13.2.1 Definition of elliptic curves

An Elliptic Curve (EC) is the set of solutions (x, y) of an equation of the form $y^2 = x^3 + ax + b$, where a and b are real coefficients. See Figure 13.2.2 below for graphs of some elliptic curves. Additionally, ECs are not allowed to have double or triple roots in the variable x. A triple root produces a cusp in the graph, and a double root produces a self-intersection (see graphs in Figure 13.2.3). See graphs in Figure 13.2.3 for examples of elliptic curves with double and triple roots. It turns out that we can guarantee that the EC has no double or triple roots if the coefficients a and b satisfy the following equation: $4a^3 + 27b^2 \neq 0$.

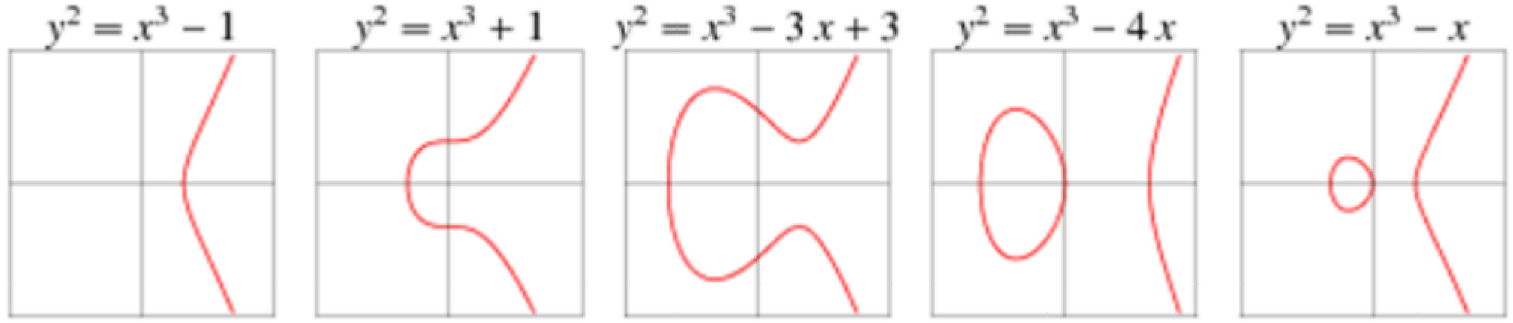


Figure 13.2.2. Geometric shapes of elliptic curves, (from reference (15))

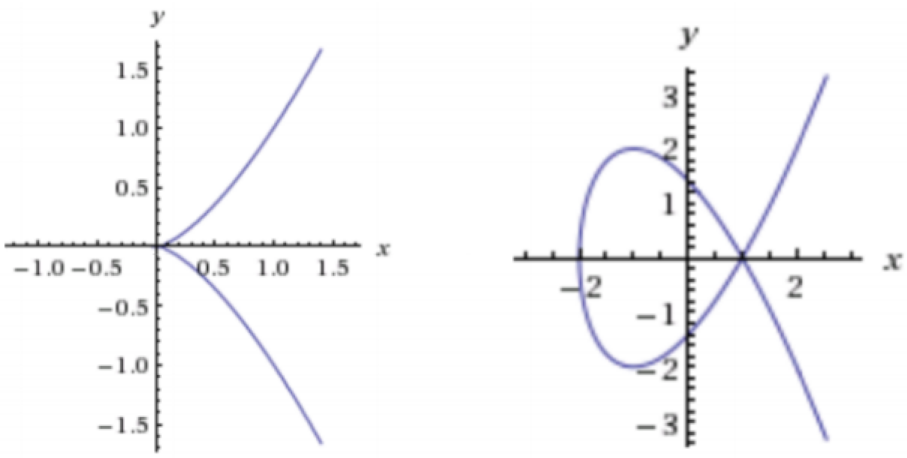


Figure 13.2.3. (Left) E: $y^2 = x^3$ and (Right) E: $y^2 = x^3 - 3x + 2$, (From reference (7)

Exercise 13.2.2.

