Exercises

(1) $\overset{1.2}{\Rightarrow}$ $\mathcal{C} = \{(x,y) \in K^2 \mid f(x,y) = ax^2 + bxy + cy^2 + dx + ey + f = 0\}$

$$M = \begin{pmatrix} 2a & b & d \\ b & 2c & e \\ d & e & 2f \end{pmatrix} \qquad \delta = |M|.$$

a) If $\delta \neq 0 \Rightarrow$ $\mathcal{C}$ has no singular points.

$C = \{(x,y) \in K^2 \mid (x,y,1)\, M \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = 0\}$. It's convenient to work in $\mathbb{P}^2(K)$:

$$\tilde{C} = \{(x:y:z) \in \mathbb{P}^2(K) \mid (x,y,z) M \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0\}.$$

So $\exists\, (x:y:z) \in \mathbb{P}^2(K)$ s.t. $\nabla F(x:y:z) = (0,0,0) \Leftrightarrow$ ($\vec{x}^t$, $F(\vec{x}) = \vec{x}^t M \vec{x}$)

$M\vec{x} + (\vec{x}^t M)^t = M\vec{x} + M^t\vec{x} = 2M\vec{x} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ (*) notice $M = M^t$.

Since $\delta \neq 0$ this can only happen if $(x,y,z) = (0,0,0)$ $\Rightarrow$ $(x:y:z) = (0:0:0)$!!.

b) If $\delta = 0$ and $b^2 - 4ac \neq 0 \Rightarrow$ there is a unique singular point in C.

If $\delta = 0 \Rightarrow$ there are ∞ many solutions of (*), but

if $b^2 - 4ac = |M_2| \neq 0$ then the system is equivalent to

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow$$ it has rank 2 $\Rightarrow$ the sols. space has dim 1

$a_{11}a_{22} \neq 0$ $\Rightarrow$ $S = \langle (x_0,y_0,z_0) \rangle = \{(x_0:y_0:z_0)\}$

(2) → 1.7

show that there are no rational points or find one

a) $x^2+y^2=6$. Want $x^2+y^2 \neq 6z^2$ with $(x,y,z) \in \mathbb{Z}^3$ pairwise coprime. Assume x odd, y ~~odd~~ even !!

Assume x odd, y odd $\Rightarrow$ $x^2+y^2 \equiv 2 \bmod 4$

$6z^2 \equiv 2z^2 \bmod 4$ way happen.

module 3? x, y cannot be $\equiv 0 \bmod 3$.

$(x,y) \equiv (3, \pm 1) \Rightarrow x^2+y^2 \equiv 1 \equiv 0 \bmod 3$!!

$(\pm 1, 3) \Rightarrow \equiv 1 \equiv 0 \bmod 3$!!

$(\pm 1, \pm 1) \Rightarrow x^2+y^2 \equiv -1 \equiv 0 \bmod 3$!!

$\Rightarrow C(\mathbb{Q}) = \emptyset$

b) $3x^2+5y^2=4$ rational sol $\Leftrightarrow$ $3x^2+5y^2=4z^2$ integer sol. pairwise coprimes.

work mod 3: if $\exists (x,y,z)$ s.t $2y^2 \equiv z^2 \bmod 3$

if $y \not\equiv 0 \bmod 3 \Rightarrow z \equiv 0 \bmod 3$!!

if not $2 \equiv t^2 \bmod 3$ $t = \frac{z}{y}$ but $2 \equiv -1$ not a square mod 3.

c) homework.

(3) (1.8) $\forall e \geq 1$, $x^2+1 \equiv 0 \bmod 5^e$ has $x_e \in \mathbb{Z}/5^e\mathbb{Z}$, also, $x_{e+1} \equiv x_e \bmod 5^e$.

$e=1$: -1 is a square mod 5 $\left(\frac{-1}{5}\right)=1$.

Suppose $\exists x_1, x_2, \dots, x_e$ s.t $x_n^2+1 \equiv x_n \bmod 5^n \Rightarrow$ $1 \leq n \leq e$

Want $x_{e+1} = x_e + t \cdot 5^e$ s.t. $x_{e+1}^2 = x_e^2 + t^2 \cdot 5^{2e} + 2 \cdot x_e \cdot t \cdot 5^e$

$t \in \{0,1,\dots,5-1\}$ $\equiv -1 \bmod 5^{e+1}$

but $x_{e+1}^2 \equiv -1 \bmod 5^{e+1}$: $x_{e+1}^2 = -1 + s_e \cdot 5^e + t^2 \cdot 5^{2e} + 2 x_e t 5^e \equiv -1 \bmod 5^{e+1}$

$\Leftrightarrow$ $s_e + 2x_e t + t^2 \equiv 0 \bmod 5$.

