Assignment 4 Question 1

Part (a)

Determine the p-adic representation of a=116 with p=5 .

```
> a := 116;
```

$$a := 116$$

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

$$p := 5$$

I'll use modp(a, p) for the positive range

```
> for k from 0 while a <> 0 do
      u[k] := modp(a,p);
      a := iquo( a-u[k], p );
  od;
```

$$u_0 := 1$$

$$a := 23$$

$$u_1 := 3$$

$$a := 4$$

$$u_2 := 4$$

$$a := 0$$

```
> u = add( u[k]*``(p)^k, k=0..2 );
```

$$u = 1 + 3\ (5) + 4\ (5)^2$$

```
> expand(%);
```

$$u = 116$$

```
> a := 116;
```

$$a := 116$$

Now for the symmetric range using mods(a, p)

```
> for k from 0 while a > 0 do
      u[k] := mods(a,p);
      a := iquo(a-u[k],p);
  od;
```

$$u_0 := 1$$

$$a := 23$$

$$u_1 := -2$$

$$a := 5$$

$$u_2 := 0$$

$$a := 1$$

$$u_3 := 1$$

$$a := 0$$

```
> u = add( u[k]*``(p)^k, k=0..3 );
```

$$u = 1 - 2\,(5) + (5)^3$$

Part (b)

Suppose $u = u_0 + u_1 \cdot p + \ldots + u_k \cdot p^{k-1}$ and u = $v_0 + v_1 \cdot p + \ldots + v_{k-1} \cdot p^{k-1}$ both satisfy the conditions $\frac{p}{2} < u_i < \frac{p}{2}$ and $\frac{p}{2} < v_i < \frac{p}{2}$. Then

$$0 = (u_0 - v_0) + (u_1 - v_1) \cdot p + \ldots + (u_{k-1} - v_{k-1}) \cdot p^{k-1}.$$

Reducing mod p we have $0 \equiv (u_0 - v_0) \pmod{p}$ which implies

$$p \mid (u_0 - v_0).$$

Now the conditions on u_0 and v_0 imply $-p < u_0 - v_0 < p$ and hence $u_0 - v_0 = 0$. Dividing the above equation by p we obtain

$$0 = (u_1 - v_1) + (u_2 - v_2) + \ldots + (u_{k-1} - v_{k-1}) \cdot p^{k-2}.$$

Repeating the above argument we show that $u_1 = v_1$ then repeating again we show that $u_i = v_i$ for all i thus we have uniqueness for this symmetric p-adic representation.

Part (c)

Given the polynomial

```
> a := x^6-531*x^5+94137*x^4-5598333*x^3+4706850*x^2-1327500*x+125000;
```

$$a := x^6 - 531\,x^5 + 94137\,x^4 - 5598333\,x^3 + 4706850\,x^2 - 1327500\,x + 125000$$

compute $\sqrt[3]{a(x)}$ if the cube root exists, i.e. solve $F(u) = u^3 - a(x) = 0$ for $u(x)$. We have that $F'(u) = 3\,u^2$. First we need to compute the cube root modulo 5 if it exists. We will do all arithmetic in the symmetric range from now on.

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

$$mod := mods$$

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

$$p := 5$$

```
> a mod p;
```

$$x^6 - x^5 + 2\,x^4 + 2\,x^3$$

We will get a cube root mod 5 by factoring

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

$$x^3\,(x-2)^3$$

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

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

```
> a-Expand(u0^3) mod p;
```

$$0$$

We need a bound on the size of the largest coefficient in the cube root. We can use the Mignotte bound for this. Hence we will stop the iteration if p^k is greater than

```
> B := 2^6*ceil(sqrt(6+1))*maxnorm(a);
```

$$B := 1074879936$$

We are ready to go

```
> u := u0;
```

$$u := x^2 - 2\,x$$

```
> for k from 1 while p^k <= B do
     e[k] := expand(u^3) - a;
     if e[k] = 0 then cuberoot := u; break; fi;
     c[k] := e[k]/p^k;
     uk := Quo(-c[k],3*u0^2,x,'r') mod p;
     if r <> 0 then print(`non-zero remainder`); break; fi;
     u := u + uk*p^k;
   od;
```