(a) Prove that if the equation $y^2 = x^3 + ax + b$ has a double or triple root, then $4a^3 + 27b^2 = 0$. (*Hint*)

(b) Prove the converse to part (a), that is show that if $4a^3 + 27b^2 = 0$, then the equation has a double or triple root. (*Hint*)

证明：(a) 如果有 double root，那么 x^3+ax+b 可写作 $(x-r_1)^2(x-r_2)$，展开可知 x^2的系数，让其$=0$即可。 (b) 易证。

Exercise 13.2.2 (a): If there is a double root , then it must be that $0 = x^3 + ax + b$ has a double root. This means that the equation can be factored: $x^3 + ax + b = (x - r_1)^2(x - r_2)$. Express a and b in terms of r_1 and r_2. (A similar approach can be used in the case of a triple root.)

Exercise 13.2.2 (b): There are 2 cases: (i) $b = 0$, (ii) $b \neq 0$. In the case $b \neq 0$, first, show that $a > 0$. Then use part (a) to express r_1 and r_2 in terms of a and b, and show the equation factors properly.

All of the cryptosystems that we have studied so far have been based on group operations associated with a particular group. For example, Diffie-Hellman used discrete exponentiation ? (which is repeated multiplication in $U(p)$) to construct a one-way function. In order to use elliptic curves to construct cryptosystems, we'll need to show that we can associate a group with each elliptic curve. In the following sections we'll define an arithmetic operation on the points of any elliptic curve, an show that this operation is in fact a group operation.

13.2.2 Elliptic curve arithmetic

In this section, we show how to do arithmetic on elliptic curves. Specifically, we define an operation (denoted by '+') which acts on two points of an elliptic curve, to give another point on the same curve.

Suppose that P_1 and P_2 are two points on an EC. We will consider first the case where $P_1 \neq P_2$: later we will consider the case where $P_1 = P_2$. Geometrically, if the two points are different then P_1+P_2 is given by drawing a line from point P_1 to point P_2 and continuing the line until it intersects the elliptic curve, then reflect that point about the x-axis. See Figure 13.2.4 for a geometric representation of the operation $P_1 + P_2$.

It turns out that $P_1 + P_2$ is always defined on the EC (except in one special case which we will explain a little bit later), even though sometimes the result of $P_1 + P_2$ is quite far away from both P_1 and P_2. For instance, take E: $y^2 = x^3 - x$, and points $P_1 = (2, \sqrt{6})$ and $P_2 = (3, -\sqrt{24})$. Then $P_1+P_2 = (49, 342.93)$ (we'll show this later in Example 13.2.6), as illustrated in Figure 13.2.5.

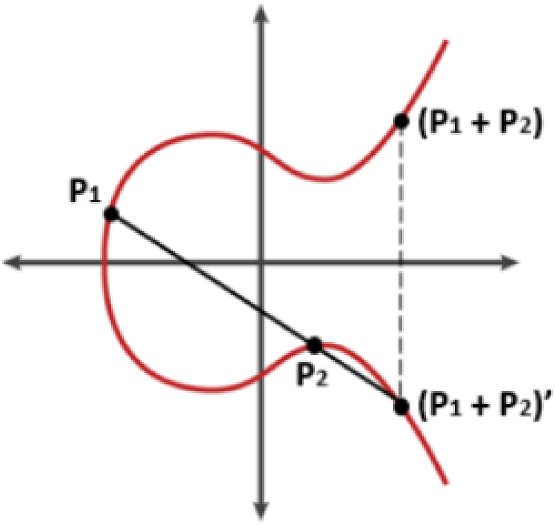


Figure 13.2.4. Adding two distinct points, $P_1 + P_2$ on the EC (from reference (9)).

