Miller Algorithm computes a function whose divisor is \( l'(p) - t'(6) \) with the intermediate function

\[
f_i, p \quad \text{such that} \quad \text{div} \left( f_i, p \right) = i(p) - (i+1)(6)
\]

of degree 0 and sum 0.

Note that \( f_i, p \) has divisor \( \text{div} \left( f_i, p \right) = i(p) - (i+1)(6) = 0 \).

In other words, \( f_i, p \) has no zero and no pole \( \Rightarrow \) this is a constant of the field.

So we can just take \( f_i, p = 1 \).

(See also prop. 11.1 in Washington's book).

We aim at computing the function \( q \) s.t. \( \text{div}(q) = l(p) - l(6) \).

But there is no function of divisor \( (p) - (6) \) on \( E \) : the simple functions are lines and tangents but because of Bezout's theorem, there are three points counted with multiplicity that intersect a line and the curve.

\[
\text{div} \left( l_{i, q} \right) = (p) + (q) + (-p+q) - 3(6).
\]

\[
\text{div} \left( l_{p, p} \right) = 2(p) + (-2p) - 3(6).
\]

\[
\text{div} \left( v_{p, p} \right) = (p) + (-p) - 2(6) \quad \text{(also valid if} \ P \text{ has order 2 : vertical tangent)}
\]

Miller step:

\[
f_{i+j}, p = f_i, p \cdot f_j, p \quad \text{line through i and j} \quad \text{tangent of} \quad i = j.
\]

\[
v_{(i+j)^p} \text{ is vertical at } (i+j)^p
\]

(See lecture of Week 5 Thursday, March 3, and Washington's book chapter 11).
From (reduced) Tate pairing to ate pairing

see Galbraith's chapter IX on pairings (week 11 PDF).

Let $E$ be an elliptic curve defined over $l(E_q)$ with a subgroup of order $l$, $l \mid \#E(l(E_q))$ but $l \nmid q - 1$ and $l^2 \nmid \#E(l(E_q))$, $(E[l], \mathbb{F}_l)$ and the embedding degree of $l$ with respect to $q$ is $n$.

**Th. IX.9** Let $P \in E(l(E_q))$ of order $l$ and $Q \in E(l(E_q))$.

\[
(e_{Tate}, l(P, Q)) \frac{p^m - 1}{l} = (e_{Tate}, N(P, Q)) \frac{p^m - 1}{N}
\]

for $N$ a multiple of $l$, and $N \mid p^m - 1$.

**Proof.** Write $N = h \cdot l$ for some cofactor $h$, and assume $h$ is coprime to $l$.

The Tate pairing is

\[
(g(Q)) \frac{p^m - 1}{l} = (g(Q))^h \frac{p^m - 1}{N} = (g^h(Q)) \frac{p^m - 1}{N}
\]

What is $g^h$? a function whose divisor is $h(l(P) - l(Q)) = N(P) - N(Q)$

\[
\Rightarrow \qquad e_{Tate}, N(P, Q) \frac{p^m - 1}{N}
\]

It holds because $lP = O \Rightarrow NP = O$.

Now, let's consider $N = gcd(T^m - 1, p^m - 1)$ where $T = t - 1$.

We have $l \mid N$ because
1) $l \mid p^m - 1$ by assumption, and
2) $l \mid T^{m-1} = (t-1)^{m-1}$ because actually $l \mid q_{n}(t-1)$ and $q_{m}(t-1) \mid (t-1)^m$.

\[
\Rightarrow \qquad \text{we can replace } l \text{ by } N \text{ in the Tate pairing. Denote } T^{m-1} = C N.
\]

Let $\mathbf{f}$ denote a Hilbert function $\mathbf{div}(\mathbf{f}_{i,P}) = \mathbf{i}(P) - \mathbf{v}(P) - \mathbf{i}(O)$.

