Modular Multiplication algorithm.

```
> A := x^4+25*x^3+145*x^2-171*x-360;
```

$$A := x^4 + 25\,x^3 + 145\,x^2 - 171\,x - 360 \tag{1}$$

```
> B := x^5+14*x^4+15*x^3-x^2-14*x-15;
```

$$B := x^5 + 14\,x^4 + 15\,x^3 - x^2 - 14\,x - 15 \tag{2}$$

```
> Bound := maxnorm(A)*maxnorm(B)*min(nops(A),nops(B));
```

$$\mathit{Bound} := 27000 \tag{3}$$

```
> p1 := 43;
  modp(A,p1);
  C1 := modp( expand(modp(A,p1) * modp(B,p1)), p1 );
```

$$p1 := 43 \tag{4}$$

$$x^4 + 25\,x^3 + 16\,x^2 + x + 27$$

$$C1 := x^9 + 39\,x^8 + 37\,x^7 + 40\,x^6 + 27\,x^5 + 12\,x^4 + 20\,x^3 + 20\,x^2 + 37\,x + 25$$

```
> p2 := nextprime(p1);
  C2 := Expand(A*B) mod p2;
```

$$p2 := 47 \tag{5}$$

$$C2 := x^9 + 39\,x^8 + 40\,x^7 + 24\,x^6 + 40\,x^5 + 16\,x^4 + 27\,x^3 + 15\,x^2 + 38\,x + 42$$

```
> p3 := nextprime(p2);
  C3 := Expand(A*B) mod p3;
```

$$p3 := 53 \tag{6}$$

$$C3 := x^9 + 39\,x^8 + 33\,x^7 + 7\,x^6 + 18\,x^5 + 47\,x^4 + 51\,x^3 + 49\,x^2 + 26\,x + 47$$

```
> M := p1*p2*p3;
```

$$M := 107113 \tag{7}$$

```
> C := chrem( [C1,C2,C3], [p1,p2,p3] );
```

$$C := x^9 + 39\,x^8 + 510\,x^7 + 2233\,x^6 + 106495\,x^5 + 98998\,x^4 + 99479\,x^3 + 579\,x^2 + 7605\,x + 5400 \tag{8}$$

Put G in the symmetric range for the integers modulo m.

```
> mods( C, M );
```

$$x^9 + 39\,x^8 + 510\,x^7 + 2233\,x^6 - 618\,x^5 - 8115\,x^4 - 7634\,x^3 + 579\,x^2 + 7605\,x + 5400 \tag{9}$$

```
> expand( A*B );
```

$$x^9 + 39\,x^8 + 510\,x^7 + 2233\,x^6 - 618\,x^5 - 8115\,x^4 - 7634\,x^3 + 579\,x^2 + 7605\,x + 5400 \tag{10}$$