrow \mathbb{R}$ infinitely differentiable such that

$$\{(x, z), f(x, z) = 0\} \cap (-a, a) \times \mathbb{R} = \{(x, g(x)), x \in (-a, a)\}.$$

Note that g is an odd function. Let V' be the image of V in the affine plane $Y = 1$, and

$$V'' = \{x, \exists z \in \mathbb{R}, (x, z) \in V'\}.$$

This is an open set of $\mathbb{R}$ containing 0, so we can find $b > 0$ such that $[-b, b] \subset V'' \cap (-a, a)$. Consider the function

$$\begin{array}{rccc} \varphi: & [-b,b]^2 & \longrightarrow & \mathbb{R} \\ & (x_1, x_2) & \longmapsto & x\left((x_1, g(x_1)) + (x_2, g(x_2))\right) \end{array}$$

where $+$ is addition of points on the curve, and $x(P)$ denotes the x-coordinate of P. This function is infinitely differentiable. In particular, on the compact $[-b, b]^2$, there exists $k_b > 0$ such that

$$|\varphi(x_1, x_2)| \leqslant k_b ||(x_1, x_2)||, \ \forall x_1, x_2 \in [-b, b].$$

Take $c = \frac{b}{k_b\sqrt{2}}$. Then

$$\forall x_1, x_2 \in (-c, c), \ |\varphi(x_1, x_2)| \leqslant k_b\sqrt{x_1^2 + x_2^2} \leqslant \sqrt{2} k_b c = b.$$

Take now $W = \{(x, g(x)), \ x \in (-c, c)\}$. □

Lemma 2.2. *Let V be any open neighborhood of $\mathcal{O}$. Then $E(\mathbb{Q}) \cap V$ is infinite.*

Proof. Let W be the open neighborhood from the previous lemma. For $P \in E(\mathbb{R})$, let

$$W_P = \{P + Q, \ Q \in W\}$$

which is an open neighborhood of P since the group law and inverse are continuous. We obviously have

$$E(\mathbb{R}) = \bigcup_{P \in E(\mathbb{R})} W_P.$$

Since $E(\mathbb{R})$ is compact, there exists a finite number of points $P_1, \cdots, P_n$ such that

$$E(\mathbb{R}) = \bigcup_{i=1}^{n} W_{P_i}.$$

Since $E(\mathbb{Q})$ is infinite, there exists a point, say P_1, such that $W_{P_1} \cap E(\mathbb{Q})$ is infinite. Fix $Q \in W_{P_1} \cap E(\mathbb{Q})$ and consider

$$\begin{array}{rccc} \theta_Q: & W_{P_i} \cap E(\mathbb{Q}) & \longrightarrow & V \cap E(\mathbb{Q}) \\ & R & \longmapsto & R - Q \end{array}.$$

This is well defined: let $R \in W_{P_1} \cap E(\mathbb{Q})$. Since $E(\mathbb{Q})$ is a group, then $\theta_Q(R) = R - Q \in E(\mathbb{Q})$. There exists $\tilde{Q}, \tilde{R} \in W$ such that $Q = P_1 + \tilde{Q}$ and $R = P_1 + \tilde{R}$. Then $\theta(R) = R - Q = \tilde{R} - \tilde{Q}$ which is in V by definition of W. θ_Q is of course injective, which shows that $V \cap E(\mathbb{Q})$ is infinite. □

Lemma 2.3. *The differential $\frac{dx}{1 - 2a_4xz - 3a_6z^2}$ is invariant, meaning that if $Q \in E(\mathbb{R})$ is fixed and $P = (x_P, y_P) \in E(\mathbb{R})$ is variable, then*

$$\frac{dx_{P+Q}}{1 - 2a_4x_{P+Q}z_{P+Q} - 3a_6z_{P+Q}^2} = \frac{dx_P}{1 - 2a_4x_Pz_P - 3a_6z_P^2}.$$

Proof. See [4, Proposition III.5.1], which gives an "elegant" proof, and a hint for a straightforward but messy proof. □

Lemma 2.4. *There exists open neighborhoods V and U of $\mathcal{O}$ and 0 respectively, and a homeomorphism $L : V \longrightarrow U$ such that if W is the neighborhood of lemma 2.1, then*

$$\forall P, Q \in W,\ L(P+Q) = L(P) + L(Q).$$

Proof. Let a, g be as in the proof of lemma 2.1, and $V = \{(x, g(x)), x \in (-a, a)\}$ which is an open neighborhood of $\mathcal{O}$. Since $g(0) = 0$, reducing a if necessary, we may assume that $1 - 2a_4 x g(x) - 3a_6 g(x)^2 > \epsilon$ for $1 > \epsilon > 0$ on $(-a, a)$, so that the integral

$$M(t) = \int_0^t \frac{dx}{1 - 2a_4 x g(x) - 3a_6 g(x)^2},\ t \in (-a, a)$$

is well defined. Define

$$M : \begin{array}{ccc} V & \longrightarrow & \mathbb{R} \\ P & \longmapsto & M(x_P) \end{array}.$$