\[
\mathbf{div} \left( f_{T^{m-1}, Q} \right) = \left( T^{m-1}(Q) - \left( T^{m-1}(Q) \right) \right) - \left( T^{m-2}(0) \right) = \left( T^{m-1}(Q) - \left( T^{m-1}(Q) \right) \right)
\]

\[
= C \cdot (N(Q) - N(O))
\]

\[
f_{T^{m-1}, Q} = g^C_{N} \quad \text{where } \mathbf{div}(g_{N}) = N(Q) - N(O).
\]

\[
\left( f_{T^{m-1}, Q} \right) \frac{p^m - 1}{N} = \left( f_{N, Q} \right) \frac{p^m - 1}{N} = C = \left( e_{Tate, N}(Q, P) \right) \frac{p^m - 1}{N} \cdot C.
\]
Finally, let's simplify $f_{T^{m-1}, Q}(P)$.

$$\text{div } (f_{T^{n}, Q}(P)) = T^n(Q) - (T^n Q) - (T^{n-1})(0)$$

where $(T^{n-1}) Q = 0$, hence $T^n Q = Q$.

$$\text{div } (f_{T^{n}, Q}(P)) = T^n(Q) - (Q) - (T^{n-1})(0)$$

$$= (T^{n-1})(Q) - (T^{n-1})(0)$$

$$= \text{div } (f_{T^{n-1}, Q})$$

We need: $f_{ab, Q} = f_{a, Q} b f_{b, [a] Q}$ where $f$ is a Hillel function.

$$\text{div } (f_{ab, Q}) = ab(Q) - (a b Q) - (ab - 1)(0)$$

$$= b \left( a(Q) - (a Q) - (a - 1)(0) \right)$$

$$+ b (a Q) - (ab Q) - (b - 1)(0) = \text{div } (f_{a, Q}) + \text{div } (f_{b, a Q})$$

$$\text{div } (f_{b, a Q}) = b (a(Q) - (a Q) - (a - 1)(0)) = ab(Q) - b(a Q) - (ab - b)(0)$$

$$\text{div } (f_{b, a Q}) = b (a Q) - (ab Q) - (b - 1)(0)$$

Let's decompose $T^n = T \cdot T^{n-1} = T \cdot T \cdot T^{n-2}$.

$$f_{T^{n}, Q} = f_{T, Q} f_{T^{n-1}, LTI Q}$$

$$= f_{T, Q} f_{T^{n-2}, LTI Q} f_{T^{n-2}, [T^2] Q}$$

$$= \cdots f_{T, Q} f_{T^{n-2}, LTI Q} f_{T^{n-3}, [T^2] Q} \cdots f_{T, [T^{n-1} Q]}$$

Note that $L \not\ni T^{n-1}$ nor $T^{n-2}$.

Finally, we need a special property on $[T^2] Q$. : $[T] Q = [Q] Q = \Pi_q(Q)$.

and $f_{a, \Pi_q(Q)} = f_{a, Q}$

$$\Rightarrow f_{T, [T^2] Q} = f_{T, Q}$$

and $f_{T^n, Q} = f_{T^n, \Pi_{q^2}} f_{T^n, q^2} f_{T^n, q} f_{T^n, 1} = f_{T^n, q} \cdots f_{T, Q}$

$$f_{T^n, Q} = f_{T, Q}$$ for some constant $c$. 


Finally, we need \( \mathcal{E}_g \) and the trace-0 subgroup.

Remember that there are \( l+1 \) distinct subgroups of order \( l \) over \( \mathbb{F}_p \).

\( G_1 \) is the only choice of \( \mathbb{F}_q \)-subgroup: \( E(\mathbb{F}_q)[l] = G_1 \).

We have many choices for \( G_2 \) and one of them will provide us with

\[ \Pi q(Q) = [q]^3 Q. \]

First, \( Q \notin E(\mathbb{F}_q) \) hence \( \Pi q \) is not the identity on \( Q \).

