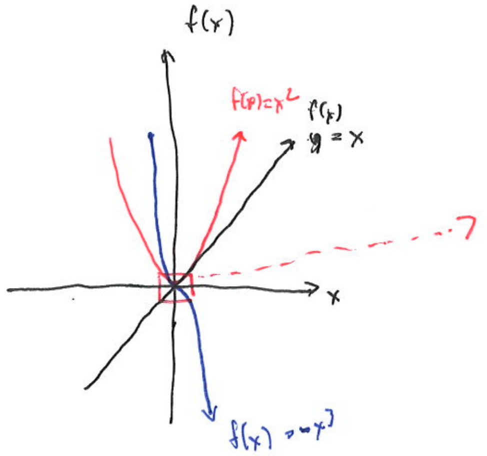
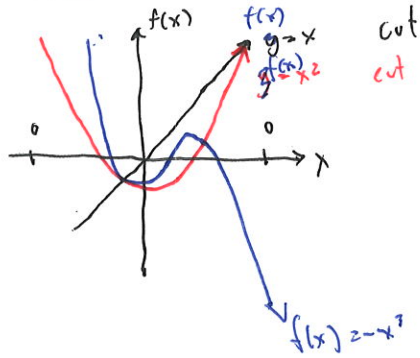
Divisor

[Washington, Chapter 11]



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



cut for one time

cut for 2 times

cut for 3 times

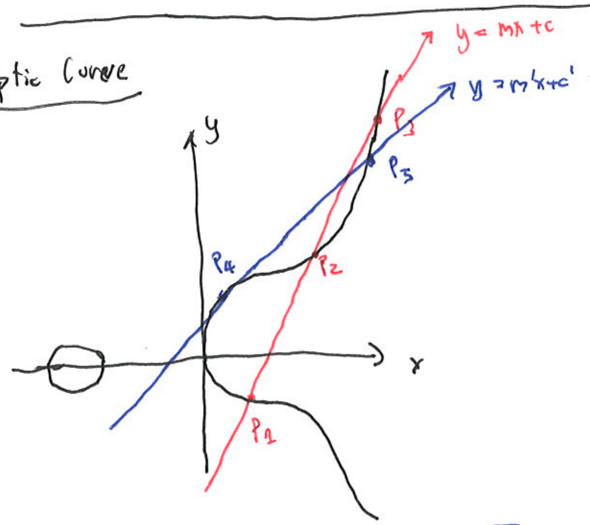
$\text{div}(x) = [0]$ $\qquad \text{ord}_0(x) = 1$ $\qquad \text{ord}_0\left(\frac{1}{x}\right) = -1$

$\text{div}(x^2) = 2[0]$ $\qquad \text{ord}_0(x^2) = 2$ $\qquad \text{ord}_0\left(\frac{1}{x^2}\right) = -2$

$\text{div}(x^3) = 3[0]$ $\qquad \text{ord}_0(x^3) = 3$ $\qquad \text{ord}_0\left(\frac{1}{x^3}\right) = -3$

$f(x) \to \infty$ poles

Elliptic Curve



$f(\underset{\in E(\mathbb{F}_p)}{P}) = f((x,y)) = y - mx - c$

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

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

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

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

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

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

$\text{div}(y-mx-c) = [P_1] + [P_2] + [P_3] - 3[\infty]$

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

very technical - skip in this class

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

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

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

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

$$\text{ord}_{(-2,8)}\left(\tfrac{3}{4}(x+2)-y+8\right)=\cancel{1}\ 2$$

$$y^2=x^3+72$$

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

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

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

Bonus Question

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

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

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

$$=\underbrace{(x+2)}_{\text{one zero.}}\underbrace{\left[\frac{3}{4}-\frac{x^2-2x+4}{y+8}\right]}_{0}$$

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

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

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

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

2 zeros

$$=\frac{(x+2)^2}{y+8}\underbrace{\left[3\frac{x^2-2x+4}{y+8}-4(x-4)\right]}_{\text{not zeros any more.}}$$

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

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

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

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,

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

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

$$\underbrace{[P_1]+[P_2]}_{2\text{ zeros}}=\underbrace{[P_1\oplus P_2]}_{1\text{ zero}}+[\infty]+\text{div}\left(\frac{y-mx-c}{x-x'}\right).$$

