Calculate $F_q = f^{-1} \bmod x^N - 1$ in Z_q, $q = 41$

$f = -x^4 - x^3 + x^2 + x + 1$, $N = 7$, $g = -x^2 - x^2 + x + 1$

$p = 3$, $d = 2$

Use Extended Euclid:

1, $A = (1, 0, x^7 - 1)$, $B = (0, 1, -x^4 - x^3 + x^2 + x + 1)$

$Q = x^7 - 1 \;\big|\; -x^4 - x^3 + x^2 + x + 1$

$-x^7 + x^6 - x^5 - x^4 - x^3 + x^2 - 2x + 2 \bmod 41 =$

$= 40x^3 + x^2 + 39x + 2$

$= Q$

quo(A3/B3)

$-x^6 + x^5 + x^4 + x^3 - 1$

$-(-x^6 - x^5 + x^4 + x^3 + x^2)$

$2x^5 - x^2 - 1$

$-(2x^5 + 2x^4 - 2x^3 - 2x^2 - 2x)$

$-2x^4 + 2x^3 + x^2 + 2x - 1$

$-(-2x^4 - 2x^3 + 2x^2 + 2x + 2)$

rem

$4x^3 - x^2 - 3 \bmod 41 = 4x^3 + 40x + 38$

$T = A - QB = (1 - q \cdot 0,\ 0 - 40x^3 - x^2 - 39x - 2,$

$4x^3 - x^2 - 3) \bmod q =$

$= (1,\ x^3 + 40x^2 + 2x + 39,\ 4x^3 + 40x^2 + 38)$

2. $A = (0, 1, -x^4 - x^3 + x^2 + x + 1)$

$B = (1, x^3 + 40x^2 + 2x + 39,\ 4x^3 + 40x^2 + 38)$

$Q = quo(A3/B3) = -x^4 - x^3 + x^2 + x + 1 \;\big|\; 4x^3 + 40x^2 + 38$

$-(40x^4 - 10x^3 - 30x)$ $\qquad 10x - 8 \bmod 41$

$9x^3 + x^2 + 31x + 1$ $\qquad = 10x + 33$

$-(-32x^3 + 8x^2 + 24)$ $\qquad \uparrow Q$

$-7x^2 - 10x - 23 \bmod 41 =$

$4^{-1} \bmod 41 = -10$

rem

$T = A - QB = (-10x - 33,\ 1 - (10x + 33)(x^3 - x^2 + 2x - 2),$
$34x^2 + 31x + 18) \bmod 41 =$

$= (31x + 8,\ 1 - (10x - 8)(x^3 - x^2 + 2x - 2), 34x^2 + 31x +$
$+18) = (31x + 8,\ 1 - 10x^4 + 8x^3 + 10x^3 - 8x^2 -$
$-20x^2 + 16x + 20x - 16,\ 34x^2 + 31x + 18) =$
$= (31x + 8,\ -10x^4 + 18x^3 - 28x^2 + 36x - 15,\ 34x^2 + 31x + 18)$
$\bmod 41 = (31x + 8,\ 31x^4 + 18x^3 + 13x^2 + 36x + 26,\ 34x^2 +$
$+ 31x + 18)$

3. $A = (1,\ x^3 + 40x^2 + 2x + 39,\ 4x^3 + 40x^2 + 38)$
$B = (31x + 8,\ 31x^4 + 18x^3 + 13x^2 + 36x + 26,\ 34x^2 +$
$+ 31x + 18)$

$Q = \text{quo}(A\,3\,|\,B) = 4x^3 + 40x^2 + 38 \;\big|\; 34x^2 + 31x + 18$

$4x^3 - x^2 - 3 \;\big|\; -7x^2 - 10x + 18$

$-168x^3 + 240x^2 - 432x - 24x - 30 \bmod 41 =$

$-164x^3 - 241x^2 + 432x - 3 \bmod 41 = 17x + 11$ ← Q

$5x^2 + 22x - 3$

$210x^2 + 300x - 540$

$-205x^2 - 278x + 537 \bmod 41$

$-32x + 4 \bmod 41$

$9x + 4 \in \text{rem}$

$7^{-1} \bmod 41 = 6$

$A = (1, 0, 41),\ B = (0, 1, 7)$

$Q = \lfloor 41/7 \rfloor = 5$

$T = (1, -5, 6)$

$A = (0, 1, 7),\ B = (1, -5, 6)$

$Q = \lfloor 7/6 \rfloor = 1$

$T = (-1, 6, 1)$

$T = A - QB = (1 - (31x+8)(17x+11),$
$x^3+40x^2+2x+39 - (17x+11)(31x^4+18x^3+13x^2+$
$+36x+26),\ 9x+4) =$

$= (1 - (-10x+8)(17x+11),\ x^3 - x^2 + 2x - 2 -$
$- (17x+11)(-10x^4+18x^3+13x^2-5x-15),\ 9x+4) =$

$= (1 + 170x^2 - 136x + 110x - 88,\ x^3 - x^2 + 2x - 2$
$+170x^5 + 110x^4 - 306x^4 - 198x^3 - 221x^3 - 143x^2$
$+85x^2 + 55x + 255x + 165,\ 9x+4) \bmod 41 =$

