Elliptic Curves Over $\mathbb{Q}$

Jordan Schettler

Department of Mathematics
University of Arizona

4/27/11

Outline

Normal Forms

Consider a general cubic equation in two variables x, y

$$\alpha x^3 + \beta x^2 y + \gamma xy^2 + \delta y^3 + \epsilon x^2 + \zeta xy + \eta y^2 + \theta x + \iota y + \kappa = 0$$

with rational coefficients $\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta, \iota, \kappa$.

Weierstraß Equations

The rational solutions (if there are any) are in bijection (up to a few exceptions) with the rational solutions of a cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with integer coefficients $a_1, \ldots, a_4, a_6$.

Weierstraß Equations

The rational solutions (if there are any) are in bijection (up to a few exceptions) with the rational solutions of a cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with integer coefficients $a_1, \ldots, a_4, a_6$.

Replacing (x, y) with $(r^{-2}x', r^{-3}y')$ takes a_n to $a_n' = r^n a_n$.

Weierstraß Equations

In fact, we may complete the square on the left, “complete the cube” on the right, and eventually get a cubic

$$y^2 = x^3 + Ax + B$$

with integer coefficients A, B.

Example

Last time, we saw that rational points on the cubic

$$C_1 \colon x^2y + xy^2 = 6(xy - 1)$$

gave us Heron triangles with the same perimeter and area as the $(3, 4, 5)$ right triangle.

Example (continued)

If we replace (x, y) with $(-y/x, x^2/y)$ in

$$C_1\colon x^2y + xy^2 = 6(xy - 1),$$

we get a Weierstraß equation

$$C_2\colon y^2 + 6xy + 6y = x^3.$$

Example (continued)

If we replace (x, y) with $(-y/x, x^2/y)$ in

$$C_1\colon x^2y + xy^2 = 6(xy - 1),$$

we get a Weierstraß equation

$$C_2\colon y^2 + 6xy + 6y = x^3.$$

Note that we got two “new” points $(0, 0), (0, -6)$.

Example (continued)

If we replace (x, y) with $(x-3, y-3x+6)$ in

$$C_2 \colon y^2 + 6xy + 6y = x^3,$$

we get

$$C_3 \colon y^2 = x^3 - 9x + 9.$$

Example (continued)

If we replace (x, y) with $(x-3, y-3x+6)$ in

$$C_2\colon y^2+6xy+6y=x^3,$$

we get

$$C_3\colon y^2=x^3-9x+9.$$

Note that a point (a, b) on C_3 corresponds to the point on C_1

$$\left(\frac{b-3a+6}{3-a}, \frac{(3-a)^2}{b-3a+6}\right).$$

The Discriminant D

The curve

$$y^2 = x^3 + Ax + B$$

is non-singular iff the cubic in x has distinct complex roots iff

$$D := -4A^3 - 27B^2 \neq 0.$$

$D \neq 0$, only one real root

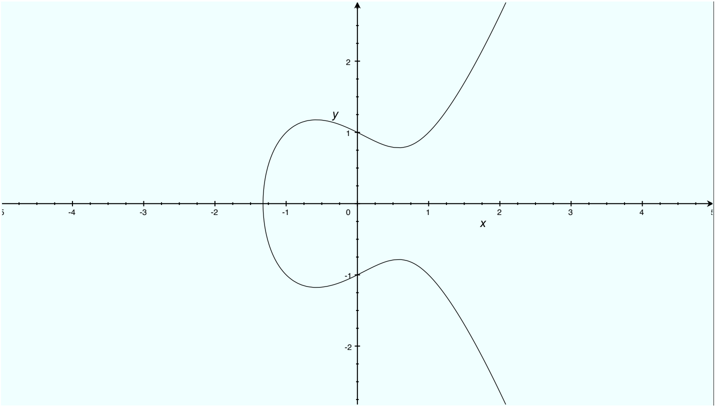

Figure: $y^2 = x^3 - 2x$

$D = 0$, double real root (node)

