Let $\mathbb{k}$ be a field

Def: A poly in two variables over $\mathbb{k}$ is a formal expression

$$f(x,y) = \sum_{\substack{0 \le i \le n \\ 0 \le j \le k}} a_{ij} x^i y^j$$

w/ $a_{n,k} \neq 0$

and $\forall \; 0 \le i \le n, \; 0 \le j \le k$

$a_{ij} \in \mathbb{k}$ - $\boxed{\deg f = n+k}$

We denote by $\mathbb{k}[x,y]$ the collection of all such poly's.

a ring R

Rem

1) $k[x,y] = \overbrace{k[x]}[y]$

2) $k[x,y]$ is a ring

Warning: We don't have long division in $k[x,y]$:

If for any $f, g \in k[x,y]$

$\exists\ q, r \in k[x,y]$ s.th

$$f = gq + r$$

w $\deg(r) < \deg(g)$

Take $f(x,y) = y$, $g(x,y) = x$

$\Rightarrow \exists\, q, r$ s.t.h

$$\boxed{y = qx + r}$$

and $\deg r < \deg g = 1$

$\Rightarrow \deg r = 0 \Rightarrow r \in \mathbb{k}$

Substitute $y = 0 = x$

$\Rightarrow r = 0$

$$y = qx$$

evaluating at $x = 0$

we get $f(0, y) = 0$

- contradiction. //

Geometry: for $\mathbb{k} = \mathbb{R}$ or $\mathbb{C}$

the solution set of

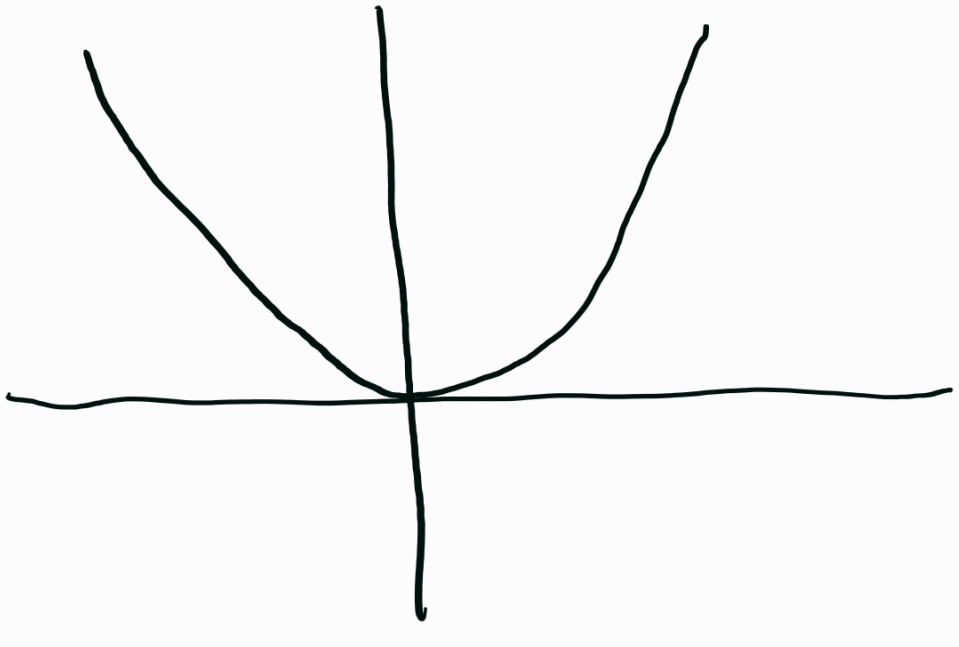
$f(x,y) = 0$ ie

$$Sol(f) = \{ (x_0, y_0) \in \mathbb{R}^2 \mid f(x_0, y_0) = 0 \}$$

eg $f(x,y) = y - x^2 \;/\; \mathbb{R}$

then $Sol(f)$

$$= \{ (x,y) \in \mathbb{R}^2 \mid y = x^2 \}$$



Diophantus: $a, b, g \in \mathbb{Z}$

$$ax + by = g$$

find all int solutions

sol x, y are Bezout's coefficients

they exist iff

$$g = \gcd(a, b).$$

In deg 3:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

To simplify $ax + by = c$

say $b \neq 0$

$$y = \underbrace{\left(-\frac{a}{b}\right)}_{m} x + \underbrace{\left(\frac{c}{b}\right)}_{b'}$$

$$y = mx + b'$$

In deg 3, simplification gives

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

" Generalised Weierstrass form"