$= (6x^2 - 26x - 5,\ 6x^5 - 32x^4 - 35x^3 - 16x^3 - 21x^2 +$
$3x^2 + 25x + 40,\ 9x+4) \bmod 41 =$

$= (6x^2 + 15x + 36,\ 6x^5 + 9x^4 - 8x^3 - 18x^2 + 25x + 39,\ 9x+4)$
$\bmod 41 = (6x^2 + 15x + 36, 6x^5 + 9x^4 + 33x^3 + 23x^2 +$
$+25x + 40,\ 9x+4)$

4. $A = (31x+8,\ 31x^4 + 18x^3 + 13x^2 + 36x + 26,\ 34x^2 +$
$31x + 18)$

$B = (6x^2 + 15x + 36,\ 6x^5 + 9x^4 + 33x^3 + 23x^2 + 25x +$
$+40,\ 9x+4)$

$Q = gcd(A3/B3) \rightarrow$

$34x^2 + 31x + 18 \quad | \ 9x+4$
$-7x^2 - 10x + 18 \qquad 22x + 21 \leftarrow Q$
$-198x^2 + 88x$
$-205x^2 - 98x + 18 \bmod 41$
$-16x + 18$
$189x + 84 \bmod 41$
$205x - 66 \bmod 41 = 16 \rightarrow$ Rem

$9^{-1} \bmod 41 = -9$
$-7 \cdot 9^{-1} \bmod 41 = 63 \bmod 41 = 22$
$\ldots 41 = 144 \bmod 41 = 21$

$T = A - QB = (31x+8 - (22x+21)(6x^2+15x+36),$
$31x^4+18x^3+13x^2+36x+26 - (22x+21)(6x^5+$
$+9x^4+33x^3+23x^2+25x+40, 16) \bmod 41 =$

$= (-10x+8+(19x+20)(6x^2+15x-5),$
$-10x^4+18x^3+13x^2-5x-15+(19x+20)(6x^5$
$+9x^4-8x^3-18x^2-16x-1, 16) \bmod 41 =$

$= (-10x+8+114x^3+120x^2+285x^2+300x-$
$-95x-100, -10x^4+18x^3+13x^2-5x-15+$
$+114x^6+120x^5+171x^5+180x^4-152x^4-160x^3-$
$-342x^3-360x^2-304x^2-320x-19x-20, 16) \bmod 41$

$= (32x^3-5x^2+31x-10, 32x^6+4x^5+18x^4+$
$-33x^3-36x^2-16x-35, 16) \bmod 41 =$
$= (32x^3+36x^2+31x+31, 32x^6+4x^5+18x^4+8x^3$
$+5x^2+25x+6, 16)$

$T3 = 16 \Rightarrow F_8 = f_8^{-1} \bmod x^7-1 =$
$= (32x^6+4x^5+18x^4+8x^3+5x^2+25x+6) \bmod 16$

$16^{-1} \bmod 41 \equiv$
$A=(1,0,41), B=(0,1,16)$
$Q = \lfloor 41/16 \rfloor = 2$
$T = A - QB = (1,-2,9)$
$A=(0,1,16), B=(1,-2,9)$

$T = A - QB = (-1,3,7)$
$A=(1,-2,9), B=(-1,3,7)$
$Q = \lfloor 9/7 \rfloor = 1$
$T = A - QB = (2,-5,2)$
$A=(-1,3,7), B=(2,-5,2)$

$T = (-1-6,\ 3+15,\ 1) \rightarrow 16^{-1} \bmod 41 = 18$

Check: $16 \cdot 18 \bmod 41 = 256+32 \bmod 41 = 288 \bmod 41 =$

$= (7 \cdot 41 + 1) \bmod 41 = \underline{1}$

$\underline{F_8} = (2x^6 + 72x^5 + 324x^4 + 144x^3 + 90x^2 + 450x + 108) \bmod 41 =$

$2x^6 + 31x^5 + 4x^4 + 21x^3 + 8x^2 + x + 26$

$\bmod 41 = \underline{2x^6 - 10x^5 - 4x^4 - 20x^3 + 8x^2 - x - 15}$

Check it:

$F_8 \cdot f = (2x^6 - 10x^5 - 4x^4 - 20x^3 + 8x^2 - x - 15)$

$(-x^4 - x^3 + x^2 + x + 1) =$

$= -2x^{10} - 2x^9 + 2x^8 + 2x^7 + 2x^6 + 10x^9 + 10x^8$

$- 10x^7 - 10x^6 - 10x^5 + 4x^8 + 4x^7 - 4x^6 - 4x^5 - 4x^4$

$+ 20x^7 + 20x^6 - 20x^5 - 20x^4 - 20x^3 - 8x^6 - 8x^5 +$

$+ 8x^4 + 8x^3 + 8x^2 + x^5 + x^4 - x^3 - x^2 - x + 15x^4 +$

$+ 15x^3 - 15x^2 - 15x - 15 = -2x^{10} + 8x^9 + 16x^8 +$

$+ 16x^7 - 41x^5 + 2x^3 - 8x^2 - 16x - 15 \bmod 41 =$

$= (2x^{10} + 8x^9 + 16x^8 + 16x^7 + 2x^3 - 8x^2 - 16x - 15)$

$\bmod (x^7 - 1) \rightarrow$

$-2x^{10} + 8x^9 + 16x^8 + 16x^7 + 2x^3 - 8x^2 - 16x - 15$ (6)

