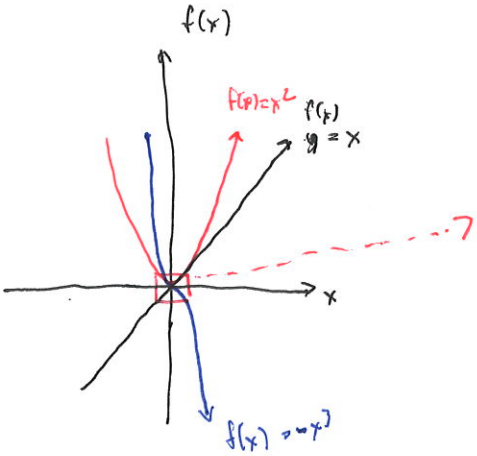
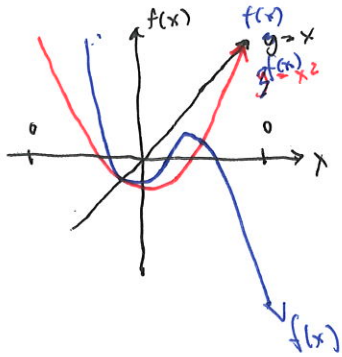
[Washington, Chapter 11]

Divisor



All functions are zeros when x=0. However, their zeros are slightly different.



cut for one time

cut for 2 times

$f(x) = -x^3$ cut for 3 times

$\text{div}(x) = [0]$

$\text{div}(x^2) = 2[0]$

$\text{div}(x^3) = 3[0]$

$\text{ord}_0(x) = 1$

$\text{ord}_{f0}(x^2) = 2$

$\text{ord}_0(x^3) = 3$

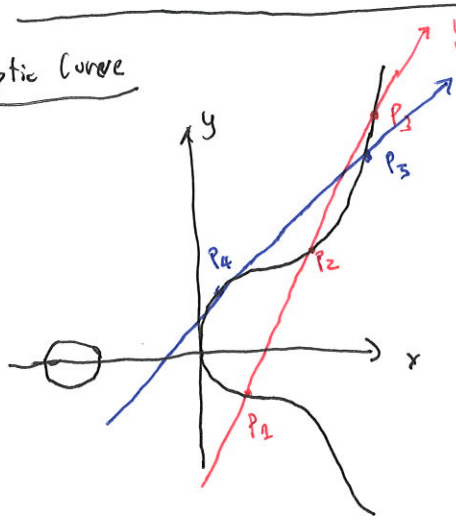
$\text{ord}_0\left(\frac{1}{x}\right) = -1$

$\text{ord}_0\left(\frac{1}{x^2}\right) = -2$

$\text{ord}_0\left(\frac{1}{x^3}\right) = -3$

$f(x) \to \infty$ poles

Elliptic Curve



$f(P) = f((x,y)) = y - mx - c$

$\in \mathbb{E}(\mathbb{F}_p)$

$\text{ord}_{P_1}(y-mx-c) = 1$

$\text{ord}_{P_2}(y-mx-c) = 1$

$\text{ord}_{P_3}(y-mx-c) = 1$

$\text{ord}_{P_4}(y-mx-c') = 2$

$\text{ord}_{P_5}(y-m'x-c') = 1$

Divisor of f = $\text{div}(f) = \sum_{P:\text{zeros or poles}} \text{ord}_P(f) \cdot [P]$

$\text{div}(y-mx-c) = [P_1] + [P_2] + [P_3] - 3[\infty]$ → very technical → skip in this class

$\text{div}(y-m'x-c') = 2[P_4] + [P_5] - 3[\infty]$ →

Properties of divisor

1. $\text{div}(f \cdot g) = \text{div}(f) + \text{div}(g)$

   Ex $\underbrace{\text{div}(x^2)}_{2[0]} = \underbrace{\text{div}(x)}_{[0]} + \underbrace{\text{div}(x)}_{[0]}$

   $\text{div}\left((y-mx-c)\cdot(y-m'x-c')\right) = [P_1] + [P_2] + [P_3] + 2[P_4] + [P_5] - 3[\infty]$

2. $\text{div}\left(\frac{f}{g}\right) = \text{div}(f) - \text{div}(g)$

   Ex $\underbrace{\text{div}(x)}_{[0]} = \underbrace{\text{div}(x^2)}_{2[0]} - \underbrace{\text{div}(x)}_{[0]}$

   $\text{div}\left(\frac{y-mx-c}{y-m'x-c'}\right) = [P_1] + [P_2] + [P_3] - 2[P_4] - [P_5]$

Example $E = \{(x,y) : y^2 = x^3 + 72\} \longrightarrow (-2,8) \in E$

$f(P) = f(x,y) = \frac{3}{4}(x+2) - y + 8 \longrightarrow$ The function is zero at $(-2,8)$

$\text{ord}_{(-2,8)}\left(\frac{3}{4}(x+2) - y + 8\right) = ?\ 2$

$y^2 = x^3 + 72$

$y^2 - 64 = x^3 + 8$

$(y-8)\cdot(y+8) = (x+2)(x^2-2x+4)$

$y - 8 = \frac{(x+2)}{y+8}(x^2-2x+4)$

$\frac{3}{4}(x+2) - (y-8)$

$= \frac{3}{4}(x+2) - \frac{(x+2)}{y+8}(x^2-2x+4)$

$= (x+2)\left[\frac{3}{4} - \frac{x^2-2x+4}{y+8}\right]$

one zero. 0

$= \frac{(x+2)}{y+8}\left[3y+24 - 4x^2 + 8x - 16\right]$

$= \frac{(x+2)}{y+8}\left[3y - 24 - 4x^2 + 8x + 32\right]$

$= \frac{(x+2)}{y+8}\left[3(y-8) - 4(x+2)(x-4)\right]$

$= \frac{(x+2)}{y+8}\left[3\frac{(x+2)}{y+8}(x^2-2x+4) - 4(x+2)(x-4)\right]$

2 zeros

$= \frac{(x+2)^2}{y+8}\left[3\frac{x^2-2x+4}{y+8} - 4(x-4)\right]$

not zeros any more.

