Omdat de berekeningen tot aan (16) (die de gevalsonderscheiding 1 of 2 bepaalt) goed lijken te zijn zal ik hier de berekeningen van case 1 en case 2 apart behandelen:
We zullen in de rest van deze tekst de volgende conventie aanhouden:

$$S := x^3 + Ax + B$$

1 Case 1

l is een vast gekozen priemgetal. Ook ga ik ervan uit dat $(\frac{q}{l}) = 1$ en dat $0 < w < l$ gekozen is zdd $w^2 \equiv q \bmod l$.
Allereerst moet er gecheckt worden of er een niet nul punt $P \in E[l]$ is zdd $\phi_l(P) = \pm wP$.
Dit komt dus neer op het checken dat de x-coordinaten gelijk zijn. Dit ga ik nu doen voor het geval dat w even en oneven is.

- (w is even.) Als $P = (x, y) \in E[l]$, dan is de x-coordinaat van $\phi_l(P) = x^q$ en de x-coordinaat van $wP = x - \frac{\psi_{w-1}\psi_{w+1}}{\psi_w^2}$. Dus (na reductie van de formules ψ:) moeten we volgende vergelijking uitwerken:

  $$x^q = x - \frac{\psi'_{w-1}\psi'_{w+1}}{\psi'^2_w}$$

  Oftewel, met behulp van (6) uit het algorithme:

  $$x^q = x - \frac{f_{w-1}f_{w+1}}{y^2 f_w^2}$$

  En dit geeft de formule van (17), waarvan we de de ggd met f_l moeten berekenen.

- (w is oneven.) Dit komt neer op De volgende vergelijking uitwerken:

  $$x^p = x - \frac{\psi_{w-1}\psi_{w+1}}{\psi_w^2} = x - \frac{\psi'_{w-1}\psi'_{w+1}}{\psi'^2_w} = x - \frac{y^2 f_{w-1}f_{w+1}}{f_w^2}$$

  Dit geeft dus precies de tweede vergelijking uit (17).

Als deze ggd berekend is en niet gelijk aan 1 is, moet worden gecheckt of $\phi_l P = wP$ voor een $P \in E[l]$. Als dit het geval is, dan geldt dat $t \equiv 2w \bmod l$ en anders $t \equiv -2w \bmod l$.
Checken of $\phi_l P = wP$ komt neer op checken of de y-coordinaten overeen komen.

- (w is even.) We moeten de volgende vergelijking uitwerken en de ggd met f_l nemen (wederom zijn de formules ψ al gereduceerd:

  $$y^q = \frac{\psi'_{w+2}\psi'^2_{w-1} - \psi'_{w-2}\psi'^2_{w+1}}{4y\psi'^3_w} = \frac{y(f_{w+2}f_{w-1}^2 - f_{w-2}f_{w+1}^2)}{4y^4 f_w^3}$$

Dit uitwerken en reduceren geeft dus volgende formule:

$$4S^{\frac{q+3}{2}}f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2$$

waarvan de ggd met f_l genomen moet worden.

- (w is oneven.) Dit komt neer op het uitwerken van de volgende gelijkheid:

$$y^q = \frac{\psi'_{w+2}\psi'^2_{w-1} - \psi'_{w-2}\psi'^2_{w+1}}{4y\psi'^3_w} = \frac{y^2(f_{w+2}f_{w-1}^2 - f_{w-2}f_{w+1}^2)}{4yf_w^3}$$

Dit uitwerken en reduceren levert de volgende formule:

$$4S^{\frac{q-1}{2}}f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2$$

2 Case 2

Hier moet gecheckt worden voor welke $0 < \tau < l$ geldt dat $\phi_l^2(P) + kP = \tau\phi_l(P)$ voor alle $P \in E[l]$ ($k \equiv q \bmod l$)
Nu geldt voor $P = (x, y)$ dat

$$\phi_l^2(P) + kP = (-x^{q^2} - x + \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2} + \lambda^2, -y^{q^2} - \lambda(-2x^{q^2} - x + \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2} + \lambda^2))$$

waar

$$\lambda = \frac{\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2 - 4y^{q^2+1}\psi_k^3}{4\psi_k y((x - x^{q^2})\psi_k^2 - \psi_{k-1}\psi_{k+1})} = \frac{\alpha}{\beta}$$

En $\tau\phi_l(P) = (x^q - (\frac{\psi_{\tau+1}\phi_{\tau-1}}{\psi_\tau^2})^q, (\frac{\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2}{4y\psi_\tau^3})^q)$
Vanwege efficientie van het algoritme is het wederom handig om de formules f te gebruiken in plaats van ψ.
Hieronder volgen de verkregen formules voor α en β:

- (k is even)

$$\alpha = f_{k+2}f_{k-1}^2 - f_{k-2}f_{k+1}^2 - 4S^{\frac{q^2+3}{2}}f_k^3$$

(Merk op dat hier α door y gedeeld is om op het juiste andwoord te komen.)

$$\beta = 4Sf_k((x - x^{q^2})Sf_k^2 - f_{k-1}f_{k+1})$$

- (k is oneven)

$$\alpha = S(f_{k+2}f_{k-1}^2 - f_{k-2}f_{k+1}^2) - 4S^{\frac{q^2+1}{2}}f_k^3$$

$$\beta = 4f_k((x - x^{q^2})f_k^2 - Sf_{k-1}f_{k+1})$$

(Merk op dat hier β door y gedeeld is om op het juiste andwoord te komen.)

