① 重数：根、零点、交点的重数

~~贝~~贝祖定理

② 除子

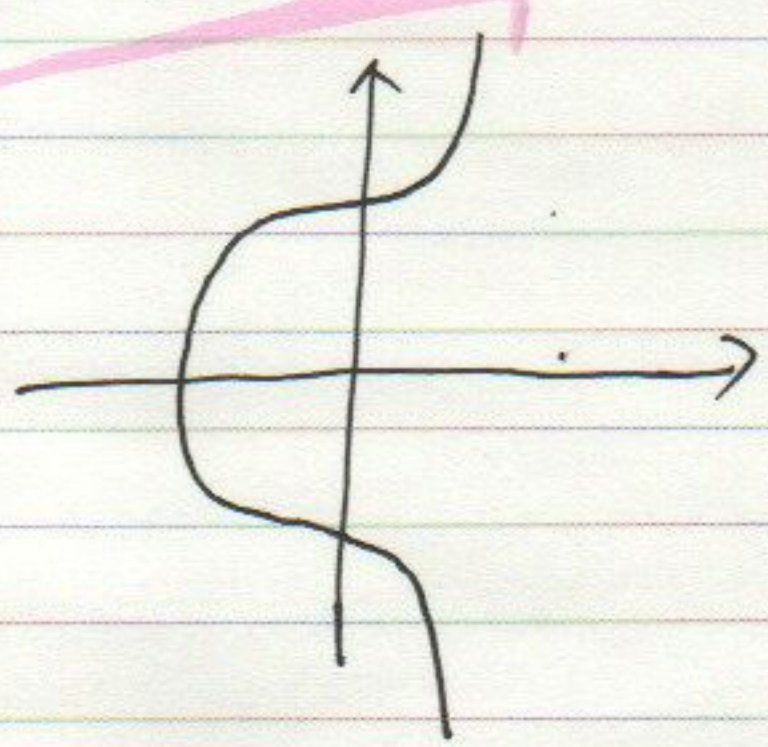
黎曼罗赫定理

③ Weil Pairing

④ 计算Weil Pairing

Miller算法

Secp256K1 $y^2=x^3+7$ 曲线 C



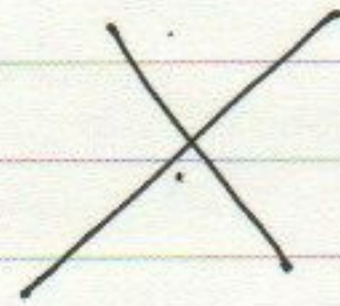
问题 ① 两条直线有几个交点? 0,1,∞

② 直线与曲线C有几个交点? 0,1,2,3

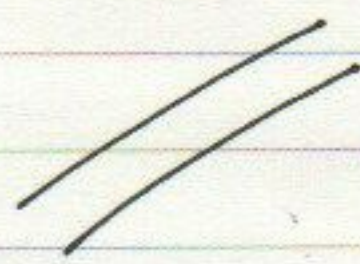
贝祖定理

m度 和 n度 曲线 有 m·n个交点

① 两条直线有几个交点

△ 相交  1个交点

△△ 重合  ∞个交点

△△△ 平行  0个交点？

1个交点？

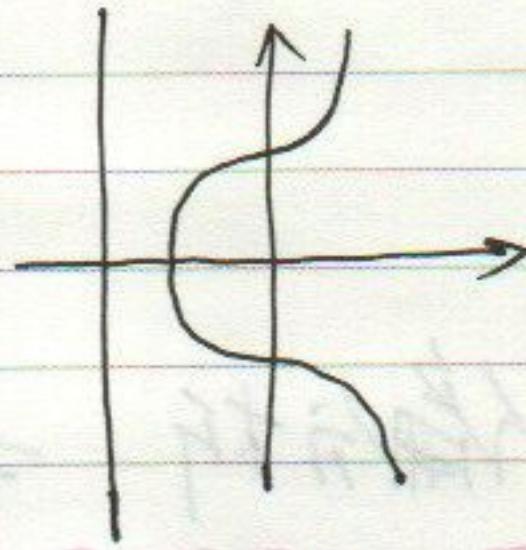
例子 $\begin{cases} y=x \\ y=x+1 \end{cases} \xRightarrow{\text{齐次方程}} \begin{cases} y=x \\ y=x+z \end{cases}$