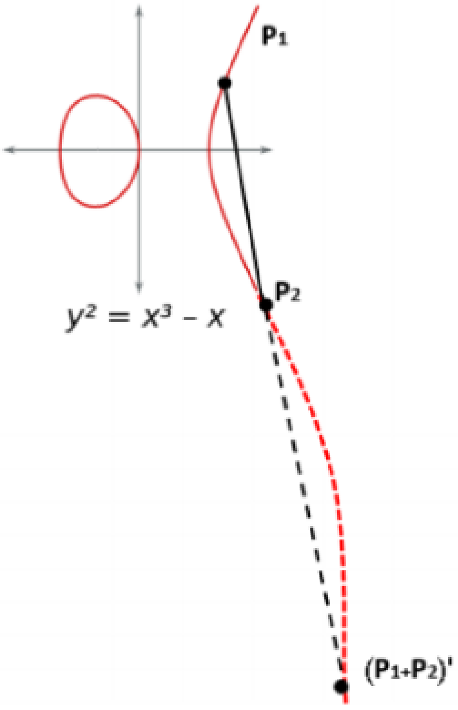


Figure 13.2.5. $P_1 + P_2$ is always defined on the EC (from reference (9)).

Example 13.2.3. Given E: $y^2 = x^3 + ax + b$, $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and $P_3 = (x_3, y_3)$. Find P_3, where $P_3 = P_1 + P_2$.

The steps of this calculation are as follows:

(a) Compute the slope of the line m through P_1 and P_2 as follows:

$$m = (y_2 - y_1) \cdot (x_2 - x_1)^{-1}, \text{for } P_1 \neq P_2$$

(b) Use the point-slope formula $y - y_1 = m(x - x_1)$ in order to find equation of the line that passes through the two points. Rewrite as:

$$y = m(x - x_1) + y_1$$

(c) It turns out that the sum of the roots is m^2 (see Exercise 13.2.4). So we have

高次韦达定理

$$x_1 + x_2 + x_3 = m^2, \text{ which implies } x_3 = m^2 - x_1 - x_2.$$

(d) The third point of intersection is $(x_3, -y_3)$. So we may plug x_3 into $(-y_3) = m(x_3 - x_1) + y_1$ to obtain y_3.

(e) Finished! $P_3 = (x_3, y_3)$.

$$P_3 = (x_3, y_3) = \left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2, \ \frac{(x_1-x_3)(y_2-y_1)}{x_2-x_1} + y_1\right)$$

Exercise 13.2.4. In part (c) of Example 13.2.3 we mentioned that $x_1 + x_2 + x_3 = m^2$, where x_1, x_2, x_3 are the x-coordinates of three intersections of the a with the EC and m is the slope of the line. In this exercise, we will prove this.

(a) Substitute the equation for y in (b) of Example 13.2.3 into equation E. The resulting equation can be rearranged to form a cubic equation in x of the form: $0 = x^3 + c_2x^2 + c_1x + c_0$, where c_0, c_1, c_2 depend on the parameters a, b, m, x_1, y_1. Express the coefficient c_2 in terms of these parameters.

(b) The cubic equation $0 = x^3 + c_2x^2 + c_1x + c_0$ has three roots, so the cubic equation can be factored: $x^3 + c_2x^2 + c_1x + c_0 = (x - x_1)(x - x_2)(x - x_3)$. Use this equality to express c_2 in terms of x_1, x_2, x_3.

(c) Based on your results in (a) and (b), show that $m^2 = x_1 + x_2 + x_3$.