- The # zeros is reduced by 1

$$a_1[P_1] + a_2[P_2] + \dots + a_n[P_n] \xrightarrow{\text{after many steps}} [\underbrace{a_1P_1 \oplus \dots \oplus a_nP_n}_{[\infty]}] \underbrace{+ -1[\infty]}_{\text{cancel}} + \mathrm{div}(\text{something})$$

$$\longrightarrow \mathrm{div}(\text{something}) \qquad \square$$

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

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

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

$$= [(2,7)] + [(4,5)] + [(6,3)] - 3[\infty] + \mathrm{div}\left(\frac{y-2x}{x-2}\right)$$

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

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

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

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

$$= \mathrm{div}\left(\cancel{x-6} \cdot \frac{y-10x-9}{\cancel{x-6}} \cdot \frac{y-2x}{x-2}\right) = \mathrm{div}\left(\underbrace{\frac{(y-10x-9)\cdot(y-2x)}{x-2}}_{f}\right) \qquad \square$$

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

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

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

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

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

<u>Theorem</u>

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

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

<u>Proof</u>: ~~$f_{P_1 \oplus P_2}$ ... $= n[P_1 \oplus P_2] - n[\infty]$~~

Weil reciprocity

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

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

$$f(\mathrm{div}(g)) = f(P_1)^{a_1} \dots f(P_n)^{a_n}$$

$$g(\mathrm{div}(f)) = g(Q_1)^{b_1} \dots g(Q_n)^{b_n}$$

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

$$e(P_1 \oplus P_2, Q) = e(P_1, Q)\cdot e(P_2, Q)$$

$$\frac{f_{P_1\oplus P_2}(Q\oplus S)}{f_{P_1\oplus P_2}(S)} \Big/ \frac{f_Q(P_1\oplus P_2\oplus \neg S)}{f_Q(S)} = \left(\frac{f_{P_1}(Q\oplus S)}{f_{P_1}(S)} \Big/ \frac{f_Q(P_1\oplus \neg S)}{f_Q(\neg S)}\right)\cdot\left(\frac{f_{P_2}(Q\oplus S)}{f_{P_2}(S)} \Big/ \frac{f_Q(P_2\oplus \neg S)}{f_Q(\neg S)}\right)$$

$$= \frac{f_{P_1}(Q\oplus S)\cdot f_{P_2}(Q\oplus S)}{f_{P_1}(S)\, f_{P_2}(S)} \Big/ \frac{f_Q(P_1\oplus \neg S)\, f_Q(P_2\oplus \neg S)}{f_Q(\neg S)\cdot f_Q(\neg S)}$$

$$\boxed{\frac{f_{P_1\oplus P_2}(Q\oplus S)}{f_{P_1}(Q\oplus S)\cdot f_{P_2}(Q\oplus S)} \Big/ \frac{f_{P_1\oplus P_2}(S)}{f_{P_1}(S)\, f_{P_2}(S)}} = \frac{f_Q(P_1\oplus P_2\oplus \neg S)\cdot f_Q(\neg S)\cdot \cancel{f_Q(\neg S)}}{f_Q(P_1\oplus \neg S)\, f_Q(P_2\oplus \neg S)\cdot \cancel{f_Q(\neg S)}}$$

$$F_{P_1,P_2}(X) = \frac{f_{P_1\oplus P_2}(X)}{f_{P_1}(X)\cdot f_{P_2}(X)}$$

$$\mathrm{div}(F_{P_1,P_2}) = \mathrm{div}(f_{P_1\oplus P_2}) - \mathrm{div}(f_{P_1}) - \mathrm{div}(f_{P_2})$$
$$= n[P_1\oplus P_2] - \cancel{n[\infty]} - n[P_1] + \cancel{n[\infty]} - n[P_2] + n[\infty]$$
$$= n[P_1\oplus P_2] - n[P_1] - n[P_2] + n[\infty]$$