$\Rightarrow$ 交点 $(x\neq 0,\ y=x,\ 0)$

$\Rightarrow$ 射影空间中交点 $(1, 1, 0)$

$\boxed{\text{两条不同直线相交于 1 点}}$

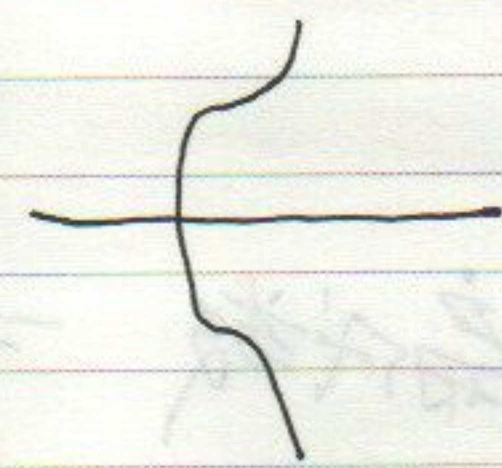
② 直线和曲线C相交于几个点？



$$\begin{cases} y^2=x^3+7 \\ x=-2 \end{cases} \Rightarrow y^2=-1 \Rightarrow y=\pm i$$

⇒ 复数域＋射影空间相交于3个点

$(-2, i, 1)$ $(-2, -i, 1)$ $(0, 1, 0)$



$$\begin{cases} y^2=x^3+7 \\ y=0 \end{cases} \Rightarrow x^3=-7 \Rightarrow x=-7^{1/3}, -7^{1/3}\omega, -7^{1/3}\omega^2$$

⇒ 复数域有3个交点

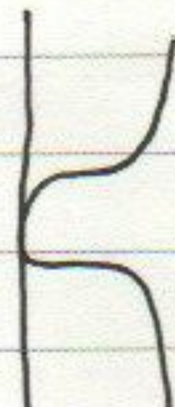
$(-7^{1/3}, 0)$ $(-7^{1/3}\omega, 0)$ $(-7^{1/3}\omega^2, 0)$

$$\begin{cases} y^2=x^3+7 \\ x=0 \end{cases} \Rightarrow y^2=7 \Rightarrow y=\pm\sqrt{7}$$

⇒ 射影空间相交于3个点

$(0, \sqrt{7}, 1)$ $(0, -\sqrt{7}, 1)$ $(0, 1, 0)$

相交于3个点



$$\begin{cases} y^2=x^3+7 \\ x=-7^{1/3} \end{cases} \Rightarrow y^2=0 \Rightarrow y=0$$

⇒ 射影空间相交于2个点

$(-7^{1/3}, 0, 1)$ $(0, 1, 0)$

⇒ $\boxed{\text{交点的重数？}}$

交点的重数

△ 根的重数

例子 $y=f(x)=x^2$ 的根为 $x=0$，重数为2。

① 微扰法

$$\Rightarrow y=x^2+\delta \quad (\delta\to 0)$$

$\Rightarrow$ 根为 $x=\pm\sqrt{-\delta}$ 有两个根，故重数为2.

