The Ben-Or / Tiwari interpolation algorithm.

```
> M1, M2, M3 := x^3*y^4, x*y^3*z, x^6*z^2;
```

$$M1, M2, M3 := x^3 y^4, x y^3 z, x^6 z^2$$

```
> a1, a2, a3 := 101,103,997;
```

$$a1, a2, a3 := 101, 103, 997$$

```
> f := a1*M1+a2*M2+a3*M3;
```

$$f := 997 x^6 z^2 + 101 x^3 y^4 + 103 x y^3 z$$

```
> d := degree(f);
```

$$d := 8$$

```
> T := 3;
```

$$T := 3$$

```
> for i from 0 to 2*T-1 do v||i := eval( f, {x=2^i,y=3^i,z=5^i} ) od ;
```

$$v0 := 1201$$

$$v1 := 1688458$$

$$v2 := 2602239004$$

$$v3 := 4113221225992$$

$$v4 := 6552294840520816$$

$$v5 := 10465990263818548768$$

```
> V := Matrix([[v0,v1,v2],[v1,v2,v3],[v2,v3,v4]]);
```

$$V := \begin{bmatrix} 1201 & 1688458 & 2602239004 \\ 1688458 & 2602239004 & 4113221225992 \\ 2602239004 & 4113221225992 & 6552294840520816 \end{bmatrix}$$

```
> S := Vector([-v3,-v4,-v5]);
```

$$S := \begin{bmatrix} -4113221225992 \\ -6552294840520816 \\ -10465990263818548768 \end{bmatrix}$$

```
> L := LinearAlgebra:-LinearSolve(V,S);
```

$$L := \begin{bmatrix} -279936000 \\ 1643760 \\ -2518 \end{bmatrix}$$

```
> Lambda := L[1]+L[2]*z+L[3]*z^2+z^3;
```

$$\Lambda := z^3 - 2518 z^2 + 1643760 z - 279936000$$

```
> factor(Lambda);
```

$$(z - 1600)\ (z - 270)\ (z - 648)$$

```
> m1,m2,m3 := 1600,270,648;
```

$$m1, m2, m3 := 1600, 270, 648$$

```
> ifactor(m1), ifactor(m2), ifactor(m3);
```

$$(2)^6\,(5)^2,\ (2)\,(3)^3\,(5),\ (2)^3\,(3)^4$$

```
> M1,M2,M3 := x*y^3*z, x^3*y^4, x^6*z^2;
```

$$M1, M2, M3 := x\,y^3\,z,\ x^3\,y^4,\ x^6\,z^2$$

```
> M := Matrix([[1,1,1],[m1,m2,m3],[m1^2,m2^2,m3^2]]);
```

$$M := \begin{bmatrix} 1 & 1 & 1 \\ 1600 & 270 & 648 \\ 2560000 & 72900 & 419904 \end{bmatrix}$$

```
> V := <v0,v1,v2>;
```

$$V := \begin{bmatrix} 1201 \\ 1688458 \\ 2602239004 \end{bmatrix}$$

```
> LinearAlgebra:-LinearSolve(M,V);
```

$$\begin{bmatrix} 997 \\ 103 \\ 101 \end{bmatrix}$$

```
> a1,a2,a3 := 103,101,997;
```

$$a1, a2, a3 := 103, 101, 997$$

```
> a1*M1+a2*M2+a3*M3;
```

$$997\,x^6\,z^2 + 101\,x^3\,y^4 + 103\,x\,y^3\,z$$

```
> f ;
```

$$997\,x^6\,z^2 + 101\,x^3\,y^4 + 103\,x\,y^3\,z$$

If we don't know the number of terms of $f(x, y, z)$ then we can try T = 3 then T = 5 etc. say. So we would do

```
> T := 5; for i from 0 to 2*T-1 do v||i := eval( f, {x=2^i,y=3^i,z=5^i}
  ) od ;
```

$$T := 5$$
$$v0 := 1201$$
$$v1 := 1688458$$
$$v2 := 2602239004$$
$$v3 := 4113221225992$$
$$v4 := 6552294840520816$$
$$v5 := 10465990263818548768$$
$$v6 := 16734402014359905801664$$
$$v7 := 26767871324579900233478272$$
$$v8 := 42823966790660259295273920256$$
$$v9 := 68515353772682930688212100325888$$

This leads to very large integers. Instead we will also work mod p to eliminate arithmetic with large rationals. We need $p > m_i$ to recover the monomial evaluations uniquely and we can bound $m_i < p_n^d = 5^8$.

```
> p := nextprime(5^8);
```

$$p := 390647$$

```
> T := 5; for i from 0 to 2*T-1 do v||i := Eval( f, {x=2^i,y=3^i,z=5^i}
  ) mod p od ;
```

$$T := 5$$
$$v0 := 1201$$
$$v1 := 125870$$
$$v2 := 139337$$
$$v3 := 129301$$
$$v4 := 120236$$
$$v5 := 351724$$
$$v6 := 57901$$
$$v7 := 288243$$
$$v8 := 152006$$
$$v9 := 260059$$

```
> V := Matrix([seq([seq(v||(i+j),j=0..T-1)],i=0..T-1)]);
```

$$V := \begin{bmatrix} 1201 & 125870 & 139337 & 129301 & 120236 \\ 125870 & 139337 & 129301 & 120236 & 351724 \\ 139337 & 129301 & 120236 & 351724 & 57901 \\ 129301 & 120236 & 351724 & 57901 & 288243 \\ 120236 & 351724 & 57901 & 288243 & 152006 \end{bmatrix}$$

```
> k := Gausselim(V) mod p;
```

$$k := \begin{bmatrix} 1 & 389776 & 161449 & 91508 & 245027 \\ 0 & 1 & 373721 & 270330 & 37740 \\ 0 & 0 & 1 & 2518 & 8800 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

```
> T := 3;
```

$$T := 3$$

```
> V := Matrix([seq([seq(v||(i+j),j=0..T-1)],i=0..T-1)]);
```

$$V := \begin{bmatrix} 1201 & 125870 & 139337 \\ 125870 & 139337 & 129301 \\ 139337 & 129301 & 120236 \end{bmatrix}$$

```
> S := Vector([-v3,-v4,-v5]);
```

$$S := \begin{bmatrix} -129301 \\ -120236 \\ -351724 \end{bmatrix}$$

```
> L := Linsolve(V,S) mod p;
```

$$L := \begin{bmatrix} 157899 \\ 81172 \\ 388129 \end{bmatrix}$$

```
> Lambda := L[1]+L[2]*z+L[3]*z^2+1*z^3;
```

$$\Lambda := z^3 + 388129\, z^2 + 81172\, z + 157899$$

```
> Roots(Lambda) mod p;
```

$$[[1600, 1], [270, 1], [648, 1]]$$