Vieta's Theorem/Zero-coefficient Relationship

Assume $x_1, x_2, \ldots, x_n$ are the roots of the polynomial

$$P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

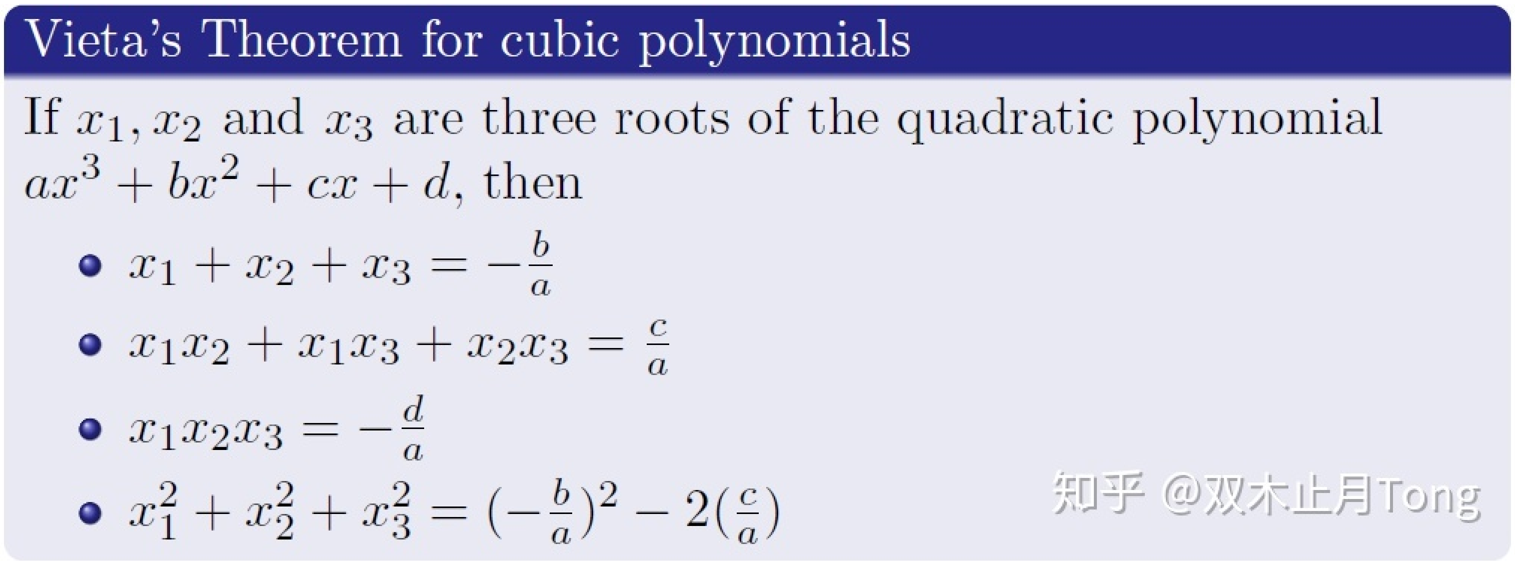
then

$$x_1 + x_2 + x_3 + \cdots + x_n = -\frac{a_{n-1}}{a_n},$$

$$x_1x_2 + x_1x_3 + \cdots + x_nx_{n-1} = \frac{a_{n-2}}{a_n},$$

$$\cdots,$$

$$x_1x_2x_3 \cdots x_n = (-1)^n \frac{a_0}{a_n}.$$



Vieta's Theorem for cubic polynomials

If x_1, x_2 and x_3 are three roots of the quadratic polynomial $ax^3 + bx^2 + cx + d$, then

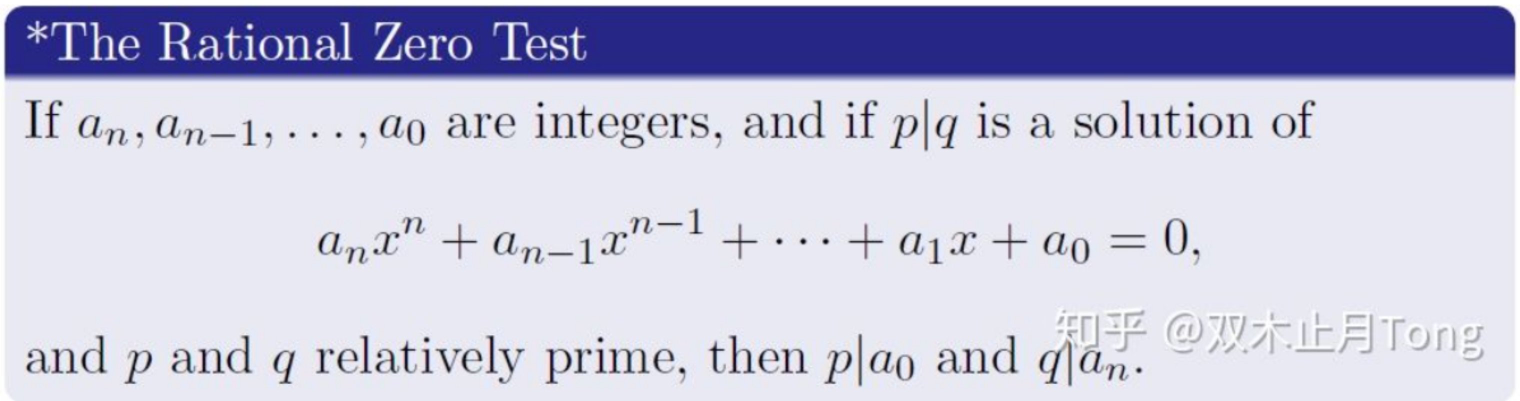
- $x_1 + x_2 + x_3 = -\frac{b}{a}$
- $x_1x_2 + x_1x_3 + x_2x_3 = \frac{c}{a}$
- $x_1x_2x_3 = -\frac{d}{a}$
- $x_1^2 + x_2^2 + x_3^2 = (-\frac{b}{a})^2 - 2(\frac{c}{a})$