Er moeten nu dus twee gelijkheden uitgeschreven worden:

1.
$$-x^{q^2} - x + \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2} + \frac{\alpha^2}{\beta^2} = x^q - (\frac{\psi_{\tau+1}\phi_{\tau-1}}{\psi_\tau^2})^q$$
$$\Rightarrow -(x^{q^2} + x^q + x)\psi_k^2 + \psi_{k-1}\psi_{k+1} + \psi_k^2\frac{\alpha^2}{\beta^2} = -\psi_k^2(\frac{\psi_{\tau+1}\phi_{\tau-1}}{\psi_\tau^2})^q$$
$$\Rightarrow \psi_\tau^{2q}(\beta^2(-(x^{q^2} + x^q + x)\psi_k^2 + \psi_{k-1}\psi_{k+1}) + \psi_k^2\alpha^2) + \beta^2\psi_k^2\psi_{\tau+1}^q\psi_{\tau-1}^q = 0$$

Dit polynoom (vanaf nu genaamd Pol_1.) wordt genoteerd als $Pol_1 = \psi_\tau^{2q}\delta_1 + (\psi_{\tau-1}\psi_{\tau+1})^q\delta_2$.

Eerst worden δ_1 en δ_2 berekend:
(Merk op dat hier voor k is even $y\alpha$ gescheven is in plaats voor α omdat we in de voorgaande berekening door y gedeeld hebben. Hetzelfde geld voor β voor het geval dat k oneven is.)

- (k is even)
$$\delta_1 = \beta^2(f_{k-1}f_{k+1} - (x^{q^2} + x^q + x)Sf_k^2) + \alpha^2S^2f_k^2$$
- (k is oneven)
$$\delta_1 = \beta^2S(Sf_{k-1}f_{k+1} - (x^{q^2} + x^q + x)f_k^2) + \alpha^2f_k^2$$

En voor zowel k is even als oneven:
$$\delta_2 = \beta^2Sf_k^2$$

Vervolgens wordt Pol_1 uitgeschreven:

- (τ is even)
$$Pol_1 = f_\tau^{2q}S^q\delta_1 + (f_{\tau-1}f_{\tau+1})^q\delta_2$$
- (τ is oneven)
$$Pol_1 = f_\tau^{2q}\delta_1 + (f_{\tau-1}f_{\tau+1})^qS^q\delta_2$$

En van deze formule moet dus gecheckt worden dat het nul modulo f_l is.

2.
$$-y^{q^2} - \frac{\alpha}{\beta}(-2x^{q^2} - x + \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2} + \frac{\alpha^2}{\beta^2}) = (\frac{\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2}{4y\psi_\tau^3})^q$$
$$\Rightarrow 4y^q\psi_\tau^{3q}(-\beta^3y^{q^2} - \alpha(\beta^2(-2x^{q^2} - x + \frac{\psi_{k-1} + \psi_{k+1}}{\psi_k^2}) + \alpha^2)) = \beta^3(\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2)^q$$
$$\Rightarrow 4y^q\psi_\tau^{3q}(-\beta^3\psi_k^2y^{q^2} - \alpha\beta^2(\psi_k^2(-2x^{q^2} - x) + \psi_{k-1}\psi_{k+1}) + \alpha^3\psi_k^2) - \beta^3\psi_k^2(\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2)^q = 0$$

En deze formule kan iets mooier geschreven worden als

$$4y^q\psi_\tau^{3q}(\alpha\beta^2(\psi_k^2(2x^{q^2}+x)-\psi_{k-1}\psi_{k+1})-\psi_k^2(\alpha^3+\beta^3y^{q^2}))-\beta^3\psi_k^2(\psi_{\tau+2}\psi_{\tau-1}^2-\psi_{\tau-2}\psi_{\tau+1}^2)^q$$

Dit polynoom wordt vanaf nu geschreven als

$$Pol_2 = \psi_\tau^{3q}\delta_3 - (\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2)^q\delta_4$$

Eerst worden δ_3 en δ_4 berekend:

- (k is even)

$$\delta_3 = 4y^q(y\alpha\beta^2(y^2f_k^2(2x^{q^2}+x) - f_{k-1}f_{k+1}) - y^5\alpha^3f_k^2 - y^{q^2+2}\beta^3f_k^2)$$

$$= 4S^{\frac{q+1}{2}}(\alpha\beta^2(Sf_k^2(2x^{q^2}+x) - f_{k-1}f_{k+1}) - S^2f_k^2(\alpha^3 + S^{\frac{q^2-3}{2}}\beta^3))$$

- (k is oneven)

$$\delta_3 = 4y^q(y^2\alpha\beta^2(f_k^2(2x^{q^2}+x) - y^2f_{k-1}f_{k+1}) - f_k^2(\alpha^3 + y^{q^2+3}\beta^3))$$

$$= 4S^{\frac{q-1}{2}}(S\alpha\beta^2(f_k^2(2x^{q^2}+x) - Sf_{k-1}f_{k+1}) - f_k^2(\alpha^3 + S^{\frac{q^2+3}{2}}\beta^3))$$

En in beide gevallen geldt dat

$$\delta_4 = \beta^3Sf_k^2$$

Nu hoeft dus alleen nog maar Pol_2 uitgewerkt te worden:

- (τ is even)

$$Pol_2 = f_\tau^{3q}S^{\frac{3q+1}{2}}\delta_3 - (f_{\tau+2}f_{\tau-1}^2 - f_{\tau-2}f_{\tau+1}^2)^qS^{\frac{q+1}{2}}\delta_4$$

  (Dit polynoom is verkregen door een directe berekening en het geheel vervolgens te delen door y.)

- (τ is oneven)

$$Pol_2 = f_\tau^{3q}\delta_3 - (f_{\tau+2}f_{\tau-1}^2 - f_{\tau-2}f_{\tau+1}^2)^qS^q\delta_4$$

En dit is dus het polynoom waarvan gecheckt moet worden dat het nul modulo f_l is.