Hensel lifting example : monic case

```
> a := x^5-19*x^3+9*x^2+84*x-108;
```

$$a := x^5 - 19\,x^3 + 9\,x^2 + 84\,x - 108$$

Let us try to factor a over $\mathbb{Z}$.

```
> Factor(a) mod 5;
```

$$\left(x^2 + 3\right)\,(x + 1)\,(x + 2)^2$$

```
> Factor(a) mod 7;
```

$$\left(x^3 + 2\right)\,\left(x^2 + 2\right)$$

Perhaps a has a quadratic and cubic factor.

```
> p := 7;
  `mod` := mods;
```

$$p := 7$$

$$mod := mods$$

```
> u0 := x^3+2;
```

$$u0 := x^3 + 2$$

```
> w0 := x^2+2;
```

$$w0 := x^2 + 2$$

Now, to perform Hensel lifting modulo , we need to ensure that u0 and w0 are relatively prime modulo p.

```
> Gcd(u0,w0) mod p;
```

$$1$$

The first order approximations are just

```
> u := u0; w := w0;
```

$$u := x^3 + 2$$

$$w := x^2 + 2$$

```
> e1 := expand( a - u*w );
```

$$e1 := -21\,x^3 + 7\,x^2 + 84\,x - 112$$

```
> c1 := e1/p;
```

$$c1 := -3\,x^3 + x^2 + 12\,x - 16$$

Solve mod using the extended Euclidean algorithm.

```
> Gcdex( w0, u0, x, 's', 't' ) mod p;
```

$$1$$

Now we want to find the solution to where we have .

```
> u1 := Rem(c1*s,u0,x,'q') mod p;
```

$$u1 := -x + 1$$

```
> w1 := Expand( w0*q+c1*t ) mod p;
```

$$w1 := -2$$

```
> expand(u1*w0 + w1*u0 = c1) mod p;
```

$$-3\,x^3 + x^2 - 2\,x - 2 = -3\,x^3 + x^2 - 2\,x - 2$$

Now we want the new th order p-adic approximations

```
> u := u + u1*p;
```

$$u := x^3 - 7\,x + 9$$

```
> w := w + w1*p;
```

$$w := x^2 - 12$$

```
> e2 := expand( a - u*w );
```

$$e2 := 0$$

Since the error is zero we are done.

```
> factor(a);
```

$$\left(x^3 - 7\,x + 9\right)\left(x^2 - 12\right)$$