>

> $norm1 := \mathrm{proc}(a,b,c)\,\mathrm{global}\,k;\ k := a^3 - 2\cdot b^3 + 4\cdot c^3 + 6\cdot a\cdot b\cdot c;\,\mathrm{end};$

$$norm1 := \textbf{\textit{proc}}\,(a,b,c) \quad \textbf{\textit{global}} \quad k; \quad k := a^3 - 2*b^3 + 4*c^3 + 6*b*a*c \quad \text{end proc} \tag{1}$$

> $norm1\,(66,53,0);$

$$-10258 \tag{2}$$

> $mult2 := \mathrm{proc}(a,b,c,d,e,f)\mathrm{global}\,mul1\,, mul2\,, mul3;\ mul1 := a\cdot d - 2\cdot b\cdot f - 2\cdot c\cdot e;$
$mul2 := a\cdot e + b\cdot d - 2\cdot c\cdot f;$
$mul3 := a\cdot f + b\cdot e + c\cdot d;$
$RETURN(mul1\,, mul2\,, mul3);\,\mathrm{end};$

$$mult2 := \textbf{\textit{proc}}\,(a,b,c,d,e,f) \quad \textbf{\textit{global}} \quad mul1\,, mul2\,, mul3; \quad mul1 := a*d - 2*b*f - 2*c*e; \quad mul2 := a*e + b*d - 2*c*f; \quad mul3 := f*a + b*e + c*d; \quad RETURN(mul1\,, mul2\,, mul3) \quad \text{end proc} \tag{3}$$

>

> $U := [1,1,0]; A := [0,1,0]; B := [-1,1,0]; C := [1,0,1]; D1 := [1,1,-1]; E := [1,-2,0]; F := [3,0,-1];$

$$U := [1,1,0]$$
$$A := [0,1,0]$$
$$B := [-1,1,0]$$
$$C := [1,0,1]$$
$$D1 := [1,1,-1]$$
$$E := [1,-2,0]$$
$$F := [3,0,-1] \tag{4}$$

> $mult1 := \mathrm{proc}(x,y);\ mult2(x[1],x[2],x[3],y[1],y[2],y[3])\,;\,\mathrm{end};$

$$mult1 := \textbf{\textit{proc}}\,(x,y) \quad mult2(x\,[1]\,, x\,[2]\,, x\,[3]\,, y\,[1]\,, y\,[2]\,, y\,[3]) \quad \text{end proc} \tag{5}$$

>
>

> $mult4 := \text{proc}()\text{global } L;\ L := [];\ \text{for } i \text{ from } 1 \text{ to } nargs \text{ do } L := [op(L), args[i]];\ \text{od};\ \text{if } nops(L) = 2 \text{ then } mult1(op(1, L), op(2, L)) \text{ else } k := [mult1(op(1, L), op(2, L))];\ L := subsop(1 = NULL, L);\ L := subsop(1 = NULL, L);\ L := [k, op(L)];\ mult4(op(L));\ \text{fi};\ \text{end};$

Warning, (in mult4) 'i' is implicitly declared localWarning, (in mult4) 'k' is implicitly declared local

$$
\begin{array}{l}
mult4 := \\
\quad \textbf{proc}() \quad \textbf{local} \quad i, k; \quad \textbf{global} \quad L; \\
\quad\quad L := [] ; \quad \textbf{for} \quad i \quad \textbf{to} \quad nargs \quad \textbf{do} \quad L := [op(L), args[i]] \quad \text{end do}; \\
\quad\quad \textbf{if} \quad nops(L) = 2 \quad \textbf{then} \quad mult1(op(1, L), op(2, L)) \quad \textbf{else} \\
\quad\quad \text{end if} \\
\quad\quad \text{end proc}
\end{array}
\tag{6}
$$