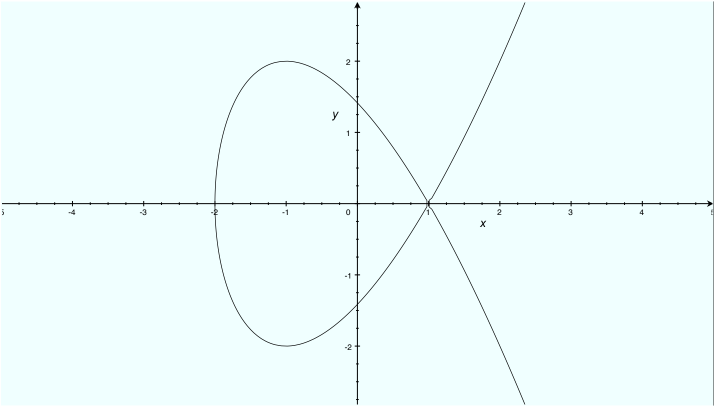

Figure: $y^2 = x^3 - 3x + 2$

$D \neq 0$, three distinct real roots

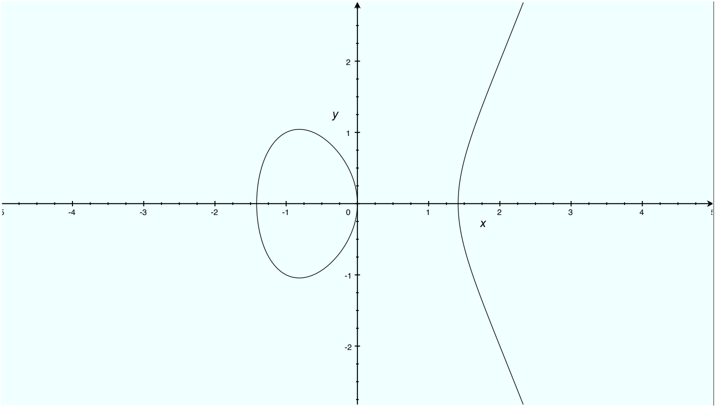

Figure: $y^2 = x^3 - x - 1$

$D = 0$, triple real root (cusp)

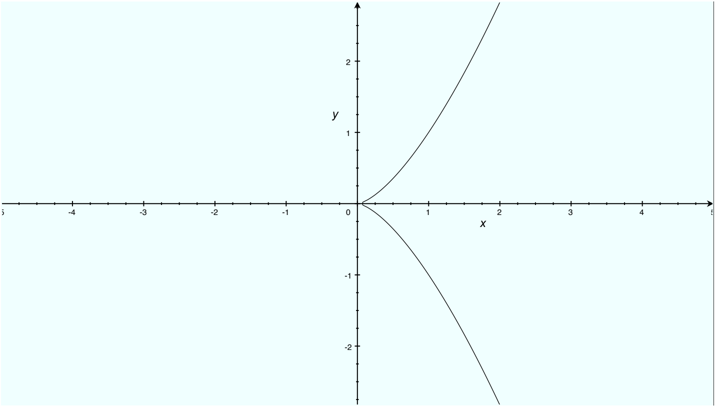

Figure: $y^2 = x^3$

Example (continued)

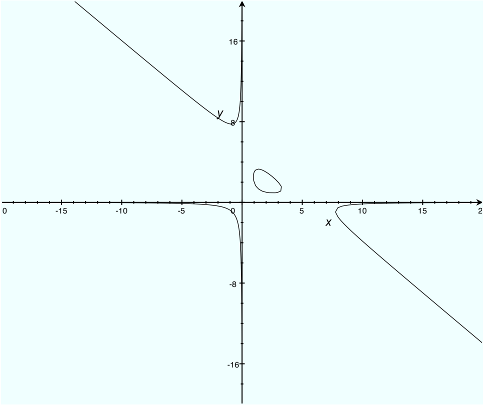

Figure: $C_1 : x^2y + xy^2 = 6(xy - 1)$

Example (continued)

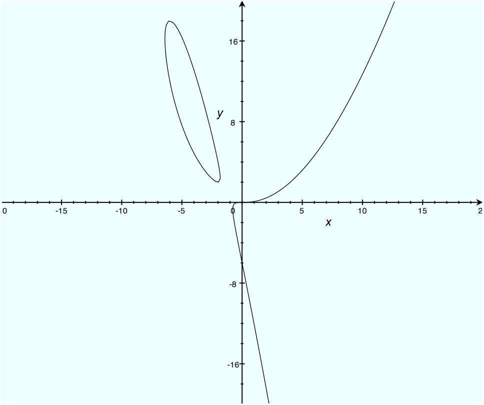

Figure: $C_2: y^2 + 6xy + 6y = x^3$

Example (continued)