② 流根法

$y=x$ 的根为 1重

1重 × 1重 = 2重

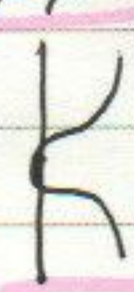
m重 × n重 = m+n重

$\Rightarrow x^2=x\cdot x$ 为2重

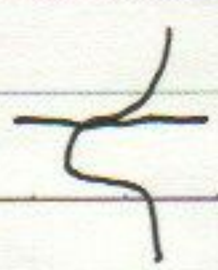
例 x^2 在 $x=0$，$(x-1)^3$ 在 $x=1$

$x^2(x-1)^3$ 在 $x=0$，$x=1$

△ 交点重数

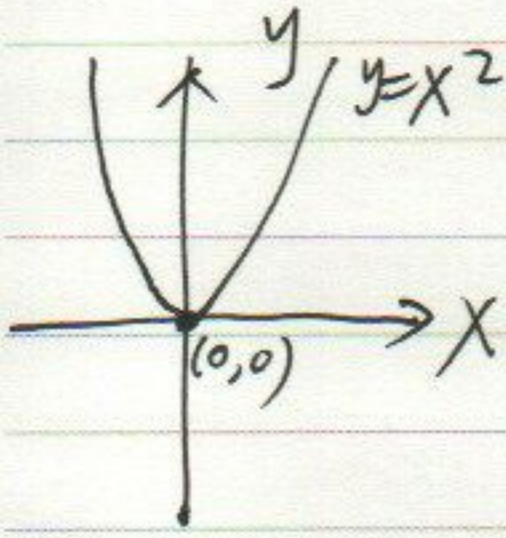


$\begin{cases} y^2=x^3+7 \\ x=-7^{1/3} \end{cases} \Rightarrow \begin{array}{l} x=-7^{1/3} \\ y\text{为 } y^2=0 \text{ 的根} \end{array}$ ⇒ 交点重数为2



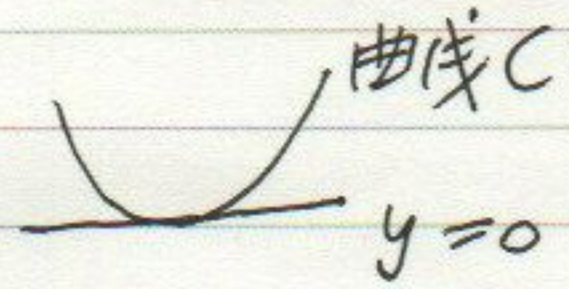
$\begin{cases} y^2=x^3+7 \\ y=\sqrt{7} \end{cases} \Rightarrow \begin{cases} x\text{为 } x^3=0 \text{ 的根} \\ y=\sqrt{7} \end{cases}$ ⇒ 交点重数为3