(这些补充一些由此而得的推论:

（1）复数根都是成对出现的；

> 根据高次韦达定理，所有根的和、乘积等都是实数($a_i \in R$)，如果有复数根一定是与其共轭一起成对出现的， 即$a + bi$ 与 $a - bi$ 一起出现。
>
> 1. 那么告诉我们一个复数根，其实是告诉了我们方程的两个根；
>
> 2. 如果多项式的度(Degree of the Polynomials，多项式最高次)是奇数，那么一定存在实数根，因为复数根成对出现；

（2）试根法



*The Rational Zero Test

If $a_n, a_{n-1}, \dots, a_0$ are integers, and if $p|q$ is a solution of

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0,$$

and p and q relatively prime, then $p|a_0$ and $q|a_n$.

图：试根法

因为 $x_1x_2x_3\cdots x_n = (-1)^n\frac{a_0}{a_n}$ ，那么如果存在一个根 $\frac{p}{q}$,那么 p 是 a_0 的因子， q 是 a_n 的因子。)

Exercise 13.2.7. Given E: $y^2 = x^3 - 2x$, $P_1 = (2, 2)$, $P_2 = (-1, 1)$, find P_3, where $P_3 = P_1 + P_2$. ◊

解： $k = \frac{2-1}{2+1} = \frac{1}{3}$　∴ 直线方程： $y - 2 = \frac{1}{3}(x-2)$

∴ $x_1 + x_2 + x_3 = k^2 = \frac{1}{9}$

∴ $x_3 = \frac{1}{9} - 2 + 1 = -\frac{8}{9}$ ， $y_3 = -\frac{26}{27} + 2 = \frac{28}{27}$

∴ $P_3 \ (-\frac{8}{9}, -\frac{28}{27})$

If the two points are the same, $P_1 = P_2 = (x_1, y_1)$, then a tangent line to the point is drawn and the point of intersection to the EC is then reflected about the x-axis. This is often referred to as ***point doubling***. The slope for this line is,

$$\boxed{m = (3x_1^2 + a) \cdot (2y_1)^{-1},}$$

which may be found using implicit differentiation (note that a refers to the coefficient of x in the elliptic curve equation–see Example 13.2.3). See Figure 13.2.6 below for a geometrical representation of point doubling.

Exercise 13.2.9. Derive the equation for m by taking derivatives of both sides of equation E and solving for $\frac{dy}{dx}$. Show your steps. ◊

解： 隐函数求导。 设 $y^2 = x^3 + ax + b$

∴ $2yy' = 3x^2 + a$

∴ $\frac{dy}{dx} = (3x^2 + a)(2y)^{-1}$

∴ $k = (3x_1^2 + a)(2y_1)^{-1}$

In the case of point doubling, once m is found the expression for the x coordinate of the other intersection of the tangent line with the curve is:

$$x_3 = m^2 - x_1 - x_1$$

(this is because x_1 is a double root of the cubic expression which gives the x-coordinates of the intersections between the EC and the tangent line). Once we have x_3, then we may find y_3 as before:

$$-y_3 = m(x_3 - x_1) + y_1$$

and $2P_1$ is given by (x_3, y_3).