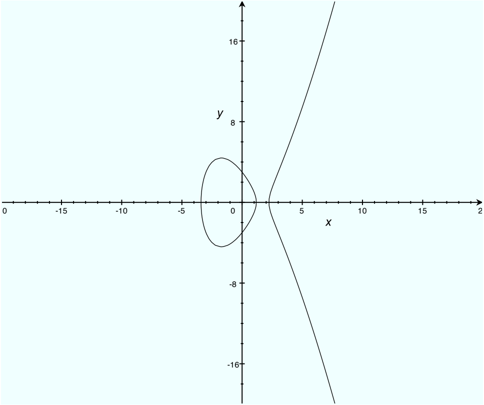

Figure: $C_3 : y^2 = x^3 - 9x + 9$, $D = 729 = 3^6$

The Group Law

Example (continued)

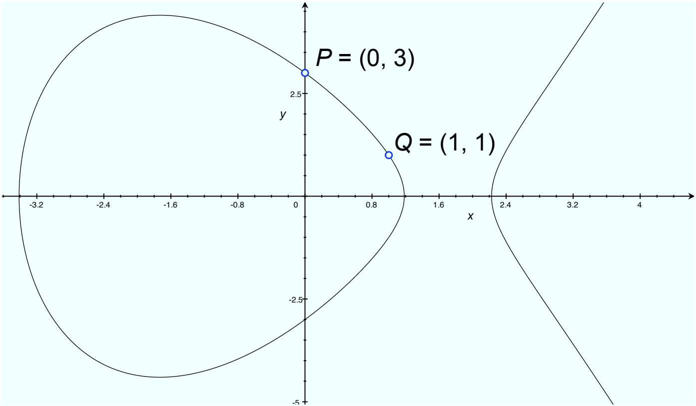

Figure: Our cubic $C_3 : y^2 = x^3 - 9x + 9$

Example (continued)

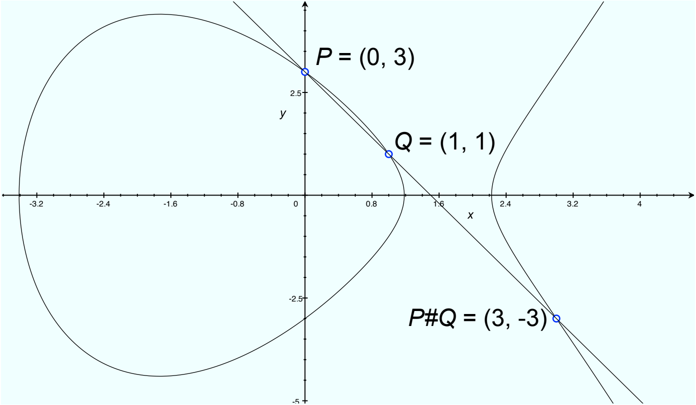

Figure: Our cubic $C_3 : y^2 = x^3 - 9x + 9$

Example (continued)

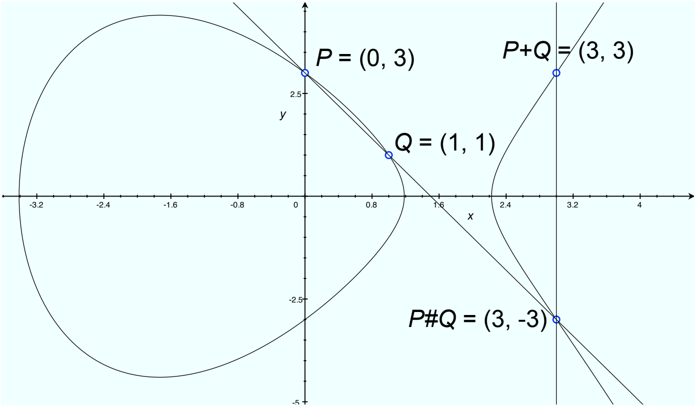

Figure: Our cubic $C_3 : y^2 = x^3 - 9x + 9$

Example (continued)

