

with(numtheory) : with(linalg) : with(IntegerRelations) : with(LinearAlgebra) :
with(LinearAlgebra[Modular]) : with(Bits) :

> ##### 24 FEB 2015..... $F(e_1, e_2, e_3, e_4) = 0 \pmod{p}$

?

> $e_1 := g_1^{t_1}; e_2 := g_2^{t_2}; c := g_1^{t_1+t_3} - g_2^{t_2+t_4}; w := g_1^{t_3} \cdot g_2^{t_2} - g_1^{t_1} \cdot g_2^{t_4}; a_1 := \frac{-r \cdot e_1}{w}; a_2$
 $:= \frac{r \cdot e_2 + a_1 \cdot c}{w}; r := 1;$

$$e_1 := g_1^{t_1}$$

$$e_2 := g_2^{t_2}$$

$$c := g_1^{(t_1+t_3)} - g_2^{(t_2+t_4)}$$

$$w := g_1^{t_3} g_2^{t_2} - g_1^{t_1} g_2^{t_4}$$

$$a_1 := -\frac{g_1^{t_1}}{g_1^{t_3} g_2^{t_2} - g_1^{t_1} g_2^{t_4}}$$

$$a_2 := \frac{g_2^{t_2} - \frac{g_1^{t_1} (g_1^{(t_1+t_3)} - g_2^{(t_2+t_4)})}{g_1^{t_3} g_2^{t_2} - g_1^{t_1} g_2^{t_4}}}{g_1^{t_3} g_2^{t_2} - g_1^{t_1} g_2^{t_4}}$$

$$r := 1$$

(1)

> $e_3 := a_1 \cdot g_1^{t_3} + a_2 \cdot g_2^{t_4}; e_4 := a_2 \cdot c;$

$$e_3 := -\frac{g_1^{t_1} g_1^{t_3}}{g_1^{t_3} g_2^{t_2} - g_1^{t_1} g_2^{t_4}} + \frac{\left(g_2^{t_2} - \frac{g_1^{t_1} (g_1^{(t_1+t_3)} - g_2^{(t_2+t_4)})}{g_1^{t_3} g_2^{t_2} - g_1^{t_1} g_2^{t_4}} \right) g_2^{t_4}}{g_1^{t_3} g_2^{t_2} - g_1^{t_1} g_2^{t_4}}$$

$$e_4 := \frac{\left(g_2^{t_2} - \frac{g_1^{t_1} (g_1^{(t_1+t_3)} - g_2^{(t_2+t_4)})}{g_1^{t_3} g_2^{t_2} - g_1^{t_1} g_2^{t_4}} \right) (g_1^{(t_1+t_3)} - g_2^{(t_2+t_4)})}{g_1^{t_3} g_2^{t_2} - g_1^{t_1} g_2^{t_4}}$$

(2)

> $simplify(e_1 \cdot e_2 + e_3 \cdot e_4);$

(3)

$$\begin{aligned}
& - \frac{1}{\left(\begin{smallmatrix} t_3 & t_2 \\ g_1 & g_2 \end{smallmatrix} - \begin{smallmatrix} t_1 & t_4 \\ g_1 & g_2 \end{smallmatrix} \right)^4} \left(-g_1^{\binom{5t_1}{1}} g_2^{\binom{t_2+4t_4}{2}} - 2g_1^{\binom{t_1+3t_3}{1}} g_2^{\binom{4t_2+t_4}{2}} + 2g_1^{\binom{3t_1+3t_3}{1}} g_2^{\binom{t_4+2t_2}{2}} - \right. \\
& \quad g_1^{\binom{4t_1+4t_3}{1}} g_2^{\binom{t_2}{2}} - g_1^{\binom{2t_1+2t_3}{1}} g_2^{\binom{3t_2+2t_4}{2}} + 4g_1^{\binom{2t_1+3t_3}{1}} g_2^{\binom{4t_2+t_4}{2}} - 6g_1^{\binom{3t_1+2t_3}{1}} g_2^{\binom{3t_2+2t_4}{2}} \\
& \quad \left. + 4g_1^{\binom{4t_1+t_3}{1}} g_2^{\binom{3t_4+2t_2}{2}} + g_2^{\binom{5t_2+2t_4}{2}} g_1^{\binom{2t_3}{1}} - g_1^{\binom{t_1+4t_3}{1}} g_2^{\binom{5t_2}{2}} + g_1^{\binom{2t_1+4t_3}{1}} g_2^{\binom{3t_2}{2}} \right) \tag{3}
\end{aligned}$$