Then, for P, Q in W, we know that $P + Q \in V$. Moreover, we define

$$\begin{aligned} L(Q) &= \int_0^{x_Q} \frac{dx_R}{1 - 2a_4 x_R g(x_R) - 3a_6 g(x_R)^2} \\ &= \int_{x_P}^{x_{P+Q}} \frac{dx_{P+R}}{1 - 2a_4 x_{P+R} z_{P+R} - 3a_6 z_{P+R}^2} \end{aligned}$$

which in turns gives

$$L(P) + L(Q) = \int_0^{x_{P+Q}} \frac{dx}{1 - 2a_4 x g(x) - 3a_6 g(x)^2} = L(P+Q).$$

M is obviously infinitely differentiable, and since $M'(0) = 1$, reducing the open neighborhood if necessary, we can assume that M (and therefore L) is an homeomorphism from V onto its image. □

Lemma 2.5. *Let L, V, U, W from the previous lemma and let $G = L(E(\mathbb{Q}) \cap W) \subset L(W)$. Then $\overline{G} = L(W)$.*

Proof. Let $x \in L(W)$. Assume that $x \geqslant 0$ for simplicity. Let $\epsilon > 0$ small enough so that $\{y \in U, |y - x| < \epsilon\} \subset L(W)$. We shall show that $\{y \in G, |x - y| < \epsilon\} \neq \emptyset$. The set $L^{-1}((-\epsilon, \epsilon))$ is an open neighborhood of $\mathcal{O}$, and has therefore an infinite number of rational points from lemma 2.2. Let $P \neq \mathcal{O}$ be one of them, and taking $-P$ if necessary, we may assume that $x(P) > 0$. Let $\xi = L(P)$. Then $0 < \xi < \epsilon$. Write $x = n\xi + \rho$ with $n \in \mathbb{N}$ and $0 \leqslant \rho < \xi$. We show by induction that $nP \in W \cap E(\mathbb{Q})$ and $n\xi = L(nP) \in G$. This is true for $n = 1$. Assume that it is true for $n - 1$. Then $(n-1)P, P \in W \cap E(\mathbb{Q})$, so that $nP = (n-1)P + P \in V \cap E(\mathbb{Q})$, and $n\xi = (n-1)\xi + \xi = L((n-1)P) + L(P) = L(nP)$. Now, $|L(nP) - x| = \rho < \epsilon$, which means that nP is acually in W since L is an homeomorphism. That shows that $n\xi \in G$. □

We can now prove the theorem:

Proof. The set $\overline{E(\mathbb{Q}) \cap E(\mathbb{R})_{\mathcal{O}}}$ is by definition closed in $E(\mathbb{R})$. By the last lemma, there exists an open O such that $\mathcal{O} \in O \subset \overline{E(\mathbb{Q}) \cap E(\mathbb{R})_{\mathcal{O}}}$. Then, for any point $P \in \overline{E(\mathbb{Q}) \cap E(\mathbb{R})_{\mathcal{O}}}$, $P \in O_P \subset \overline{E(\mathbb{Q}) \cap E(\mathbb{R})_{\mathcal{O}}}$, which shows that $\overline{E(\mathbb{Q}) \cap E(\mathbb{R})_{\mathcal{O}}}$ is also open in $E(\mathbb{R})$. Since it is obviously a subset of $E(\mathbb{R})_{\mathcal{O}}$ which is a connected component of $E(\mathbb{R})$, we have proved the first part of the theorem.
If there exists a second component with a rational point Q on it, then we have an homeomorphism

$$\begin{array}{ccc} E(\mathbb{R})_{\mathcal{O}} & \longrightarrow & E(\mathbb{R})_Q \\ Q & \longmapsto & P+Q \end{array}$$

which shows that $E(\mathbb{Q}) \cap E(\mathbb{R})_Q$ is dense in $E(\mathbb{R})_Q$, and therefore $E(\mathbb{Q})$ dense in $E(\mathbb{R})$. □