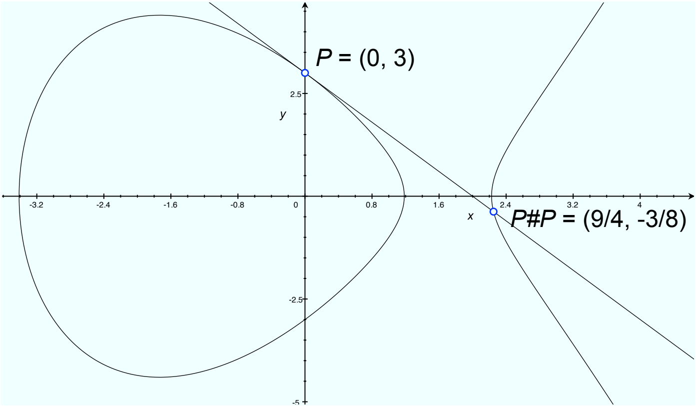

Figure: Our cubic $C_3 : y^2 = x^3 - 9x + 9$

Example (continued)

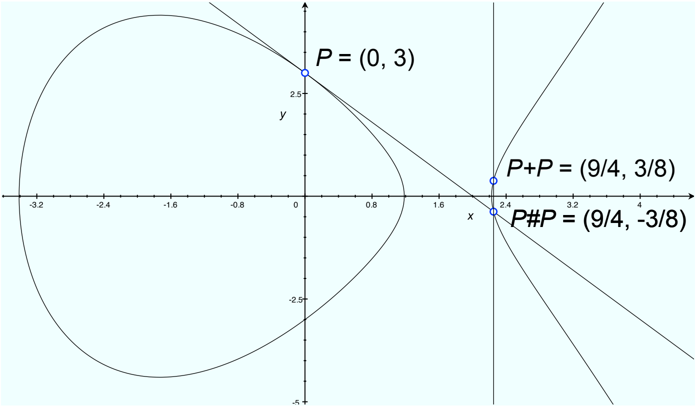

Figure: Our cubic $C_3 : y^2 = x^3 - 9x + 9$

Example (continued)

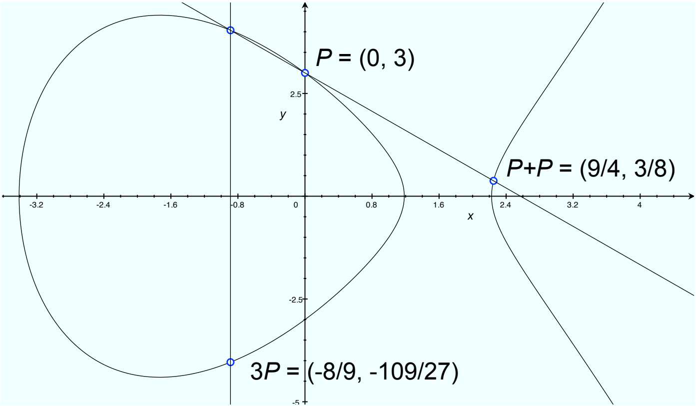

Figure: Our cubic $C_3 : y^2 = x^3 - 9x + 9$

The Point at ∞

Consider a non-singular cubic

$$E : y^2 = x^3 + Ax + B$$

with integer coefficients A, B.

The Point at ∞

Consider a non-singular cubic

$$E : y^2 = x^3 + Ax + B$$

with integer coefficients A, B.

'$+$' is a binary operation on the rational points of E as above.

The Point at ∞

Consider a non-singular cubic

$$E : y^2 = x^3 + Ax + B$$

with integer coefficients A, B.

'$+$' is a binary operation on the rational points of E as above.

Is there an identity element?

The Point at ∞

$$E : y^2 = x^3 + Ax + B \;\Big|\; Y^2 Z = X^3 + AXZ^2 + BZ^3$$

The Point at ∞

$E : y^2 = x^3 + Ax + B$	$Y^2Z = X^3 + AXZ^2 + BZ^3$
$(x, y) = (X/Z, Y/Z)$ affine rational points	$(X : Y : Z), Z \neq 0$ projective integral points

The Point at ∞

$E : y^2 = x^3 + Ax + B$	$Y^2Z = X^3 + AXZ^2 + BZ^3$
$(x, y) = (X/Z, Y/Z)$ affine rational points	$(X : Y : Z), Z \neq 0$ projective integral points
$\mathcal{O}$ $\cap$ (vertical lines)	$(0 : 1 : 0)$ point at ∞

The Point at ∞

$E : y^2 = x^3 + Ax + B$	$Y^2Z = X^3 + AXZ^2 + BZ^3$
$(x, y) = (X/Z, Y/Z)$ affine rational points	$(X : Y : Z), Z \neq 0$ projective integral points
$\mathcal{O}$ $\cap$ (vertical lines)	$(0 : 1 : 0)$ point at ∞

The rational points on E along with $\mathcal{O}$ form an abelian group $E(\mathbb{Q})$ under $+$ with identity $\mathcal{O}$ s.t. $P + Q = \mathcal{O}\#(P\#Q)$.

