Assignment 4 Question 2 (Hensel Lifting)

Part (a) (monic case)

```
> restart;
```

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

$$mod := mods$$

$$p := 7$$

```
> a := x^4-2*x^3-233*x^2-214*x+85;
```

$$a := x^4 - 2\,x^3 - 233\,x^2 - 214\,x + 85$$

```
> u0 := x^2-3*x-2;
```

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

```
> w0 := x^2+x+3;
```

$$w0 := x^2 + x + 3$$

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

$$0$$

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

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

$$1$$

The first order approximations are just

```
> u1 := u0; w1 := w0;
```

$$u1 := x^2 - 3\,x - 2$$

$$w1 := x^2 + x + 3$$

```
> e1 := expand( a - u1*w1 );
```

$$e1 := -231\,x^2 - 203\,x + 91$$

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

$$c1 := -33\,x^2 - 29\,x + 13$$

Solve $s\,w0 + t\,u0 = 1 \bmod p$ using the extended Euclidean algorithm.

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

$$1$$

```
> s, t;
```

$$-x - 1,\ x - 2$$

Now we want to find the solution to $\sigma\,w0 + \tau\,u0 = c_k$. We have

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

$$\sigma := -2\,x + 1$$

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

$$\tau := 2x + 2$$

Now let's just verify that the solution is correct

```
> Expand( sigma*w0 + tau*u0 = c1 ) mod p;
```

$$2x^2 - x - 1 = 2x^2 - x - 1$$

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

```
> u2 := u1 + sigma*p;
```

$$u2 := x^2 - 17x + 5$$

```
> w2 := w1 + tau*p;
```

$$w2 := x^2 + 15x + 17$$

A check that they really are 2nd order approximations

```
> Expand( a - u2*w2 ) mod p^2;
```

$$0$$

```
> e2 := expand( a - u2*w2 );
```

$$e2 := 0$$

Since the error is zero we are done. The solution is

```
> a = u2*w2;
```

$$x^4 - 2x^3 - 233x^2 - 214x + 85 = (x^2 - 17x + 5)(x^2 + 15x + 17)$$

Part (b) (the non-monic case)

```
> a := 48*x^4-22*x^3+47*x^2+144;
```

$$a := 48x^4 - 22x^3 + 47x^2 + 144$$

```
> u0 := x^2+4*x+2; w0 := x^2+4*x+5;
```

$$u0 := x^2 + 4x + 2$$

$$w0 := x^2 + 4x + 5$$

```
> Expand(a-6*u0*w0) mod p;
```

$$0$$

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

$$1$$

Okay, so we are able to use this prime. We need to fix the leading coefficients. We multiply a(x) by

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

$$\alpha := 48$$

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

$$a := 2304x^4 - 1056x^3 + 2256x^2 + 6912$$

Now adjust u0 and w0 so that lcoeff(u0,x) = lcoeff(w0,x) = alpha mod p so that the new a (x) satisfies

a(x) == u0 w0 (mod p)

```
> u0 := alpha*u0 mod p;
```

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

```
> w0 := alpha*w0 mod p;
```

$$w0 := -x^2 + 3x + 2$$

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

$$0$$

```
> u1 := u0; w1 := w0;
```

$$u1 := -x^2 + 3x - 2$$

$$w1 := -x^2 + 3x + 2$$

```
> e1 := expand( a-u1*w1 );
```

$$e1 := 2303x^4 - 1050x^3 + 2247x^2 + 6916$$

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

$$c1 := 329x^4 - 150x^3 + 321x^2 + 988$$

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

$$1$$

```
> s,t;
```

$$2, -2$$

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

$$\sigma := x$$

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

$$\tau := 2x + 3$$

```
> u2 := u1 + p*sigma;
```

$$u2 := -x^2 + 10x - 2$$

```
> w2 := w1 + p*tau;
```

$$w2 := -x^2 + 17x + 23$$

Now we need to force the leading coefficients to be $\alpha \bmod p^2$.

```
> u2 := alpha/lcoeff(u2,x)*u2 mod p^2;
```

$$u2 := -x^2 + 10x - 2$$

```
> w2 := alpha/lcoeff(w2,x)*w2 mod p^2;
```

$$w2 := -x^2 + 17x + 23$$

```
> e2 := expand( a-u2*w2 );
```

$$e2 := 2303x^4 - 1029x^3 + 2107x^2 - 196x + 6958$$

The error in the second approximation is not zero so we continue.

```
> c2 := e2/p^2;
```

$$c2 := 47x^4 - 21x^3 + 43x^2 - 4x + 142$$

```
> sigma := Rem(c2*s,u0,x,'q') mod p;
```

$$\sigma := x$$

```
> tau := Expand( w0*q+c2*t ) mod p;
```

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

```
> u3 := u2 + p^2*sigma;
```

$$u3 := -x^2 + 59\,x - 2$$

```
> w3 := w2 + p^2*tau;
```

$$w3 := 97\,x^2 - 81\,x - 26$$

```
> u3 := alpha/lcoeff(u3)*u3 mod p^3;
```

$$u3 := 48\,x^2 - 88\,x + 96$$

```
> w3 := alpha/lcoeff(w3)*w3 mod p^3;
```

$$w3 := 48\,x^2 + 66\,x + 72$$

```
> e3 := expand( a-u3*w3 );
```

$$e3 := 0$$

So we are done. We now make u3 and w3 primitive.

```
> u := primpart(u3);
```

$$u := 6\,x^2 - 11\,x + 12$$

```
> w := primpart(w3);
```

$$w := 8\,x^2 + 11\,x + 12$$

```
> expand( a-alpha*u*w );
```

$$0$$