Then, writing \( \Pi q(Q) = [q]^3 Q \) means we want \( G_2 \) to be "orthogonal" to \( G_1 \) with respect to the Frobenius endomorphism, that is, the matrix representing \( \Pi q \) will be diagonal over \( \mathbb{Z}/l\mathbb{Z} \).

\[ \Pi q \leftrightarrow M = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \text{ in the basis } (G_1, G_2). \]

This would mean \( \Pi q(Q) = [q]^3 Q \).

\( \chi_q = X^2 - tX + q \) is the characteristic polynomial of \( \Pi q \) and \( M \).

Let's factor it mod \( l \): \( (X-t)(X-q) = X^2 - (t+q)X + q \) indeed.

Because \( l \mid q+1-t \iff q+1 \equiv -t \mod l \).

(in all generality: with \( l \mid q+1-t, M = \begin{pmatrix} 1 & q \\ 0 & q \end{pmatrix} \).

So there exists one choice of \( G_2 \) such that \( \Pi q(Q) = [q]^3 Q \forall Q \in G_2 \).

Finally, \( f_q a, \Pi q(Q)(p) = f_q a, a, a(p) \) as long as \( P \in E(\mathbb{F}_q) \) is fixed by \( \Pi q \).

Trace-0 subgroup. Galbraith's chapter IX, § 14.7.4.

\[ \text{Tr}(Q) = \sum_{\sigma \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(Q) \quad = \sum_{i=0}^{n-1} (x^{q^i}, y^{q^i}). \]

\( \text{Tr}(Q) \in E(\mathbb{F}_q) \) even if \( Q \in E(\mathbb{F}_{q^m}) \).

Define \( Q = [n]Q \sim \text{Tr}(Q) \) where \( n \) is the embedding degree.

\[ \text{Tr}(Q) = \text{Tr}(Q^n) - \text{Tr}(\text{Tr}(Q)) = [n] \text{Tr}(Q) - \sum_{i=0}^{n-1} \Pi q^i(\text{Tr}(Q)) \]

\( = [n] \text{Tr}(Q) - [n^2] \text{Tr}(Q) = 0 \).
Lemma 1X.16. Let $E$ be a finite field of characteristic $p$ and let $E$ be a finite field extension of $F_p$. Let $m$ be a positive integer. Then the trace zero subgroup of order $l$ of $E/F_p$ is defined as:

\[ C = \{ Q \in E(F_p^m)[l] : Tr(Q) = 0 \} \]

\[ = \{ Q \in E(F_p)[l] : \pi_q(Q) = [qI]Q \} \]

where $\pi_q$ is the $q$-th power Frobenius automorphism.

Then $C$ is the trace-zero subgroup of order $l$ and $C$ is cyclic.

Proof:

1. If $Q \in E(F_q)$ then $Tr(Q) = \sum_{i=0}^{n-1} \pi_i^q(Q) = q^m Q - q^m (q^n - 1) = 0$.

2. For $Q \in E(F_q)[l]$, $Tr(Q) = \sum_{i=0}^{l-1} \pi_q(Q) = [qI]Q = 0$.

Now consider the 2nd def of $C$: \{ $Q \in E(F_p^m)[l]$ : $\pi_q(Q) = [qI]Q$ \}.

Let $Q_2$ a generator of the subgroup of order $l$ of $E(F_q)$ such that $\pi_q(Q_2) = [qI]Q_2$.

$\pi_q(Q_2) = \sum_{i=0}^{n-1} \pi_i^q(Q_2) = \sum_{i=0}^{n-1} [q^i]Q_2 = [1 + q + q^2 + \ldots + q^{n-1}]Q_2$

But note that $q^{n-1} = (q-1)(1 + q + q^2 + \ldots + q^{n-1})$.

And $l \mid q^n - 1$ but $l \nmid q - 1$ hence $l \mid 1 + q + q^2 + \ldots + q^{n-1}$ and $Tr(Q_2) = 0$.

So $Q_2 \in C$ (1st definition). \( \square \)