Example (continued)

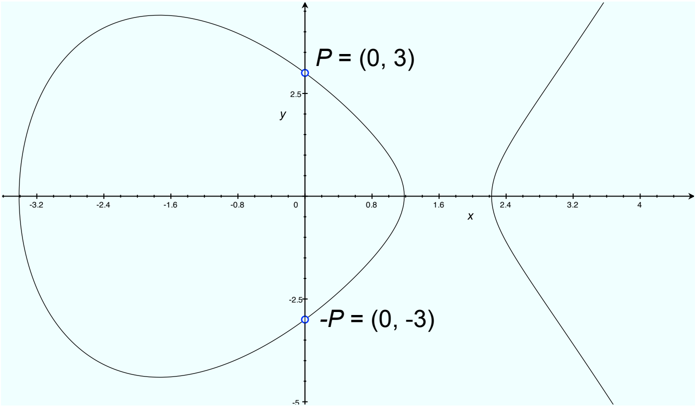

Figure: $-P = \mathcal{O} \# P$ since $\mathcal{O} \# \mathcal{O} = \mathcal{O}$

Torsion Points

Consider a non-singular cubic

$$E : y^2 = x^3 + Ax + B$$

with integer coefficients A, B. We define a torsion subgroup

$$E(\mathbb{Q})_{\text{tors}} := \{P \in E(\mathbb{Q}) : nP = \mathcal{O} \text{ for some } n \in \mathbb{N}\}.$$

Theorem (Nagell-Lutz)

Suppose $P = (a, b) \in E(\mathbb{Q})_{\text{tors}}$. Then a and b are integers, and either $b = 0$ (when $2P = \mathcal{O}$) or b divides D.

Theorem (Mazur)

More specifically,

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/n\mathbb{Z}$$

for some $n \in \{1, \ldots, 10\} \cup \{12\}$ *or*

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$$

for some $n \in \{1, \ldots, 4\}$.

Example (continued)

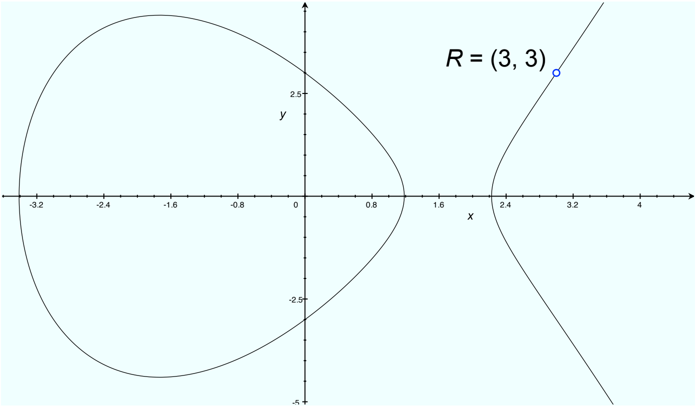

Figure: $3R = \mathcal{O}$

Example (continued)

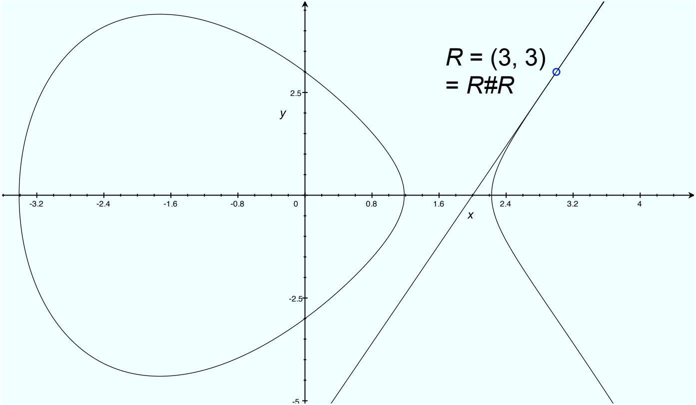

Figure: $3R = \mathcal{O}$

Example (continued)