> *simplify*($e_1 \cdot e_3 + e_2 \cdot e_4$);

$$\begin{aligned}
& \frac{1}{\left(\begin{smallmatrix} t_3 & t_2 \\ g_1 & g_2 \end{smallmatrix} - \begin{smallmatrix} t_1 & t_4 \\ g_1 & g_2 \end{smallmatrix} \right)^2} \left(-g_1^{\binom{2t_1+2t_3}{1}} g_2^{\binom{t_2}{2}} + g_1^{\binom{t_1+t_3}{1}} g_2^{\binom{t_4+2t_2}{2}} + g_1^{\binom{t_1+2t_3}{1}} g_2^{\binom{3t_2}{2}} + g_1^{\binom{2t_1+t_3}{1}} \right. \\
& \quad \left. g_2^{\binom{t_4+2t_2}{2}} - g_1^{\binom{3t_1+2t_3}{1}} g_2^{\binom{t_2}{2}} - g_2^{\binom{4t_2+t_4}{2}} g_1^{\binom{t_3}{1}} \right) \tag{4}
\end{aligned}$$

> *simplify*($e_1 \cdot e_4 + e_2 \cdot e_3$);

$$\begin{aligned}
& \frac{1}{\left(\begin{smallmatrix} t_3 & t_2 \\ g_1 & g_2 \end{smallmatrix} - \begin{smallmatrix} t_1 & t_4 \\ g_1 & g_2 \end{smallmatrix} \right)^2} \left(g_1^{\binom{2t_1+2t_3}{1}} g_2^{\binom{2t_2}{2}} + g_1^{\binom{3t_1+t_3}{1}} g_2^{\binom{t_2+t_4}{2}} - g_1^{\binom{4t_1+2t_3}{1}} - g_2^{\binom{3t_2+t_4}{2}} g_1^{\binom{t_1+t_3}{1}} \right. \\
& \quad \left. - g_1^{\binom{t_1+2t_3}{1}} g_2^{\binom{2t_2}{2}} + g_2^{\binom{3t_2+t_4}{2}} g_1^{\binom{t_3}{1}} \right) \tag{5}
\end{aligned}$$

> *simplify*(($e_1 + e_2$) $\cdot e_3$);

$$\frac{-g_1^{\binom{2t_1+2t_3}{1}} g_2^{\binom{t_2}{2}} + g_1^{\binom{t_1+t_3}{1}} g_2^{\binom{t_4+2t_2}{2}} - g_1^{\binom{t_1+2t_3}{1}} g_2^{\binom{2t_2}{2}} + g_2^{\binom{3t_2+t_4}{2}} g_1^{\binom{t_3}{1}}}{\left(\begin{smallmatrix} t_3 & t_2 \\ g_1 & g_2 \end{smallmatrix} - \begin{smallmatrix} t_1 & t_4 \\ g_1 & g_2 \end{smallmatrix} \right)^2} \tag{6}$$

> *simplify*(($e_1 - e_2$) $\cdot e_3$);

$$\frac{-g_1^{\binom{2t_1+2t_3}{1}} g_2^{\binom{t_2}{2}} + g_1^{\binom{t_1+t_3}{1}} g_2^{\binom{t_4+2t_2}{2}} + g_1^{\binom{t_1+2t_3}{1}} g_2^{\binom{2t_2}{2}} - g_2^{\binom{3t_2+t_4}{2}} g_1^{\binom{t_3}{1}}}{\left(\begin{smallmatrix} t_3 & t_2 \\ g_1 & g_2 \end{smallmatrix} - \begin{smallmatrix} t_1 & t_4 \\ g_1 & g_2 \end{smallmatrix} \right)^2} \tag{7}$$

> *simplify*(($e_1 + e_2$) $\cdot e_4$);

$$\begin{aligned}
& \frac{1}{\left(\begin{smallmatrix} t_3 & t_2 \\ g_1 & g_2 \end{smallmatrix} - \begin{smallmatrix} t_1 & t_4 \\ g_1 & g_2 \end{smallmatrix} \right)^2} \left(g_1^{\binom{2t_1+2t_3}{1}} g_2^{\binom{2t_2}{2}} + g_1^{\binom{3t_1+t_3}{1}} g_2^{\binom{t_2+t_4}{2}} - g_2^{\binom{3t_2+t_4}{2}} g_1^{\binom{t_1+t_3}{1}} - g_1^{\binom{4t_1+2t_3}{1}} \right. \\
& \quad \left. + g_1^{\binom{t_1+2t_3}{1}} g_2^{\binom{3t_2}{2}} + g_1^{\binom{2t_1+t_3}{1}} g_2^{\binom{t_4+2t_2}{2}} - g_2^{\binom{4t_2+t_4}{2}} g_1^{\binom{t_3}{1}} - g_1^{\binom{3t_1+2t_3}{1}} g_2^{\binom{t_2}{2}} \right) \tag{8}
\end{aligned}$$