> $mult4(U, U, B, E);$

$$1, 5, 3 \tag{7}$$

> $H := mult4(U, A, A, A);$

$$H := -2, -2, 0 \tag{8}$$

>

> $H := [-2, -2, 0];$

$$H := [-2, -2, 0] \tag{9}$$

> $mult4(H, A, A, A);$

$$4, 4, 0 \tag{10}$$

> $H := [4, 4, 0];$

$$H := [4, 4, 0] \tag{11}$$

> $mult4(H, A, A, B);$

$$0, -8, -4 \tag{12}$$

> $H := [0, -8, -4];$

$$H := [0, -8, -4] \tag{13}$$

> $mult4(U, H, B, E);$

$$32, -16, -28 \tag{14}$$

> $M := mult1(0, -8, -4, -1, 1, 0);$

$$M := 0, 0, 0 \tag{15}$$

> $mult1(0, 0, 0, 1, -2, 0)$;

$$0, 0, 0 \tag{16}$$

>

$U := [1, 1, 0]; A := [0, 1, 0]; B := [-1, 1, 0]; C := [1, 0, 1]; D1 := [1, 1, -1]; E := [1, -2, 0]; F := [3, 0, -1];$

A = [0,1,0], B = [-1,-1,0], C = [1,0,1], D = [1,1,-1], E = [1,-2,0], F = [3,0,-1]

Factor Base : [-1, 2, 3, 5, 7,11, 13,-1, U, A, B, C, D, E, F]

Row 23: [0, 1, 1, 0, 1, 0, 0, 1, 0, 4, 0, 0, 0, 0, 0],
Row 37: [0, 1, 1, 0, 0, 0, 0, 1, 1, 3, 3, 0, 0, 0, 0],
Row 41: [0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 2, 0],
Row 45: [0, 5, 0, 1, 0, 0, 0, 1, 0, 9, 1, 0, 0, 0, 0],

U*A^8*B^2*E = $[1, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [-1, 1, 0] \cdot [-1, 1, 0] \cdot [1, -2, 0]$;
>
> $mult1(U, A)$;

$$0, 1, 1 \tag{17}$$

> $UA := [0, 1, 1]$;

$$UA := [0, 1, 1] \tag{18}$$

> $mult1(UA, A)$;

$$-2, 0, 1 \tag{19}$$

> $UAA := [-2, 0, 1]$;

$$UAA := [-2, 0, 1] \tag{20}$$

> $mult1(UAA, A)$;

$$-2, -2, 0 \tag{21}$$

> $UAAA := [-2, -2, 0]$;

$$UAAA := [-2, -2, 0] \tag{22}$$

> $mult1(UAAA, A)$;

$$0, -2, -2 \tag{23}$$

> $UAAAA := [0, -2, -2]$;

$$UAAAA := [0, -2, -2] \tag{24}$$

> $mult4(UAAAA, A, A, A)$;

$$0, 4, 4 \tag{25}$$

> $UAAAAAAA := [0, 4, 4]$;

$$UAAAAAAA := [0, 4, 4] \tag{26}$$

> $mult4(UAAAAAAA, A)$;

$$-8, 0, 4 \tag{27}$$

> $UA8 := [-8, 0, 4]$;

$$UA8 := [-8, 0, 4] \tag{28}$$

> $mult4(UA8, B, B, E)$;

$$-8, -8, -20 \tag{29}$$

>

u = phi(a + bz + czˆ2) = a + 21b + 21ˆ2c = -8 + 21*-8 + 21ˆ2 * -20 = -8996
v = 2ˆ4*3*5*7 = 1680
vˆ2 mod 9263 = 6448
uˆ2 mod 9263 = 6448

gcd(9263, 1680 + 8996) = 157
gcd(9263, 1680 - 8996) = 59

> $igcd(9263, 10676)$;

$$157 \tag{30}$$

> $igcd(9263, 7316)$;

$$59 \tag{31}$$

> $ifactor(9263)$;

$$(59)\,(157) \tag{32}$$

>