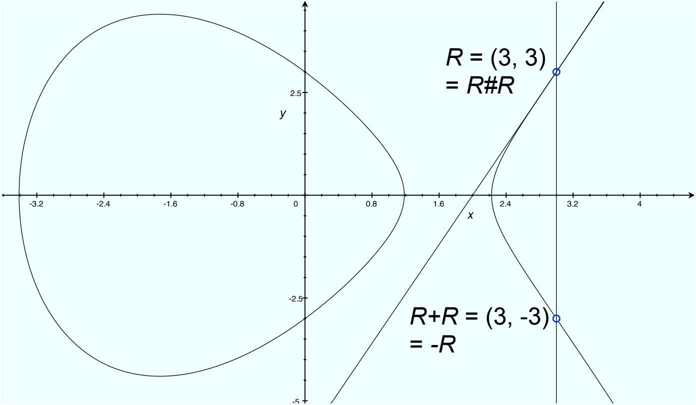

Figure: $3R = \mathcal{O}$

Descent

Suppose there are integers X, Y, Z with $Z > 0$ and

$$X^4 + Y^4 = Z^2$$

Suppose there are integers X, Y, Z with $Z > 0$ and

$$X^4 + Y^4 = Z^2$$

WLOG $(X, Y, Z) = 1$, X is odd, Y is even, so

$$Y^4 = (Z + X^2)(Z - X^2) = (2Z_1^4)(8W^4)$$

with $(Z_1, W) = 1$, Z_1 odd, $Z > Z_1 > 0$.

Now

$$4W^2 = (Z_1^2 - X)(Z_1^2 + X) = (2X_1^4)(2Y_1^4),$$

for some X_1, Y_1, so we get another solution

$$X_1^4 + Y_1^4 = Z_1^2.$$

Now

$$4W^2 = (Z_1^2 - X)(Z_1^2 + X) = (2X_1^4)(2Y_1^4),$$

for some X_1, Y_1, so we get another solution

$$X_1^4 + Y_1^4 = Z_1^2.$$

Continuing this process, we get a chain of positive integers

$$Z > Z_1 > Z_2 > \ldots > Z_Z > 0,$$

a contradiction since $Z_Z \leq Z - Z = 0$.

Consider a non-singular cubic

$$E : y^2 = x^3 + Ax + B$$

with integer coefficients A, B.

Lemma

We have

$$E(\mathbb{Q}) = (Q_1 + 2E(\mathbb{Q})) \cup \cdots \cup (Q_n + 2E(\mathbb{Q}))$$

for some $Q_1, \ldots, Q_n \in E(\mathbb{Q})$.

Start with a point $P \in E(\mathbb{Q})$. Then

Start with a point $P \in E(\mathbb{Q})$. Then

$$P = Q_{k_1} + 2P_1$$

Start with a point $P \in E(\mathbb{Q})$. Then

$$P = Q_{k_1} + 2P_1$$

$$= Q_{k_1} + 2Q_{k_2} + 4P_2$$

Start with a point $P \in E(\mathbb{Q})$. Then

$$P = Q_{k_1} + 2P_1$$

$$= Q_{k_1} + 2Q_{k_2} + 4P_2$$

$$= \ldots = Q_{k_1} + 2Q_{k_2} + \cdots + 2^{m-1}Q_{k_m} + 2^m P_m$$

Start with a point $P \in E(\mathbb{Q})$. Then

$$P = Q_{k_1} + 2P_1$$

$$= Q_{k_1} + 2Q_{k_2} + 4P_2$$

$$= \ldots = Q_{k_1} + 2Q_{k_2} + \cdots + 2^{m-1}Q_{k_m} + 2^m P_m$$

and we have a decreasing sequence of “heights”

$$H(P) > H(P_1) > H(P_2) > \ldots > H(P_{m-1}) \geq K > H(P_m)$$

where K is a constant independent of P.

The height of a point $(a, b) \in E(\mathbb{Q})$ is

$$H((a, b)) = \max\{|e|, |d|\}$$

where e, d are relatively prime integers with $a = e/d$.

The height of a point $(a, b) \in E(\mathbb{Q})$ is

$$H((a, b)) = \max\{|e|, |d|\}$$

where e, d are relatively prime integers with $a = e/d$.

Note that

$$\{R \in E(\mathbb{Q}) : K > H(R)\}$$

is a finite set.

Theorem (Mordell)

$E(\mathbb{Q})$ is a finitely generated abelian group. Thus

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

We call r the rank of E.