Remark. *We never used the fact that the points were in $E(\mathbb{Q})$. The only thing we used was that it was a group with an infinite number of points. We actually proved that any infinite subgroup of $E(\mathbb{R})$ is dense in the identity component. This result is well known and an immediate consequence of standards results on infinite subgroups of $E(\mathbb{R}) = \mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

As promised earlier, here is an example of a curve with an infinite number of rational points, but those are not dense on the curve (by the theorem, we know that they are dense in the compenent of the point of infinity though). Consider the curve $E : y^2 = x^3 - 47088x - 2522880$ in the affine plane. An application of the Mordell-Weil theorem tells us that the group $E(\mathbb{Q})$ is generated by 2 points, namely $P_1 = (240, 0)$ which is a point of order 2, and $P_2 = (8304/25, 537408/125)$ which is a point of infinite order. Both of them lie on the connected component of $\mathcal{O}$. And there are no rational point on the other component. Namely, if P, Q are on the identity component, then $P + Q$ is there too. By symmetry, $-Q$ is there, and we have a continuous map

$$\lambda_Q : \begin{array}{ccc} E(\mathbb{R})_{\mathcal{O}} & \longrightarrow & E(\mathbb{R}) \\ R & \longmapsto & R+Q \end{array}$$

such that $\lambda_Q(-Q) = \mathcal{O}$ and $\lambda_Q(P) = P + Q$. That means that both $\mathcal{O}$ and $P + Q$ are on the same component. Since both generators are on this component, all the rational points have to be. The next figure plots nP_2 for $n \in [1, 1000]$ (the big dots) and the curve itself.

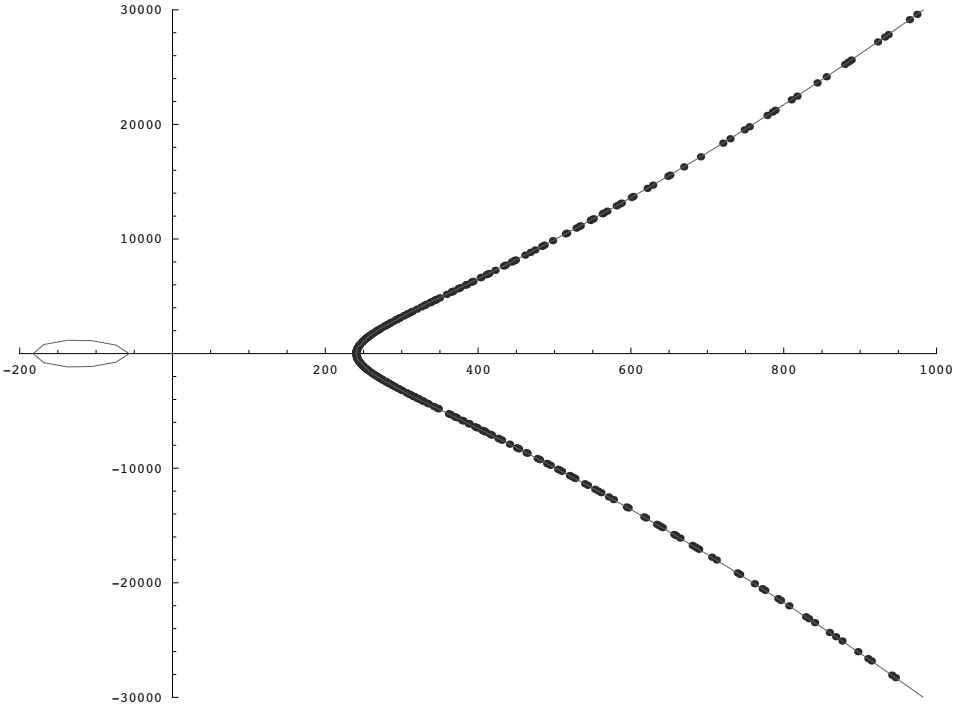

Figure 3: nP_2, $1 \leqslant n \leqslant 1000$, and $E(\mathbb{R})$

Density of rational points on curves of higher degree

We won't try to prove anything in this section, as this is far beyond the scope of this article. We mention that in 1983, G. Faltings [1] proved that on these curves, the number of rational points is finite.

References

[1] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), 349–366; Erratum ibid. **75** (1984), 381.

[2] B. Mazur, *Modular curves and the Eisenstein ideal.* IHES Pub. Math. **47** (1977), 33–186.

[3] B. Mazur, *The topology of rational points.* Exp. Math. **1**, No.1, 35–45, 1992.

[4] J.H. Silverman, *The arithmetic of elliptic curves.* Number 106 in Graduate texts in mathematics, Springer-Verlag, New York, 1986.

[5] J. H. Silverman, and J. Tate, *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992