Hensel lifting example.

This procedure solves $\sigma\, a + \tau\, b = c$ for σ and τ in Zp[x]

```
> DiophantSolve := proc(a,b,c,x,p)
  local g,sigma,tau,q,s,t;
      g := Gcdex(a,b,x,'s','t') mod p;
      if g <> 1 then error "a and b are not relatively prime!" fi;
      sigma := Rem(c*s,b,x,'q') mod p;
      # c s a = b (aq) + sigma a
      tau := Expand(c*t+q*a) mod p;
      return( sigma,tau );
  end:
```

```
> a := 10*x^5-59*x^3+45*x^2+84*x-108;
```

$$a := 10\,x^5 - 59\,x^3 + 45\,x^2 + 84\,x - 108$$

```
> b := 2*x^5-3*x^3-5*x^2+4*x^4+4*x+18;
```

$$b := 2\,x^5 - 3\,x^3 - 5\,x^2 + 4\,x^4 + 4\,x + 18$$

```
> gcd(a,b);
```

$$2\,x^3 - 7\,x + 9$$

Use Hensel lifting to find g = GCD(a, b) where, note, a and b are primitive.

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

$$mod := mods$$

$$p := 7$$

```
> u0 := Gcd(a,b) mod p;
```

$$u0 := x^3 + 1$$

```
> w0 := Quo(a,u0,x) mod p;
```

$$w0 := 3\,x^2 - 3$$

Hensel lifting modulo p^k . Ensure $GCD\left(u_0, w_0\right) = 1$.

```
> Gcd(u0,w0) mod 7;
```

$$x + 1$$

I'll try another prime.

```
> p := 11;
```

$$p := 11$$

```
> u0 := Gcd(a,b) mod p;
```

$$u0 := x^3 + 2\,x - 1$$

```
> w0 := Quo(a,u0,x) mod p;
```

$$w0 := -x^2 - 2$$

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

$$1$$

```
> alpha := lcoeff(a);
```

$$\alpha := 10$$

```
> a := alpha*a;
```

$$a := 100\,x^5 - 590\,x^3 + 450\,x^2 + 840\,x - 1080$$

```
> u0 := alpha*u0/lcoeff(u0) mod p;
```

$$u0 := -x^3 - 2\,x + 1$$

```
> w0 := alpha*w0/lcoeff(w0) mod p;
```

$$w0 := -x^2 - 2$$

Just to check that the new a and u0, w0 satisfy $a - u0\,w0 = 0 \ \mathbf{mod}\ p$.

```
> expand( a - u0*w0 ) mod p;
```

$$0$$

The first order approximations are just

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

$$u := -x^3 - 2\,x + 1$$

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

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

$$e1 := 99\,x^5 - 594\,x^3 + 451\,x^2 + 836\,x - 1078$$

```
> c1 := (e1/p) mod p;
```

$$c1 := x^3 - x - 3\,x^2 + 1 - 2\,x^5$$

```
> u1,w1 := DiophantSolve(w0,u0,c1,x,p);
```

$$u1, w1 := -5\,x + 5, 2\,x^2$$

```
> Expand( u1*w0 + w1*u0 - c1 ) mod p;
```

$$0$$

Now we want the new $k + 1$th order p-adic approximations

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

$$u := -x^3 - 57\,x + 56$$

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

$$w := 21\,x^2 - 2$$

```
> u := alpha * u/lcoeff(u) mod p^2;
```

$$u := 10\,x^3 - 35\,x + 45$$

```
> w := alpha * w/lcoeff(w) mod p^2;
```

$$w := 10\,x^2 - 24$$

A check that they really are 2nd order approximations

```
> expand( a - u*w ) mod p^2;
```

$$0$$

Computer the new error. Since it's zero we are done.

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

$$e2 := 0$$

```
> u,w := primpart(u),primpart(w);
```

$$u, w := 2\,x^3 - 7\,x + 9, 5\,x^2 - 12$$