Bonus Question

What is $\text{div}\left(\frac{3}{4}(x+2) - y + 8\right)$?

Theorem For any divisor $a_1[P_1] + a_2[P_2] + \cdots + a_n[P_n]$ such that $a_1 + \cdots + a_n = 0$ and $a_1 \cdot P_1 \oplus a_2 \cdot P_2 \oplus \cdots \oplus a_n P_n = \infty$, there exists a rational function f such that $\text{div}(f) = a_1[P_1] + \cdots + a_n[P_n]$.

Proof Consider a line between P_1 and P_2. The line also passes $[\neg(P_1 \oplus P_2)]$. Suppose that the line is $y - mx - c = 0$. We have.

negative of $P_1 \oplus P_2$

$\text{div}(y - mx - c) = [P_1] + [P_2] + [\neg(P_1 \oplus P_2)] - 3[\infty]$

Now, consider a line between $[\neg(P_1 \oplus P_2)]$ and $[P_1 \oplus P_2]$. Suppose that the line is $x - x' = 0$

$\text{div}(x - x') = [P_1 \oplus P_2] + [\neg(P_1 \oplus P_2)] - 2[\infty]$

Then,

$\text{div}(y - mx - c) - \text{div}(x - x') = [P_1] + [P_2] + [\neg(P_1 \oplus P_2)] - 3[\infty] - [P_1 \oplus P_2] - [\neg(P_1 \oplus P_2)] + 2[\infty]$

$\text{div}\left(\frac{y - mx - c}{x - x'}\right) = [P_1] + [P_2] - [P_1 \oplus P_2] - [\infty]$

$[P_1] + [P_2] = [P_1 \oplus P_2] + [\infty] + \text{div}\left(\frac{y - mx - c}{x - x'}\right)$.

2 zeros 1 zero

- The # zeros is reduced by 1

$a_1[P_1] + a_2[P_2] + \cdots + a_n[P_n] \longrightarrow [a_1P_1 \oplus \cdots \oplus a_nP_n] + \overline{-1}[\infty] + \operatorname{div}(\text{something})$

after many steps $[\infty]$ cancel

$\longrightarrow \operatorname{div}(\text{something})$ □

Example $E(\mathbb{F}_{11}) = \{(x,y) \in \mathbb{F}_{11}^2 : y^2 = x^3 + 4x\}$

$[(0,0)] + [(2,4)] + [(4,5)] + [(6,3)] - 4[\infty]$

$= [(0,0) \oplus (2,4)] + [\infty] + \operatorname{div}\left(\frac{y-2x}{x-2}\right) + [(6,3)] + [(4,5)] - 4[\infty]$

$= [(2,4) \oplus (4,5)] + [(6,3)] - 3[\infty] + \operatorname{div}\left(\frac{y-2x}{x-2}\right)$

$= [(6,8)] + [\infty] + \operatorname{div}\left(\frac{y-10x-9}{x-6}\right) + [(6,3)] - 3[\infty] + \operatorname{div}\left(\frac{y-2x}{x-2}\right)$

$\operatorname{div}(x-6) = [(6,8)] + [(6,3)] - 2[\infty]$

$\operatorname{div}(x-6) + 2[\infty] = [(6,8)] + [(6,3)]$

$= \operatorname{div}(x-6) + 2[\infty] + \operatorname{div}\left(\frac{y-10x-9}{x-6} \cdot \frac{y-2x}{x-2}\right) - 2[\infty]$

$= \operatorname{div}\left(x-6, \frac{y-10x-9}{x-6} \cdot \frac{y-2x}{x-2}\right) = \operatorname{div}\left(\underbrace{\frac{(y-10x-9)\cdot(y-2x)}{x-2}}_{f}\right)$ □

Weil Pairing : We want to calculate $e(P,Q)$. f_P and f_Q be a function such that

$nP = \infty$, $nQ = \infty$

$\operatorname{div}(f_P) = n[P] - n[\infty]$, $\operatorname{div}(f_Q) = n[Q] - n[\infty]$.

we can use the above algorithm to calculate that as $n-n=0$ and $nP - n\infty = \infty$

We have $e(P,Q) = \dfrac{f_P(Q \oplus S)}{f_P(Q)} \Big/ \dfrac{f_Q(P \oplus S)}{f_Q(-S)}$ where $S \notin \{\infty, P, -Q, P \oplus -Q\}$.

Theorem

$e(P_1 \oplus P_2, Q) = e(P_1, Q) \cdot e(P_2, Q) \longrightarrow e(mP, Q) = e(P,Q)^m$

$e(P, Q_1 \oplus Q_2) = e(P, Q_1) \cdot e(P, Q_2) \longrightarrow e(P, mQ) = e(P,Q)^m$

Proof :

Weil reciprocity

$\operatorname{div}(f) = a_1[P_1] + \cdots + a_n[P_n]$

$\operatorname{div}(g) = b_1[Q_1] + \cdots + b_n[Q_n]$

$f(\operatorname{div}(g)) = f(P_1)^{b_1} \cdots f(P_n)^{b_n}$

$g(\operatorname{div}(f)) = g(Q_1)^{a_1} \cdots g(Q_n)^{a_n}$

$f(\operatorname{div}(g)) = g(\operatorname{div}(f))$