> *simplify*(($e_1 + e_3$) $\cdot e_2$);

$$\frac{g_1^{\binom{t_1+2t_3}{1}} g_2^{\binom{3t_2}{2}} - 2g_1^{\binom{2t_1+t_3}{1}} g_2^{\binom{t_4+2t_2}{2}} + g_1^{\binom{3t_1}{1}} g_2^{\binom{2t_4+t_2}{2}} - g_1^{\binom{t_1+2t_3}{1}} g_2^{\binom{2t_2}{2}} + g_2^{\binom{3t_2+t_4}{2}} g_1^{\binom{t_3}{1}}}{\left(\begin{smallmatrix} t_3 & t_2 \\ g_1 & g_2 \end{smallmatrix} - \begin{smallmatrix} t_1 & t_4 \\ g_1 & g_2 \end{smallmatrix} \right)^2} \tag{9}$$

> *simplify*(($e_1 + e_3$) $\cdot e_4$);

$$\begin{aligned}
& - \frac{1}{\left(g_1^3 g_2^2 - g_1^1 g_2^4\right)^4} \left(-2 g_1^{\binom{t+3t}{1}} g_2^{\binom{4t+t}{2}} + 2 g_1^{\binom{3t+3t}{1}} g_2^{\binom{t+2t}{2}} - g_1^{\binom{4t+4t}{1}} g_2^{\binom{t}{2}} - \right. \\
& \quad g_1^{\binom{2t+2t}{1}} g_2^{\binom{3t+2t}{2}} - g_1^{\binom{2t+4t}{1}} g_2^{\binom{4t}{2}} + g_1^{\binom{4t+4t}{1}} g_2^{\binom{2t}{2}} + g_1^{\binom{6t+2t}{1}} g_2^{\binom{2t}{4}} + \\
& \quad g_2^{\binom{5t+2t}{2}} g_1^{\binom{2t}{3}} - g_1^{\binom{5t+t}{1}} g_2^{\binom{t+3t}{2}} + g_2^{\binom{t+5t}{4}} g_1^{\binom{t+3t}{1}} + g_1^{\binom{2t+4t}{1}} g_2^{\binom{3t}{2}} + \\
& \quad g_1^{\binom{3t+3t}{1}} g_2^{\binom{3t+t}{2}} + g_1^{\binom{4t+2t}{1}} g_2^{\binom{2t+2t}{2}} - 2 g_1^{\binom{5t+3t}{1}} g_2^{\binom{t+t}{2}} - 2 g_2^{\binom{4t+2t}{2}} \\
& \quad \left. g_1^{\binom{2t+2t}{1}} + g_2^{\binom{3t+3t}{2}} g_1^{\binom{3t+t}{1}} \right) \tag{10}
\end{aligned}$$

> *simplify*((e₁ + e₄) · e₂);

$$\begin{aligned}
& \frac{2 g_1^{\binom{t+2t}{1}} g_2^{\binom{3t}{2}} - g_1^{\binom{2t+1+t}{1}} g_2^{\binom{t+2t}{2}} + g_1^{\binom{3t}{1}} g_2^{\binom{2t+t}{2}} - g_1^{\binom{3t+2t}{1}} g_2^{\binom{t}{2}} - g_2^{\binom{4t+t}{2}} g_1^{\binom{t}{3}}}{\left(g_1^3 g_2^2 - g_1^1 g_2^4\right)^2} \tag{11}
\end{aligned}$$

> *simplify*((e₁ + e₄) · e₃);

$$\begin{aligned}
& - \frac{1}{\left(g_1^3 g_2^2 - g_1^1 g_2^4\right)^4} \left(-3 g_1^{\binom{t+3t}{1}} g_2^{\binom{4t+t}{2}} - g_1^{\binom{4t+4t}{1}} g_2^{\binom{t}{2}} + g_1^{\binom{2t+2t}{1}} g_2^{\binom{3t+2t}{2}} + \right. \\
& \quad \left. g_1^{\binom{4t+2t}{1}} g_2^{\binom{2t+t}{2}} - g_1^{\binom{3t+t}{1}} g_2^{\binom{3t+2t}{2}} + g_2^{\binom{5t+2t}{2}} g_1^{\binom{2t}{3}} + 2 g_1^{\binom{2t+4t}{1}} g_2^{\binom{3t}{2}} \right) \tag{12}
\end{aligned}$$