If char $k \neq 2, 3$ we can further simplify to short Weierstras form

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

Def: An elliptic curve over a field k is an equation of the form ($\mathrm{char} k \neq 2, 3$)

$$E/k : \boxed{y^2 = x^3 + Ax + B}$$

w/ $A, B \in k$.

(if $k \subseteq k'$ is a field extension, we can consider E/k')

such that

$$\rightarrow \boxed{\Delta := 4A^3 + 27B^2 \neq 0.}$$

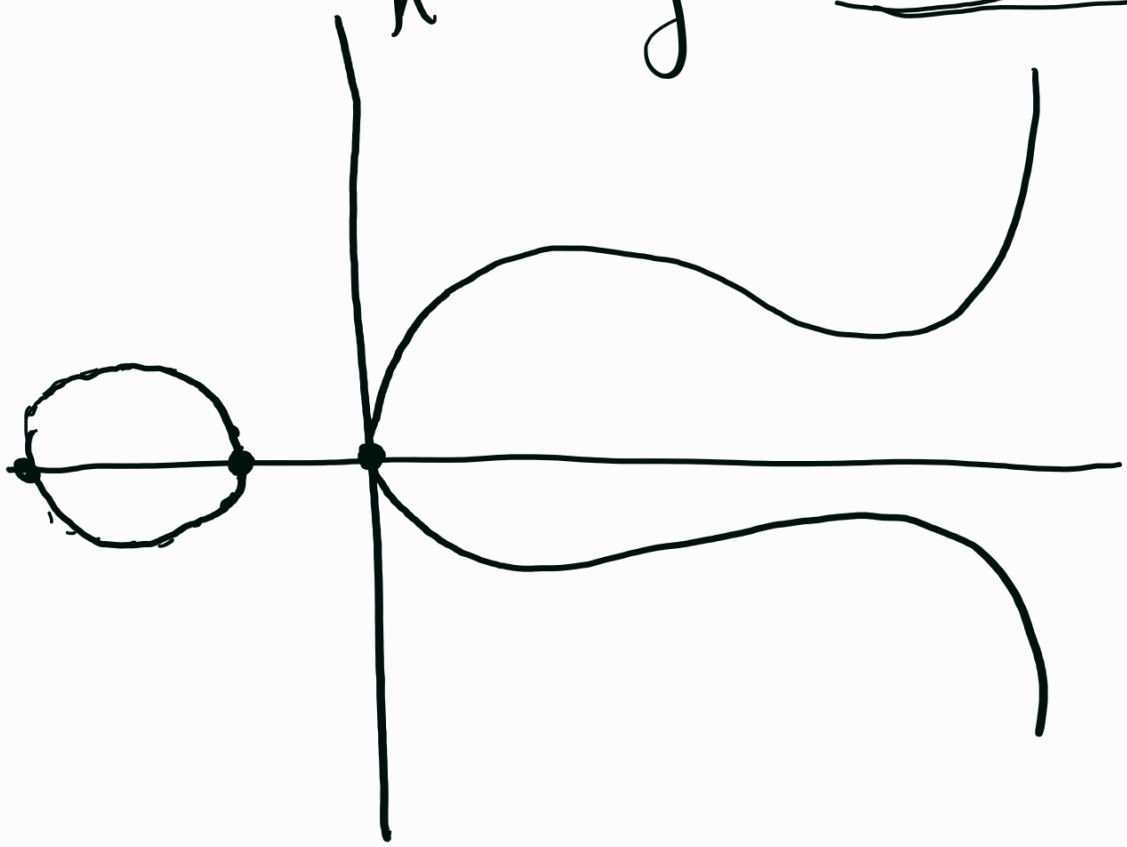
Henceforth, we assume that

char k $\neq 2, 3$.