交点重数 换个视角

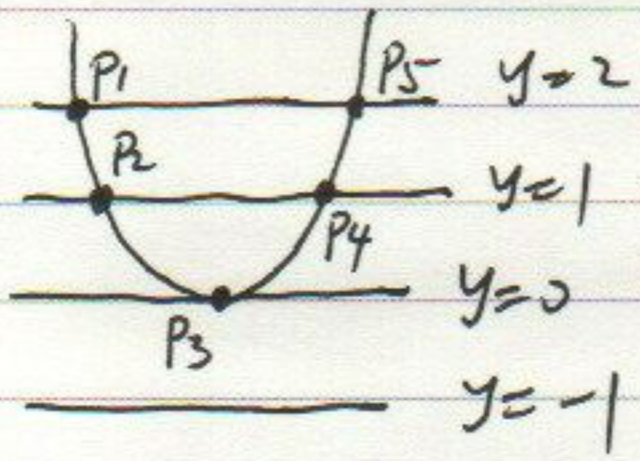


$\Rightarrow \begin{cases} y=x^2 \\ y=0 \end{cases}$ 的根是2重

$\Rightarrow$



在曲线 $y=x^2$ 上
函数 y 的根的重数



函数 $f(p)=y_p$

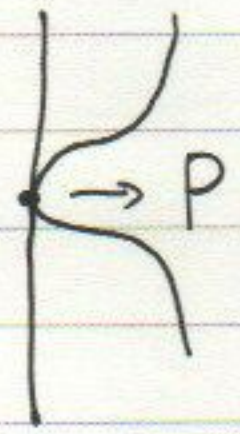
$\Rightarrow f(P_1)=2=f(P_5)$

$f(P_2)=f(P_4)=1$

$f(P_3)=0$

$\boxed{\text{函数为坐标 } x, y \text{ 的有理函数，即 } \dfrac{\text{多项式}}{\text{多项式}}}$

例子 $\begin{cases} y^2 = x^3+7 \\ x = -7^{1/3} \end{cases}$ 求交点 P的重数



⇒ 在曲线 C : $y^2=x^3+7$ 上

函数 $x+7^{1/3}$ 的根的重数

在P有 $y=0$, $x+7^{1/3}=0$, 即 $P=(-7^{1/3},0)$ 是根

重数 ≥ 1

$$x+7^{1/3} = \frac{x^3+7}{x^2-7^{1/3}x+7^{2/3}} = \frac{y^2}{x^2-7^{1/3}x+7^{2/3}}$$

y的重数 ≥ 1, ⇒ y^2 重数 ≥ 2

$1/x^2-7^{1/3}x+7^{2/3}$ 在P的值为 $\frac{1}{7^{2/3}} \neq 0$

⇒ $x+7^{1/3}$ 的根 ≥ 2

严格的论证需要用环和理想的语言

有理函数的零点和极点

$$f(P)=f(x,y)=\frac{f_1(x,y)}{f_2(x,y)}\begin{array}{l}\in \text{多项式}\\ \in \text{多项式}\end{array}$$

$\boxed{\text{定义 } \mathrm{ord}_P f = f_1 \text{ 的零点重数} - f_2 \text{ 的零点重数}}$

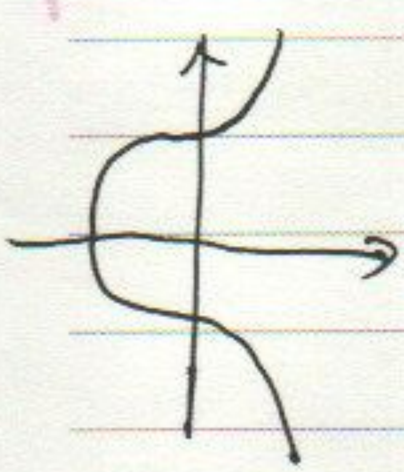
>0 零点

$=0$

<0 极点

除子

在 $C: y^2=x^3+7$ 上



函数 $x=0$ 的除子为

$P_1=(0,\sqrt{7},1)$ $P_2=(0,-\sqrt{7},1)$ $P_3=(0,1,0)$

$$\mathrm{div}(x) = (P_1)+(P_2)-\underbrace{2}_{\mathrm{ord}_{P_3}x}(P_3)$$

有理函数除子的性质（主除子）

① $\deg \operatorname{div}(f) = 0$

例 $\operatorname{div}(f) = (P_1) + (P_2) - 2(P_3)$

$\deg \operatorname{div}(f) = 1 + 1 - 2 = 0$

② $\operatorname{div}(f) = (P_1) + (P_2) - 2(P_3)$

$\Rightarrow P_1 + P_2 - P_3 - P_3 = 0 \rightarrow$ 零点

③ 除子几乎唯一确定了函数（仅常数区别）

$\operatorname{div}(f_1 \cdot f_2) = \operatorname{div}(f_1) + \operatorname{div}(f_2)$

$\operatorname{div}(f_1/f_2) = \operatorname{div}(f_1) - \operatorname{div}(f_2)$