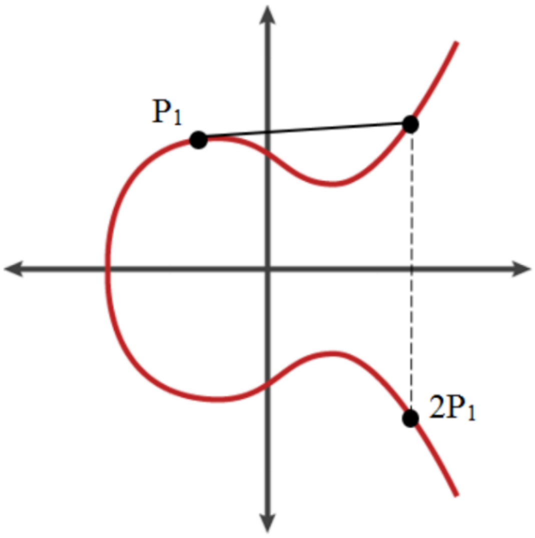


Figure 13.2.6. Point doubling on the EC (from reference (7)).

There is one scenario where addition of two points doesn't give a point on the curve. Given a point P, we define $-P$ as the reflection of P about the x axis: so if $P = (x, y)$, then $-P = (x, -y)$. The line through P and $-P$ is vertical, and does not intersect the curve at any other point. In order to make addition well-defined in this case we may create a notional ***point at infinity***. See Figure 13.2.7 below for a geometrical representation of the point at infinity. The point at infinity can be thought of as located at the point $(0, \infty)$, so that the line through any point (x, y) and the point at infinity is a vertical line with infinite slope. Additionally, the point at infinity is its own reflection, so we consider $(0, \infty)$ and $(0, -\infty)$ as a single point, which we denote by the symbol ∞. You may think of the y axis "wrapping around" so that when you keep moving in the +y direction eventually you wrap around to the -y axis.

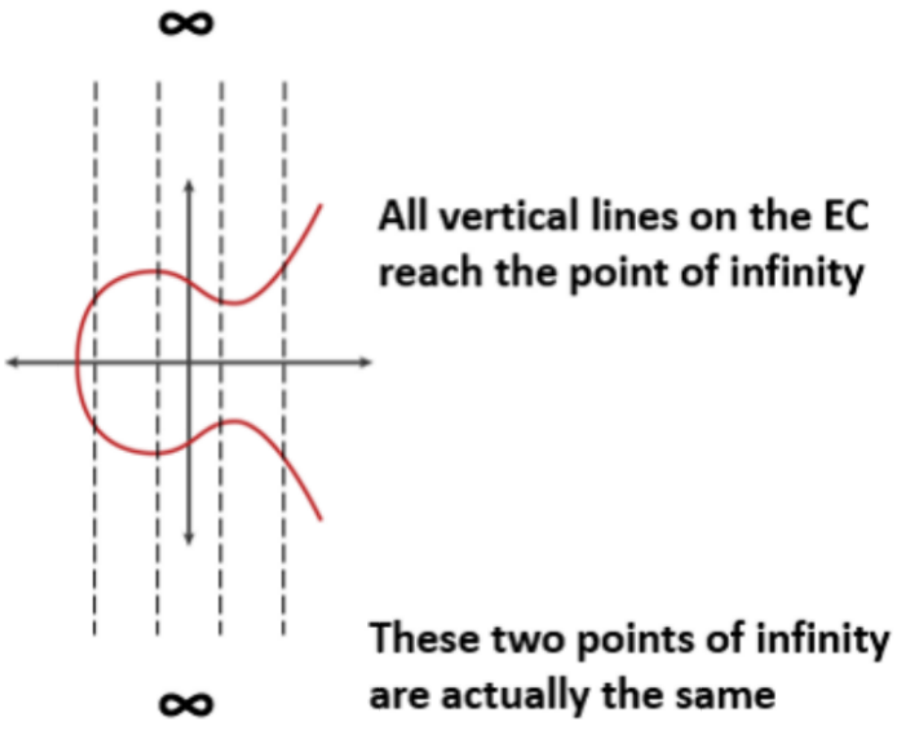

∞
All vertical lines on the EC reach the point of infinity
These two points of infinity are actually the same
∞

Figure 13.2.7. The point at infinity located at $(0, \infty)$ (from reference (9)).