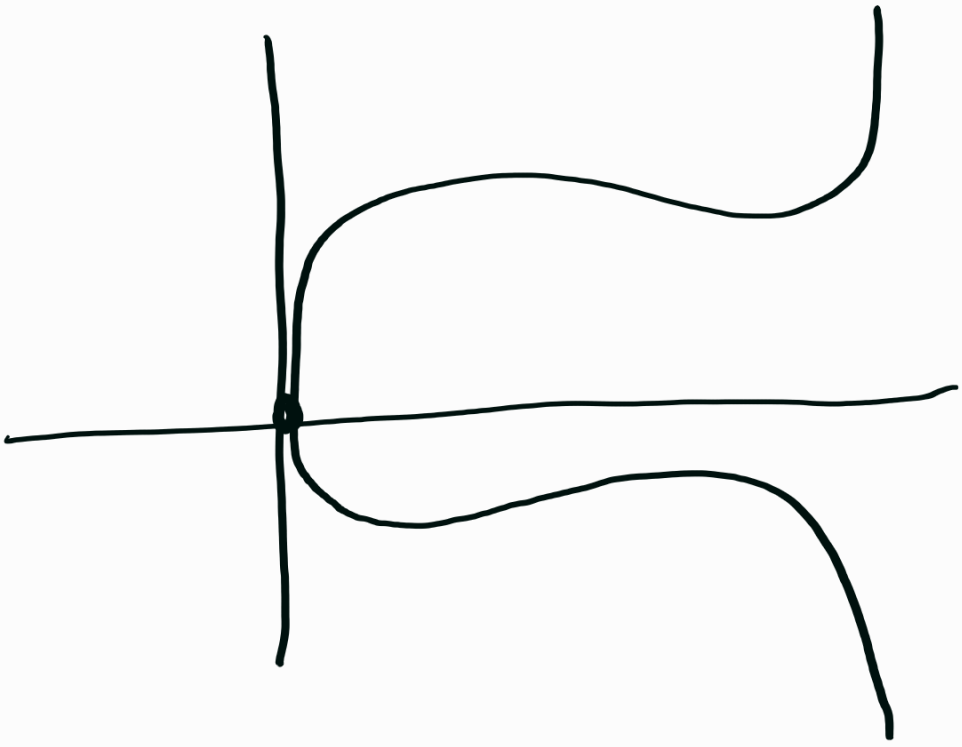
Typically, over $\mathbb{R}$,

$\mathbb{R}^2$ $y^2 = x^3 + Ax + B$

(i)



(ii)



Warning: Take eg.