$|x^7 - 1$

$-2x^3 +$
$+8x^2$
$+16x +$
$+16$

$-2x^{10} + 2x^3$

$8x^9 + 16x^8 + 16x^7 - 8x^2 - 16x - 15$

$-8x^9 - 8x^2$

$16x^8 + 16x^7 - 16x - 15$

$-16x^8 - 16x$

$16x^7 - 15$

$-16x^7 - 16$

Calculate h:

$h = F_8 \cdot g \bmod (x^7 - 1)$ in $\frac{1}{Z_q}$; $g = -x^3 - x^2 + x + 1 \in T(2,2)$

$= (2x^6 - 10x^5 - 4x^4 - 20x^3 + 8x^2 - x - 15)(-x^3 - x^2 + x + 1)$

$= -2x^5 - 2x^8 + 2x^7 + 2x^6 + 10x^8 + 10x^7 - 10x^6 - 10x^5$

$+ 4x^7 + 4x^6 - 4x^5 - 4x^4 + 20x^6 + 20x^5 - 20x^4 - 20x^3$

$-8x^5 - 8x^4 + 8x^3 + 8x^2 + x^4 + x^3 - x^2 - x + 15x^3 +$

$+15x^2 - 15x - 15 = -2x^9 + 8x^8 + 16x^7 + 16x^6 - 2x^5$

$-31x^4 + 4x^3 + 22x^2 - 16x - 15 \bmod 41 =$

$= -2x^9 + 8x^8 + 16x^7 + 16x^6 - 2x^5 + 10x^4 + 4x^3 - 19x^2 -$

$-16x - 15 \bmod x^7 - 1$

↓

$-2x^9+8x^8+16x^7+16x^6-2x^5+10x^4+4x^3-19x^2-16x-15 \;|\; x^7-1$

$-2x^9+2x^2$ $\quad\Big|\; -2x^2+8x+16$

$8x^8+16x^7+16x^6-2x^5+10x^4+4x^3-21x^2-16x-15$

$-8x^8-8x$

$16x^7+16x^6-2x^5+10x^4+4x^3-21x^2-8x-15$

$-16x^7-16$

$16x^6-2x^5+10x^4+4x^3-21x^2-8x+1$ ← public key

Encrypt: $h = 16x^6-2x^5+10x^4+4x^3-21x^2-8x+1$

$r = -x^5+x^2+x-1 \in T(2,2)$

$e = p \cdot r \cdot h + m = 3\cdot(-x^5+x^2+x-1)(16x^6-2x^5+10x^4+4x^3+20x^2-8x+1)+x^2+1 =$

$= 3(-16x^{11}+2x^{10}-10x^9-4x^8-20x^7+8x^6-x^5+16x^8-2x^7+10x^6+4x^5+20x^4-8x^3+x^2+16x^7-2x^6+10x^5+4x^4+20x^3-8x^2+x-16x^6+2x^5-10x^4-4x^3-20x^2+8x-1)+x^2+1 =$

$= 3(-16x^{11}+2x^{10}-10x^9+12x^8-6x^7+15x^5+14x^4+8x^3-27x^2+9x-1)+x^2+1 =$

$= -48x^{11}+6x^{10}-30x^9+36x^8-18x^7+45x^5+42x^4+24x^3-81x^2+27x-3+x^2+1 \bmod 41 =$

$= -7x^{11}+6x^{10}+11x^9-5x^8-18x^7+4x^5+x^4-17x^3+2x^2-14x-2 \bmod x^7-1$

↓1

(8)

$-7x^{11} + 6x^{10} + 11x^9 - 5x^8 - 18x^7 + 4x^5 + x^4 - 17x^3 + 2x^2 - 14x - 2 \;|\; x^7 - 1$

$-7x^{11} + 7x^4$

$-7x^4 + 6x^3 + 11x^2 - 5x - 18$

$6x^{10} + 11x^9 - 5x^8 - 18x^7 + 4x^5 - 6x^4 - 17x^3 + 2x^2 - 14x - 2$

$6x^{10} - 6x^3$

$11x^9 - 5x^8 - 18x^7 + 4x^5 - 6x^4 - 11x^3 + 2x^2 - 14x - 2$

$11x^9 - 11x^2$

$-5x^8 - 18x^7 + 4x^5 - 6x^4 - 11x^3 + 13x^2 - 14x - 2$

$-5x^8 + 5x$

$-18x^7 + 4x^5 - 6x^4 - 11x^3 + 13x^2 - 19x - 2$

$-18x^7 + 18$

$4x^5 - 6x^4 - 11x^3 + 13x^2 - 19x - 20$

↑ ciphertext