Example by Hand KZG commitments

1) System / Preliminaries / Setup

$(\mathbb{F}_{11}, +)$, $p = 11$, $t = 2$, $g = 2$ (any element $\neq 0$ generates)

→ Pairing $e(x,y) = x \cdot y \bmod 11$.

① $e(x_1 + x_2, y) = (x_1 + x_2)y = x_1 y + x_2 y = e(x_1, y) + e(x_2, y)$ ✓

$e(x, y_1 + y_2) = x(y_1 + y_2) = xy_1 + xy_2 = e(x, y_1) + e(x, y_2)$ ✓

② $e(g,g) = e(2,2) = 4 \neq 0$ ✓

→ Trusted Setup $(\alpha = 3)$

$PP = \langle g, \alpha g, \alpha^2 g \rangle = \langle 2, 3 \cdot 2, 3^2 \cdot 2 \rangle = \langle 2, 6, 18 \rangle \equiv \langle 2, 6, 7 \rangle$

$g \quad \alpha g \quad \alpha^2 g$

and DELETES α.

2) Commitment

We want to commit $\phi(x) = 3x^2 + 5x + 7$

$C = [\phi(\alpha)] = 3\alpha^2 g + 5\alpha g + 7g = 3 \cdot 7 + 5 \cdot 6 + 7 \cdot 2 = 65 \equiv 10 \bmod 11$

↳ $C = 10$.

3) Open

Open at $i = 1$ → $\phi(1) = 3 + 5 + 7 = 15 \equiv 4 \bmod 11$.

↳ $\psi(x) = \dfrac{\phi(x) - \phi(1)}{x - 1} = \dfrac{3x^2 + 5x + 7 - 4}{x - 1} = \dfrac{3x^2 + 5x + 3}{x - 1}$

$3x^2 + 5x + 3 \;|\; x - 1$

$-3x^2 + 3x \qquad 3x + 8$

$\backslash \quad 8x + 3$

$\quad -8x + 8$

$\backslash\backslash \quad 11 \equiv 0 \;/\!/$

⇝ $\psi(x) = 3x + 8$

$C_\psi = 3\alpha g + 8g = 3 \cdot 6 + 8 \cdot 2 = 34 \equiv 1$

↳ $C_\psi = 1$.

4) Verification

We have, $\mathcal{E} = 10$; $i = 1$; $\phi(i) = 4$; $\mathcal{E}_N = 1$; $g = 2$; $\langle 2, 6, 7 \rangle$; $e(x,y) = x \cdot y$

$g \quad \alpha g \quad \alpha^2 g$

$$e(\mathcal{E} + [-\phi(i)], [1]) \overset{?}{=} e(\mathcal{E}_N, [\alpha - i])$$

① ②

① $e(\mathcal{E} + [-\phi(i)], [1]) = e(\mathcal{E} + [7], [1]) = e(10 + [2 \cdot 7], 2)$

$= e(24, 2) =$

$= 48 \equiv 4 \mod 11$

$-\phi(i) = -4 \equiv 7 \mod 11$

② $e(\mathcal{E}_N, [\alpha - i]) = e(1, [\alpha + 10]) = e(1, \underbrace{g\alpha}_{6} + 10g)$

$= e(1, 6 + (10 \cdot 2))$

$= 26 \equiv 4 \mod 11$ #

$-i = -1 \equiv 10 \mod 11$

What happens if α is leaked? ($\alpha = 3$)

$P_1(x) = 3x^2 + 5x + 7 \longrightarrow P_1(\alpha) = 49$ (!!)

$P_2(x) = 2x^2 + 7x + 10 \longrightarrow P_2(\alpha) = 49$