$\operatorname{div}(cf) = \operatorname{div}(f)$ $c \neq 0$ 为常数

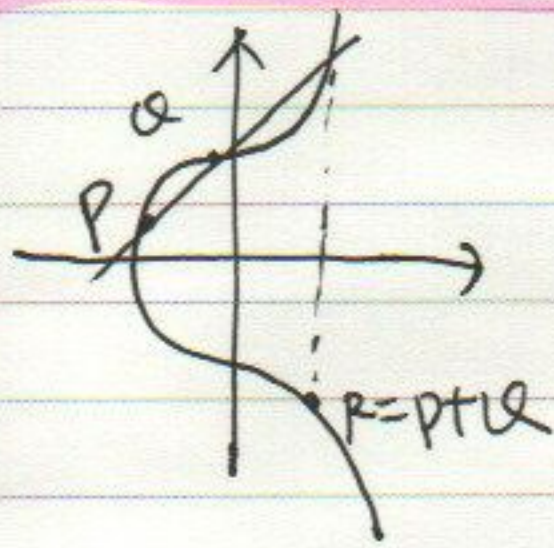
$\Rightarrow \operatorname{div}(f_1) = \operatorname{div}(f_2) \Rightarrow \operatorname{div}(f_1) - \operatorname{div}(f_2) = \cancel{\operatorname{div}(c)}\ 0$

$\Rightarrow \operatorname{div}(f_1/f_2) = \cancel{\operatorname{div}(c)}\ 0$

$\Rightarrow f_1/f_2 = c \neq 0$

$\Rightarrow f_1 = c f_2$

C线上的点，构成群 # $\quad C: y^2 = x^3 + 7$



$P \neq Q$ $\quad \lambda = \dfrac{y_Q - y_P}{x_Q - x_P} \qquad \nu = y_P - \lambda x_P$

$$R = P \oplus Q = \begin{cases} x_R = \lambda^2 - x_P - x_Q \\ y_R = -(\lambda x_R + \nu) \end{cases}$$

$P = Q$ $\quad \lambda = \dfrac{3x_P^2 + a}{2y_P} \ (a=0) \qquad \nu = y_P - \lambda x_P$

$$R = P \oplus P = \begin{cases} x_R = \lambda^2 - 2x_P \\ y_R = -(\lambda x_R + \nu) \end{cases}$$

$\boxed{\text{子群 } E[m]}$

定义 $[m]P = \underbrace{P + P + \cdots + P}_{m\text{个}} = R$

则 x_R 和 y_R 为 x_P 和 y_P 的有理函数

$E[m] = \{P \mid [m]P = 0\}$ 是一个群

其 0 元素为 0

考虑 $\#E[m]$

$m=1 \Rightarrow E[m] = \{0\} \Rightarrow \#E[m] = 1$

$m=2 \Rightarrow 0 \in E[m]$

且 $(-7^{1/3}, 0)$ $(-7^{1/3}\omega, 0)$ $(-7^{1/3}\omega^2, 0)$

$\in E[m]$

$\Rightarrow \#E[m] = 4$

$\boxed{\#E[m] = m^2}$

Weil Pairing

$\#E[m]=m^2$，对 $\forall\ T\in E[m]$

① 考虑除子 $m(T)-m(O)$

☆ $\deg=0$

☆ $[m]T-[m]O=O$

$\Rightarrow \exists\ f$ 有 $\mathrm{div}(f)=m(T)-m(O)$

② 再考虑除子 $\sum_{R\in E[m]}\{(T'+R)-(R)\}$ 其中 $[m]T'=T$

☆ $\deg=0$

☆ $\sum_R T'+R-R=[m^2]T'=O$

$\Rightarrow \exists\ g$ 有 $\mathrm{div}(g)=\sum_R\{(T'+R)-(R)\}$

③ 再考虑 $\mathrm{div}(f\circ[m])$

其零点包括 $T'\in E[m^2]$ 其中 $[m]T'=T$

包括 $R\in E[m]$

包括 $O\in E[m]$

其极点包括 $O\in E[m]$

其除子为 $\sum_{\substack{T'\in E[m^2]\\ [m]T'=T}} m(T')-\sum_{R\in E[m]} m(R)$

④ 再考虑 $\mathrm{div}(g^m)$

$$= \sum_{R \in E[m]} \{ m(T'+R) - m(R) \}$$

$$= \boxed{\sum_{\substack{T' \in E[m^2] \\ [m]T' = T}} m(T') - \sum_{R \in E[m]} m(R)}$$