> *simplify*((e₂ + e₃) · e₄);

$$\begin{aligned}
& - \frac{1}{\left(g_1^3 g_2^2 - g_1^1 g_2^4\right)^4} \left(-2 g_1^{\binom{t+3t}{1}} g_2^{\binom{4t+t}{2}} + 2 g_1^{\binom{3t+3t}{1}} g_2^{\binom{t+2t}{2}} - g_1^{\binom{4t+4t}{1}} g_2^{\binom{t}{2}} - \right. \\
& \quad g_1^{\binom{2t+2t}{1}} g_2^{\binom{3t+2t}{2}} + g_1^{\binom{2t+3t}{1}} g_2^{\binom{4t+t}{2}} + g_1^{\binom{3t+2t}{1}} g_2^{\binom{3t+2t}{2}} - g_1^{\binom{4t+t}{1}} \\
& \quad g_2^{\binom{3t+2t}{2}} + g_2^{\binom{5t+2t}{2}} g_1^{\binom{2t}{3}} - g_1^{\binom{t+4t}{1}} g_2^{\binom{5t}{2}} + g_2^{\binom{4t+3t}{2}} g_1^{\binom{2t+t}{1}} + g_1^{\binom{2t+4t}{1}} \\
& \quad g_2^{\binom{3t}{2}} + g_1^{\binom{3t+4t}{1}} g_2^{\binom{3t}{2}} + g_2^{\binom{6t+t}{2}} g_1^{\binom{3t}{3}} - 2 g_1^{\binom{4t+3t}{1}} g_2^{\binom{t+2t}{2}} + g_1^{\binom{5t+2t}{1}} \\
& \quad \left. g_2^{\binom{2t+t}{2}} - 2 g_2^{\binom{5t+2t}{2}} g_1^{\binom{t+2t}{1}} \right) \tag{13}
\end{aligned}$$

> *simplify*((e₂ + e₄) · e₃);

$$\begin{aligned}
& - \frac{1}{\left(g_1^3 g_2^2 - g_1^1 g_2^4\right)^4} \left(-2 g_1^{\binom{t+3t}{1}} g_2^{\binom{4t+t}{2}} + 2 g_1^{\binom{3t+3t}{1}} g_2^{\binom{t+2t}{2}} - g_1^{\binom{4t+4t}{1}} g_2^{\binom{t}{2}} - \right. \\
& \quad g_1^{\binom{2t+2t}{1}} g_2^{\binom{3t+2t}{2}} - g_2^{\binom{3t+3t}{2}} g_1^{\binom{2t+t}{1}} + g_2^{\binom{5t+2t}{2}} g_1^{\binom{2t}{3}} + g_1^{\binom{t+4t}{1}} g_2^{\binom{4t}{2}} - \\
& \quad \left. g_2^{\binom{t+5t}{2}} g_1^{\binom{3t}{3}} + g_1^{\binom{2t+4t}{1}} g_2^{\binom{3t}{2}} + g_1^{\binom{3t+2t}{1}} g_2^{\binom{2t+2t}{2}} - 2 g_1^{\binom{2t+3t}{1}} g_2^{\binom{3t+t}{2}} \right) \tag{14}
\end{aligned}$$

$$\begin{aligned}
 & + 2 g_2 \binom{4t_2 + 2t_4}{2} g_1 \binom{t_1 + 2t_3}{1} \\
 & \text{> } \text{simplify}((e_1 + e_3) \cdot e_2 - (e_3 - e_4)); \\
 & \frac{1}{\left(g_1^3 g_2^2 - g_1^2 g_2^4 \right)^2} \left(g_1 \binom{t_1 + 2t_3}{1} g_2 \binom{3t_2}{2} - 2 g_1 \binom{2t_1 + t_3}{1} g_2 \binom{t_4 + 2t_2}{4} + g_1 \binom{3t_1}{1} g_2 \binom{2t_4 + t_2}{2} + g_1 \binom{2t_1 + t_3}{2} \right. \\
 & \left. g_2 \binom{t_2 + t_4}{2} + g_1 \binom{t_1 + 2t_3}{1} g_2^2 - g_2 \binom{t_4 + 2t_2}{4} g_1^3 - g_1 \binom{3t_1 + 2t_3}{1} \right)
 \end{aligned} \tag{15}$$

$$\begin{aligned}
 & \text{> } \text{simplify} \left((a_2 \cdot e_1 \cdot e_3 - a_1 \cdot e_2 \cdot e_3) - \left(a_1 \cdot e_4 + a_2 \cdot e_1 \cdot e_3 - g_1^3 \cdot (a_1 \cdot a_2 \cdot e_1 + a_1 \cdot a_1 \cdot e_2) \right) \right); \\
 & \quad \quad \quad 0
 \end{aligned} \tag{16}$$

>