$\Leftrightarrow t = \frac{-s_0}{2x_0} \bmod s$

Hensel's lemma

$f(x) \in \mathbb{Z}[x]$, $x_1 \in \mathbb{F}_p$ s.t. $f(x_1) \equiv 0 \bmod p$ and $f'(x_1) \not\equiv 0 \bmod p$

$\Rightarrow \forall e \geq 1$, $\exists x_e \in \mathbb{Z}/p^e\mathbb{Z}$ s.t. $f(x_e) \equiv 0 \bmod p^e$, $x_{e+1} \equiv x_e \bmod p^e$.

$f(x) = \sum_{j=0}^{N} \frac{f^{(j)}(x_e)}{j!}(x-x_e)^j$. want $x_{e+1} = x_e + t \cdot p^e$ s.t. $f(x_{e+1}) \equiv 0 \bmod p^{e+1}$

$f(x_{e+1}) \equiv f(x_e) + f'(x_e)(x-x_e) + \sum_{j\geq 2}^{N} \frac{f^{(j)}(x_e)}{j!} t^j p^{je} \equiv f(x_e) + f'(x_e) t p^e \bmod p^{e+1}$

$f(x_{e+1}) \equiv 0$ ← want

enough: $s_e + f'(x_e)t \equiv 0 \bmod p \Leftrightarrow \boxed{t = \frac{-s_e}{f'(x_e)}}$ se p^e

Say something about p-adics.

④ 1.19 $E: y^2 = x^3 + ax^2 + bx + c$, $P = (x,y) \in E$.

a) Verify that $x(2P) = \frac{x^4 - 2bx^2 - 8cx - 4ac + b^2}{4y^2}$

b) Derive a similar formula for $y(2P)$ in terms of x, y.

c), d) home

—

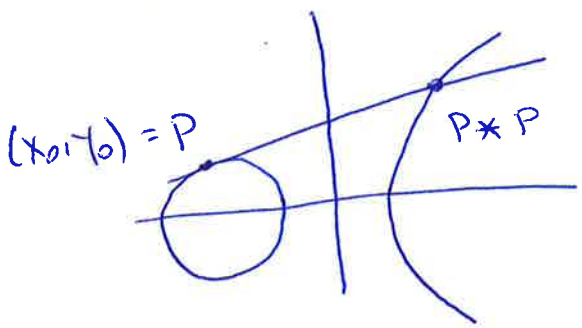
a) x-coord of $2P$ is x-coord of $P * P$.

$L: y = \lambda x + \nu$, tangent line to E at P

$L: G_x \cdot (x - x_0) + G_y (y - y_0) + G(x_0, y_0) = 0$

$G_x := G_x(x_0, y_0)$

$G_y := G_y(x_0, y_0)$



$G(x,y) = y^2 - f(x) = y^2 - (x^3 + ax^2 + bx + c) = 0$

$\Rightarrow L: G_{x_0} \cdot x + G_{y_0} \cdot y = G_{x_0} x_0 + G_{y_0} \cdot y_0$

$\Rightarrow L: -f'(x_0) \cdot x + 2y_0 \cdot y = -2y_0^2 - f'(x_0) x_0 \Rightarrow$

$$y = \underbrace{\left| \frac{f'(x_0)}{2y_0} \right|}_{\mu} x - \underbrace{\left| \frac{f'(x_0)x_0 + 2y_0^2}{2y_0} \right|}_{-\nu}.$$

$G(x, \lambda x + \nu) = (\lambda x + \nu)^2 - f(x) = 0$ ec. of $L \cap E$.

$\Rightarrow \lambda^2 x^2 + \nu^2 + 2\lambda\nu x - f(x) = -x^3 + (\lambda^2 - a)x^2 + \dots$

$\Rightarrow x_1 = \lambda^2 - a - 2x_0 =$ $\quad (= 2x_0 + x_1 \quad x_1 = x(2P))$

$$= \frac{f(x_0)^2}{4y_0^2} - \frac{4y_0^2 a}{4y_0^2} - \frac{8x_0 y_0^2}{4y_0^2} = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4(x_0^3 + ax_0^2 + bx_0 + 4c)} =$$

$$= \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4y_0^2}.$$

b) $y = \lambda x + \nu \Rightarrow$ $\quad y_1 = \frac{f'(x_0)}{2y_0} \cdot \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4y_0}$

$(= y(P * P))$

$$+ \frac{f'(x_0)x_0 + 2y_0^2}{2y_0} =$$

$$= \frac{(3x_0^2 + 2ax_0 + b)(x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac)}{8y_0^2} + \frac{4(3x_0^2 + 2ax_0 + b)x_0 + 8y_0^3}{8y_0^2}$$

$y(2P) = -y(P * P).$