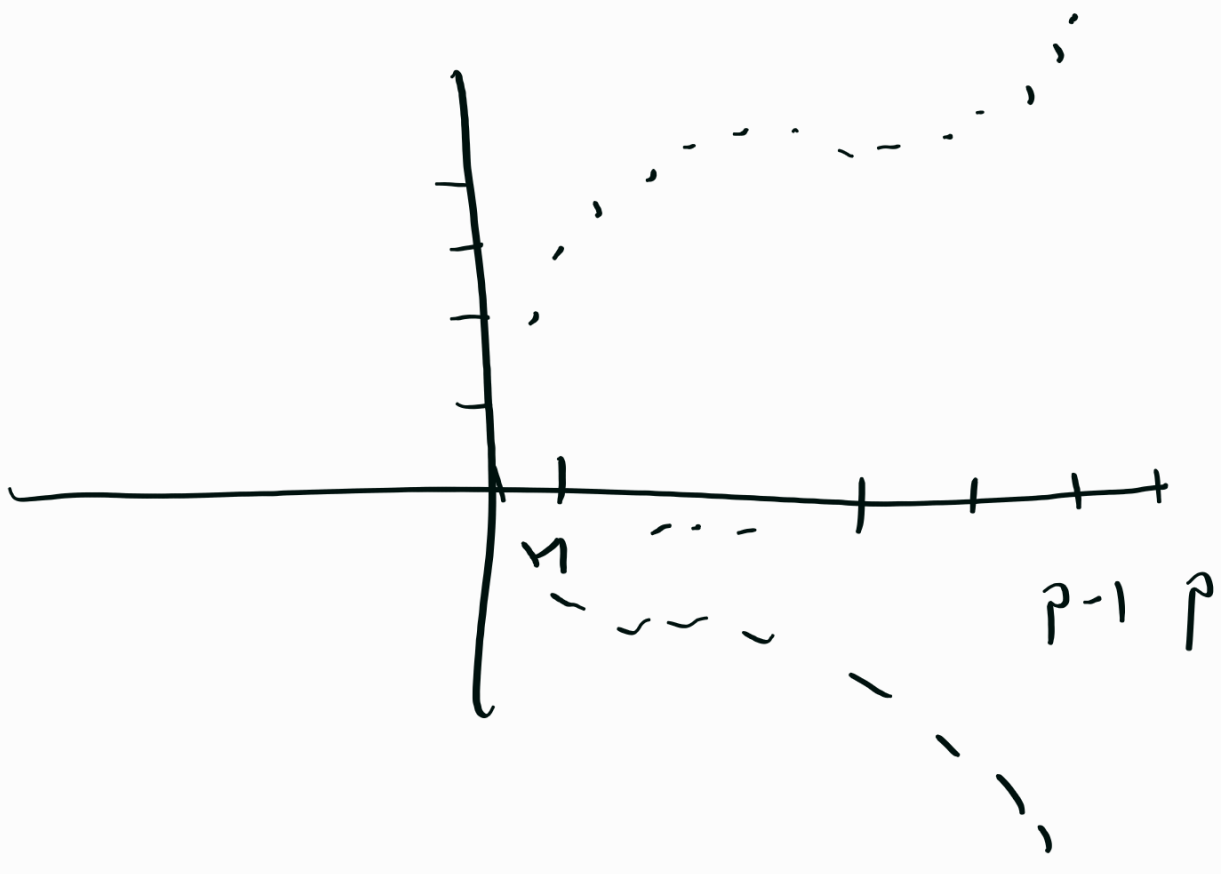
$E/\mathbb{R}$: $y^2 = x^3 + 2x + 3$

We could consider a large prime p and

$E/\mathbb{F}_p$: $y^2 = x^3 + 2x + 3$

$\mathbb{F}_p \subset \mathbb{R}$

X



eg $p = 5$

"Algebraic geometry".

$E_{A,B} = E/\mathbb{R} : y^2 = x^3 + Ax + B$

$\Delta(E) = 4A^3 + 27B^2 \neq 0$

Def suppose $f(x,y) = 0$ is an equation over $\mathbb{R}$.

A tangent line to Graph(f) at (x_0, y_0) s.th $f(x_0, y_0) = 0$ is given by

$T_{(x_0, y_0)}$:

$$(y - y_0) = m(x - x_0)$$

m is the slope of T

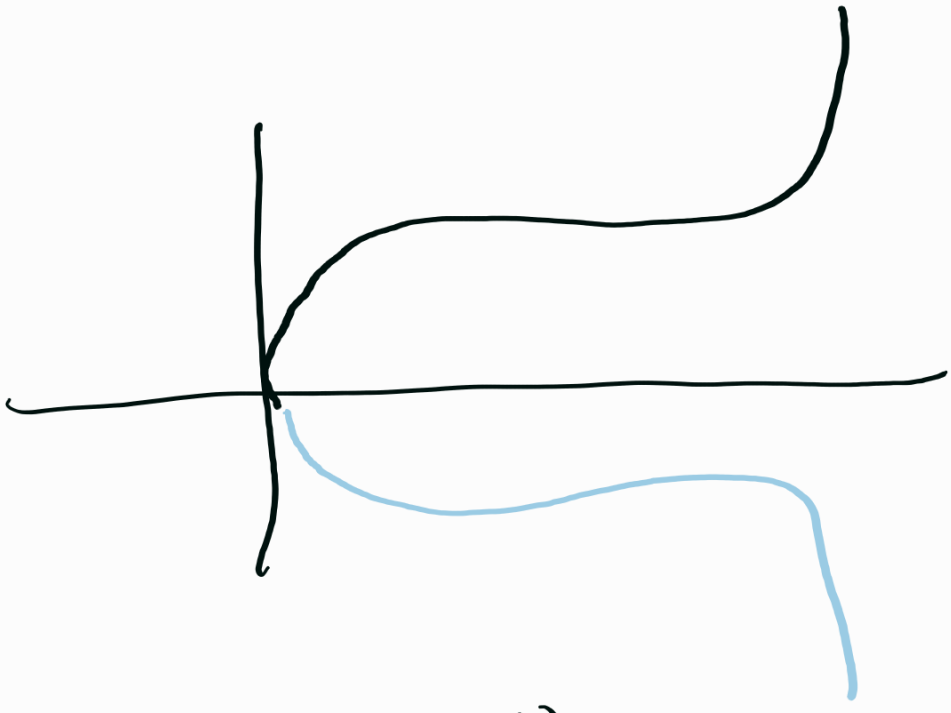
Proposition: Let $E/\mathbb{R}: y^2 = x^3 + Ax + B$

Then E is an elliptic curve (ie $\Delta \neq 0$) iff for every point (x_0, y_0) on E there is a well-defined tangent line.

Proof: We can write

$$y = \sqrt{x^3 + Ax + B}$$

$y(x) = y = \pm\sqrt{x^3 + Ax + B}$



When $y \neq 0$ then

$$\frac{dy}{dx} = \pm \frac{3x^2 + A}{2\sqrt{x^3 + Ax + B}} = 0$$

We have a well-defined tangent line if

$y \neq 0$ $\quad x^3 + Ax + B > 0$

If $x^3 + Ax + B < 0$

then there is no (x, y) on E

bcs

$$y^2 = \underbrace{x^3 + Ax + B}_{\wedge}$$

$$\wedge$$

$$0$$

If $x^3 + Ax + B = 0$

we do implicit differentiation

$$y^2 = x^3 + Ax + B \Big/ \frac{d}{dx}$$

$$d(y^2) = 2y \cdot \frac{dy}{}$$

$$\frac{dx}{dx} \qquad \int dx$$

$$\frac{d(x^3+Ax+B)}{dx} = 3x^2 + A$$

$$\Rightarrow \quad 2y \cdot \frac{dy}{dx} = 3x^2 + A$$

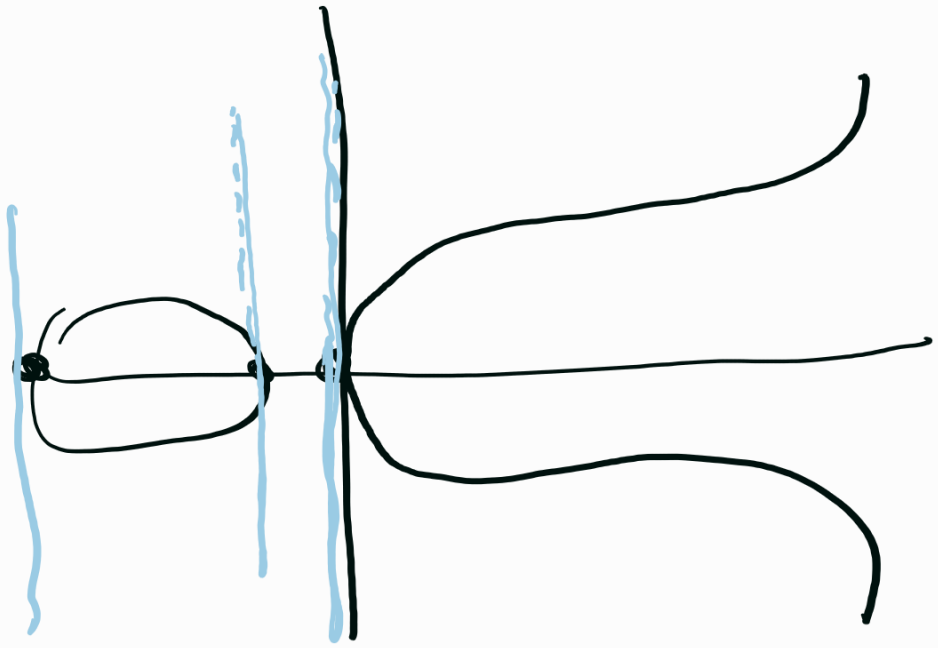
$$\boxed{\frac{dy}{dx} = \frac{3x^2+A}{2y}}$$