$$e_1 := 525\,x^5 - 94125\,x^4 + 5598325\,x^3 - 4706850\,x^2 + 1327500\,x - 125000$$

$$c_1 := 105\,x^5 - 18825\,x^4 + 1119665\,x^3 - 941370\,x^2 + 265500\,x - 25000$$

$$uk := 0$$

$$u := x^2 - 2\,x$$

$$e_2 := 525\,x^5 - 94125\,x^4 + 5598325\,x^3 - 4706850\,x^2 + 1327500\,x - 125000$$

$$c_2 := 21\,x^5 - 3765\,x^4 + 223933\,x^3 - 188274\,x^2 + 53100\,x - 5000$$

$$uk := -2\,x + 2$$

$$u := x^2 - 52\,x + 50$$

$$e_3 := 375\,x^5 - 85875\,x^4 + 5442125\,x^3 - 4293750\,x^2 + 937500\,x$$

$$c_3 := 3\,x^5 - 687\,x^4 + 43537\,x^3 - 34350\,x^2 + 7500\,x$$

$$uk := -x$$

$$u := x^2 - 177\,x + 50$$

$$e_4 := 0$$

```
> cuberoot;
```

$$x^2 - 177\,x + 50$$

Let's check.

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

$$(x^2 - 177\,x + 50)^3$$

For the second polynomial

```
> b := x^6-406*x^5+94262*x^4-5598208*x^3+4706975*x^2-1327375*x+125125;
```

$$b := x^6 - 406\,x^5 + 94262\,x^4 - 5598208\,x^3 + 4706975\,x^2 - 1327375\,x + 125125$$

```
> b mod p;
```

$$x^6 - x^5 + 2\,x^4 + 2\,x^3$$

We try to guess the cube root mod 5.

```
> Factor(b) mod p;
```

$$x^3\,(x-2)^3$$

There is a cube root

```
> u0 := Expand( x*(x-2) ) mod p;
```

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

```
> B := 2^6*ceil(sqrt(6+1))*maxnorm(a);
```

$$B := 1074879936$$

```
> u := u0;
```

$$u := x^2 - 2\,x$$

```
> for k from 1 while p^k <= B do
    e[k] := expand(u^3) - b;
    if e[k] = 0 then cuberoot := u; break; fi;
    c[k] := e[k]/p^k;
    uk := Quo(-c[k],3*u0^2,x,'r') mod p;
    if r <> 0 then print(`non-zero remainder`); break; fi;
    u := u + uk*p^k;
  od;
```

$$e_1 := 400\,x^5 - 94250\,x^4 + 5598200\,x^3 - 4706975\,x^2 + 1327375\,x - 125125$$

$$c_1 := 80\,x^5 - 18850\,x^4 + 1119640\,x^3 - 941395\,x^2 + 265475\,x - 25025$$

$$uk := 0$$

$$u := x^2 - 2\,x$$

$$e_2 := 400\,x^5 - 94250\,x^4 + 5598200\,x^3 - 4706975\,x^2 + 1327375\,x - 125125$$

$$c_2 := 16\,x^5 - 3770\,x^4 + 223928\,x^3 - 188279\,x^2 + 53095\,x - 5005$$

$$uk := -2\,x + 2$$

$$u := x^2 - 52\,x + 50$$

$$e_3 := 250\,x^5 - 86000\,x^4 + 5442000\,x^3 - 4293875\,x^2 + 937375\,x - 125$$

$$c_3 := 2\,x^5 - 688\,x^4 + 43536\,x^3 - 34351\,x^2 + 7499\,x - 1$$

$$uk := x$$

non-zero remainder

This time the algorithm terminated prematurely meaning there is no cube-root. Double check

```
> factor(b);
```

$$x^6 - 406\,x^5 + 94262\,x^4 - 5598208\,x^3 + 4706975\,x^2 - 1327375\,x + 125125$$