Suppose that G_{P_1,P_2} be a function such that $\mathrm{div}(G_{P_1,P_2}) = [P_1\oplus P_2] - [P_1] - [P_2] + [\infty]$

$$\therefore\ F_{P_1,P_2} = G^n_{P_1,P_2}$$

$$\frac{G^n_{P_1,P_2}(Q\oplus S)}{G^n_{P_1,P_2}(S)} = G_{P_1,P_2}(n[Q\oplus S] - n[S]) \longrightarrow f_{Q,S} \text{ be a function such that}$$

$$\mathrm{div}(f_{Q,S}) = n[Q\oplus S] - n[S]$$
$$f_{Q,S}(X) = f_Q(X\oplus S)$$

$$= G_{P_1,P_2}(\mathrm{div}(f_{Q,S}))$$
$$= f_{Q,S}(\mathrm{div}(G_{P_1,P_2})) = f_{Q,S}([P_1\oplus P_2] - [P_1] - [P_2] + [\infty])$$
$$= \frac{f_{Q,S}(P_1\oplus P_2)\cdot f_{Q,S}(\infty)}{f_{Q,S}(P_1)\cdot f_{Q,S}(P_2)} = \boxed{\frac{f_Q(P_1\oplus P_2\oplus\neg S)\cdot f_Q(\neg S)}{f_Q(P_1\oplus\neg S)\cdot f_Q(P_2\oplus\neg S)}} \quad ▯$$

right side

How to find f such that $\mathrm{div}(f) = n[P] - n[\infty]$ when n is large? — Miller's Algorithm

Suppose that $n = 57 = 32 + 16 + 8 + 1$.

- $y - m_1 x - c_1$ be a line touching the elliptic curve at $P = (x_1, y_1)$, and $2P = (x_2, y_2)$

$$\mathrm{div}(y - m_1 x - c_1) = 2[P] + [\neg 2P] - 3[\infty]$$
$$\mathrm{div}(x - x_2) = [2P] + [\neg 2P] - 2[\infty]$$
$$\mathrm{div}\left(\frac{y - m_1 x - c_1}{x - x_1}\right) = 2[P] - [2P] - [\infty]$$
$$2[P] = [2P] + [\infty] + \mathrm{div}\left(\frac{y - m_1 x - c_1}{x - x_1}\right)$$
$$[2P] = 2[P] - [\infty] - \mathrm{div}\left(\frac{y - m_1 x - c_1}{x - x_1}\right)$$

- $y - m_2 x - c_2$ be a line touching at $2P = (x_2, y_2)$ and $4P = (x_4, y_4)$

$$\mathrm{div}(y - m_2 x - c_2) = 2[2P] + [-4P] - 3[\infty]$$

$$\mathrm{div}(x - x_4) = [-4P] + [4P] - 2[\infty]$$

$$\mathrm{div}\left(\frac{y - m_2 x - c_2}{x - x_4}\right) = 2[2P] - [4P] - [\infty]$$

$$[4P] = 2[2P] - [\infty] - \mathrm{div}\left(\frac{y - m_2 x - c_2}{x - x_4}\right)$$

$$= 2\left[2[P] - [\infty] - \mathrm{div}\left(\frac{y - m_1 x - c_1}{x - x_1}\right)\right] - [\infty] - \mathrm{div}\left(\frac{y - m_2 x - c_2}{x - x_4}\right)$$

$$= 4[P] - 3[\infty] - \mathrm{div}\left(\left(\frac{y - m_1 x - c_1}{x - x_1}\right)^2 \left(\frac{y - m_2 x - c_2}{x - x_4}\right)\right)$$

$$[32P] = 32[P] - 31[\infty] - \mathrm{div}(\quad)$$

$$[16P] = 16[P] - 15[\infty] - \mathrm{div}(\quad)$$

$$[8P] = 8[P] - 7[\infty] - \mathrm{div}(\quad)$$

$$[P] = [P]$$

$$[\cancel{57}P] = 57[P] - 56[\infty] - \mathrm{div}(\quad)$$

Merge using the same technique

$$\mathrm{div}(\quad) = 57[P] - 57[\infty]$$

Reading for final

- Chapter 11.1 of [Dwork et al]
- Papers on l-diversity, k-anonymity, and t-closeness
- Appendix A–C of [Washington] (in case that you are not familiar with abstract algebra)
- Chapter 1, 2.1–2.3, 2.6, 4.1, 5.2, 6.1, 6.2, 6.4, 11.1–2, 11.4 of [Washington]