Suppose $y = 0$ but $3x^2 + A \neq 0$

We can interchange $x \leftrightarrow y$ so that the numerator is zero and the denomenator is non-zero so the

slope will be zero.

Interchanging $y \leftrightarrow x$ again we get a tangent line parallel to the y-axis



lastly, if $y = 0$ and $3x^2 + A = 0$ then $A < 0$ so we substitute $A = -A$ to get

(*) $y^2 = x^3 - Ax + B$

w/ $A > 0$.

In that case,

$$3x^2 - A = 0 \Rightarrow$$

$$x = \pm\sqrt{\frac{A}{3}}$$

substituting that in (*) gives:

$$\left(\sqrt{A/3}\right)^3 - A\sqrt{A/3} + B = 0$$

$$\Leftrightarrow \quad \frac{2A^{\frac{3}{2}}}{3\sqrt{3}} = B$$

$$\Leftrightarrow \quad \frac{4A^3}{27} = B^2$$

$\Leftarrow$ $\quad 4A^3 - 27B^2 = 0$

$A := -A$

$\Rightarrow \quad 4A^3 + 27B^2 = 0$

So we have a well-defined tangent line at this point $\Leftrightarrow \Delta \neq 0$. //

Rem: In general Weierstras form $\Delta(E)$ is defined differenty

Proposition: Let k be either

$\mathbb{R}$ or a field of positive char $\neq 2, 3$. A cubic

$$f(x) = x^3 + Ax + B$$ over k

admits a repeated root over $\bar{k}$ iff $\Delta = 4A^3 + 27B^2 \neq 0$.

$$ax^2 + bx + c = 0 \quad \pm\sqrt{\Delta}$$

$$\Delta = b^2 - 4ac$$

$$\bar{\mathbb{R}} = \mathbb{C}$$

Proof: over $\bar{k}$ we can write

$$\underbrace{x^3 + Ax + B}_{\text{LHS}} = f(x) = \underbrace{(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)}_{\text{RHS}}$$

$\Rightarrow$ $\alpha_1 + \alpha_2 + \alpha_3 = 0$ (

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = A$$

$$\alpha_1\alpha_2\alpha_3 = -B$$

If f had a repeated root

say $\alpha_1 = \alpha_2 =: \alpha$, then

$$\boxed{\alpha_3 = -2\alpha.}$$

$$\Rightarrow \begin{cases} A = \alpha^2 - 2\alpha^2 - 2\alpha^2 = -3\alpha^2 \\ B = -2\alpha^3 \end{cases}$$

$$\Rightarrow \begin{cases} A^3 = -27\alpha^6 \\ B^2 = 4\alpha^6 \end{cases} \Rightarrow \quad \div$$

$$=$$

$$\frac{A^3}{} \qquad 27$$

$$\frac{}{B^2} = \frac{}{4}$$

$$\Leftrightarrow \boxed{4A^3 + 27B^2 = 0}$$

So if there are repeated roots of

$$f(x) = x^3 + Ax + B$$

in $\overline{\mathbb{K}}$ then $\Delta = 0$

and if $\Delta \neq 0$ there are no repeated roots. //