⑤ $\mathrm{div}(f \circ [m]) = \mathrm{div}(g^m)$

$\Rightarrow \forall X \in E, \ S \in E[m]$

$$g(X+S)^m = c f([m]X + [m]S)$$

$$= c f([m]X)$$

$$= g(X)^m$$

$$\Rightarrow \boxed{\left(\frac{g(X+S)}{g(X)}\right)^m = 1}$$

⑥ 映射 $C \to P'$（即射影直线）

$$X \to \frac{g(X+S)}{g(X)}$$

的值是离散的 $\Rightarrow$ 是常值

⑦ 定义 Weil Pairing

$$\boxed{e_m(S,T) = g(X+S)/g(X)}$$

其中 $S, T \in E[m]$

$X \in E$ 为任意点，与具体选择无关

⑧ 性质

☆ $e_m(S_1+S_2,T) = e_m(S_1,T)\, e_m(S_2,T)$

$e_m(S,T_1+T_2) = e_m(S,T_1)\, e_m(S,T_2)$

☆ $e_m(T,T) = 1 \quad e_m(S,T) = \frac{1}{e_m(T,S)}$

☆ 非退化，即不是常值函数

有效计算 Weil Pairing

用另外一个等价定义

$$e_m(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{f_Q(P-S)}{f_Q(-S)}$$

其中 $S \in E$ 且 S不在 P,Q 生成子群中

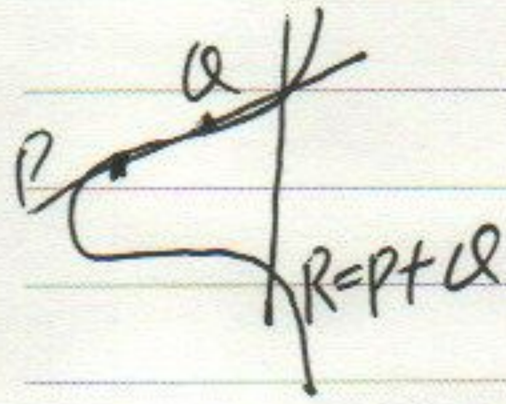
所以计算 $e_m(P,Q) \Rightarrow$ 计算 $f_P(X)$

其中 $\boxed{div(f_P) = m(P) - m(O)}$

有效算法核心

① double & add 算法

② 秘术



$$h_{P,Q} = \begin{cases} \dfrac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2} & \lambda \neq 0 \\ x - x_P & \lambda = 0 \end{cases}$$

$$\Rightarrow div(h_{P,P}) = 2(P) - (2P) - (O)$$

$$div(h_{P,Q \neq P}) = (P) + (Q) - (P+Q) - (O)$$

计算 $\mathrm{div}(f_p)$. 用例子

令 $m=9$. 计算 ~~f~~ $\mathrm{div}(f_p) = 9(p) - 9(0)$

即 $\boxed{\mathrm{div}(f_p) = 9(p) - (9p) - 8(0)}$

$h_{8p,p} \Rightarrow (8p) + (p) - (9p) - (0)$

$h_{4p,4p} \Rightarrow 2(4p) \cancel{+(p)} - (8p) - (0)$

$h_{2p,2p} \Rightarrow 2(2p) - (4p) - (0)$

$h_{p,p} \Rightarrow 2(p) - (2p) - (0)$

$\Downarrow$

$f_p = h_{8p,p} \cdot h_{4p,4p} \cdot h_{2p,2p}^{2} \cdot h_{p,p}^{4}$