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:
```

```
> p := 5;
```

$$p := 5$$

```
> `mod` := mods;
```

$$mod := mods$$

```
> a := 16*x^2+58*x+7;
```

$$a := 16\,x^2 + 58\,x + 7$$

```
> u0,w0 := x+1, x+2;
```

$$u0, w0 := x + 1, x + 2$$

Check that the conditions required for Hensel lifting to work

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

$$0$$

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

$$1$$

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

$$\alpha := 16$$

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

$$a := 256\,x^2 + 928\,x + 112$$

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

$$u, w := x + 1, x + 2$$

```
> u,w := (alpha*u mod p, 16*w mod p);
```

$$u, w := x + 1, x + 2$$

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

$$e1 := 255\,x^2 + 925\,x + 110$$

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

$$c1 := x^2 + 2$$

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

$$u1, w1 := -2, x + 1$$

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

$$0$$

```
> u,w := (u0 + u1*p, w0 + w1*p);
```

$$u, w := -9 + x, 6\,x + 7$$

```
> u,w := (alpha*u mod p^2, alpha/6*w mod p^2);
```

$$u, w := 6 - 9\,x, \text{-}9\,x + 2$$

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

$$e2 := 175\,x^2 + 1000\,x + 100$$

```
> c2 := e2/25 mod p;
```

$$c2 := 2\,x^2 - 1$$

```
> u2,w2 := DiophantSolve(w0,u0,c2,x,p);
```

$$u2, w2 := 1, 2\,x + 2$$

```
> u,w := (u+u2*p^2,w+w2*p^2);
```

$$u, w := 31 - 9\,x, 41\,x + 52$$

```
> u,w := (u/(-9)*alpha mod p^3, w/(41)*alpha mod p^3);
```

$$u, w := 56 + 16\,x, 16\,x + 2$$

```
> e3 := expand( a-u*w );
```

$$e3 := 0$$

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

$$u := 7 + 2\,x$$

$$w := 8\,x + 1$$