Contents

1 Order of Vanishing and Intersection Multiplicity

Order of vanishing simply means the intersection multiplicity of a point that when evaluated on E is zero or a pole.

2 Divisors

$$f(x) = (x-a)^3(x-b)^5$$
$$\operatorname{div}(f) = 3[a] + 5[b] - 8[\infty]$$

3 Weil Pairing

$$n \mid \operatorname{char}(K)$$

There exists f such that

$$\operatorname{div}(f) = n[T] - n[\infty]$$

because by theorem 11.2, $\deg(D) = 0, \operatorname{sum}(D) = \infty \implies \exists f : \operatorname{div}(f) = D$.

Likewise for

$$\begin{aligned} \operatorname{div}(g) &= \sum_{R \in E[n]} ([T' + R] - [R]) \\ &= \sum_{R \in E[n]} [T' + R] - \sum_{nR = \infty} [R] \end{aligned}$$

Now we want to show that given an $T' \in E[n^2]$ such that $nT' = T$ then

$$\{T'' : nT'' = T\} = \{T' + R : R \in E[n]\}$$

This is equivalent to the statement that given any $T'' \in E[n^2]$ then

$$T'' = T' + R : R \in E[n]$$

$$\alpha : E[n^2] \to E[n]$$
$$\alpha(T'') = nT''$$
$$[E[n^2] : E[n]] = n^2$$
$$\ker \alpha = E[n]$$
$$T_1'', T_2'' \in E[n^2] : nT_1'' = nT_2'' = T \implies T_1'' \in T_2'' + E[n]$$

which proves the statement from before. Therefore

$$\sum_{R \in E[n]} [T' + R] = \sum_{nT'' = T} [T'']$$

Now given

$$\mathrm{div}(f) = n[T] - n[\infty]$$

We want to show that

$$\mathrm{div}(f \circ n) = n \left(\sum_{R \in E[n]} [T' + R] \right) - n \sum_{R \in E[n]} [R]$$

3.1 Function Composition with Multiplication by n Map

$$P \to nP \to f(nP)$$

$T' + R$ generates the group of all $T'' : nT'' = T$.

$f(T) = 0 \implies f \circ n(T'') = 0$.

See here and Silverman's Proposition II.2.6(c).

Also import from Knapp's book page 316:

$$\mathrm{ord}_x(f) = \mathrm{ord}_{\psi(x)}(f \circ \psi^{-1})$$

Using this we see that

$$\mathrm{ord}_{T'}(f \circ n) = \mathrm{ord}_{nT'}(f \circ n \circ n^{-1})$$

4 Tate Pairing

ϕ is the qth power Frobenius. Since $\phi(D) = D$, the points are pemuted without changing the divisor. Since the points satisfy $f(P)$, so $f \in \mathbb{F}_q[x, y]$, and hence $\phi(f) = f$.

5 Computation of Pairings

5.1 Calculating Divisors

$3D = 3[(0, 3)] - 3[\infty]$ is easy. We just use the horizontal line that cuts through $(0, 3)$. So $3D = \mathrm{div}(y - 3)$.

Sage code to see points of intersection with the curve:

```
sage: R.<x, y> = PolynomialRing(GF(7))
sage: I = Ideal(y^2 - x^3 - 2, y - 3)
sage: I.variety()
[{y: 3, x: 0}]
```

As expected. We can also observe that the gradient of the line is 0, which is tangent to the curve at this point.

For the divisor

$$3D_{(5,1)} = 3[(3, 6)] - 3[(6, 1)]$$

Observe that the tangent to the curve is calculated by

$$y' = \frac{3x^2}{2y}$$

So we see that $y'_{(3,6)} = 4$ and that $y = 4x + 1$ is tangent to $(3, 6)$. Likewise $y'_{(6,1)} = 5$ and $y = 5x - 1$ is tangent to $(6, 1)$

$$\implies \mathrm{div}\left(\frac{4x - y + 1}{5x - y - 1}\right) = 3[(3, 6)] - 3[(6, 1)]$$

5.2 Miller Loop Divisors

$$D_j = j[P + R] - j[R] - [jP] - [\infty]$$
$$\mathrm{div}(ax + by + c) = [jP] + [kP] + [-(j + k)P] - 3[\infty]$$
$$\mathrm{div}(x + d) = [(j + k)P] + [-(j + k)P] - 2[\infty]$$
$$\mathrm{div}\left(\frac{ax + by + c}{x + d}\right) = [jP] + [kP] - [(j + k)P] - [\infty]$$

$$D_{j+k} = (j+k)[P+R] - (j+k)[R] - [(j+k)P] + [\infty]$$

$$\begin{aligned} D_j + D_k &= j[P+R] + k[P+R] - j[R] - k[R] - [jP] - [kP] + 2[\infty] \\ &= (j+k)[P+R] - (j+k)[R] - [jP] - [kP] + 2[\infty] \end{aligned}$$