Sqrt P-adic Newton Iteration

Tell Maple to do all computations modulo p in the symmetric range.

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

$$mod := mods$$

Given the polynomial

```
> a := 49*x^4-238*x^3+513*x^2-544*x+256;
```

$$a := 49\,x^4 - 238\,x^3 + 513\,x^2 - 544\,x + 256$$

compute $\sqrt{a(x)}$ if the sqrt exists, i.e. solve $F(u) = u^2 - a(x) = 0$ for $u(x)$.
We have that F'(u) = 2 u. Let's first compute the sqrt modulo 5.

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

$$p := 5$$

```
> amod5 := a mod p;
```

$$amod5 := -x^4 + 2\,x^3 - 2\,x^2 + x + 1$$

We obtain that a sqrt mod 5 (by trial and error for now) is

```
> u0 := 2*x^2-2*x+1;
```

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

```
> amod5 - ( expand(u0^2) mod p );
```

$$0$$

We need a bound on the size of the largest coefficient in the sqrt. We can use the Mignotte bound for this. Hence we must run the iteration until p^k is greater than $2\,B$ where

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

$$d := 4$$

$$B := 26112$$

We are ready to go: our fo

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

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

Note that the error is calculated over Z not mod p !!

```
> e1 := a - expand(u^2);
```

$$e1 := 45\,x^4 - 230\,x^3 + 505\,x^2 - 540\,x + 255$$

```
> e1 / 5;
```

$$9\,x^4 - 46\,x^3 + 101\,x^2 - 108\,x + 51$$

```
> u1 := Quo(e1/5,2*u0,x,'r') mod p;
```

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

```
> r;
```

$$0$$

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

$$u := 7x^2 + 8x - 9$$

```
> e2 := a - expand(u^2);
```

$$e2 := -350x^3 + 575x^2 - 400x + 175$$

```
> e2 / 25;
```

$$-14x^3 + 23x^2 - 16x + 7$$

```
> u2 := Quo(e2/25,2*u0,x,'r') mod p;
```

$$u2 := -x + 1$$

```
> r;
```

$$0$$

```
> u := u + u2*p^2;
```

$$u := 7x^2 - 17x + 16$$

```
> e3 := a - expand(u^2);
```

$$e3 := 0$$

We are done.

Consider $a(x) = 9x^2 + 18x + 24$. This polynomial obviously cannot be a perfect square because 24 is not a perfect square.

```
> a := 9*x^2+18*x+24;
```

$$a := 9x^2 + 18x + 24$$

```
> amod5 := a mod 5;
```

$$amod5 := -x^2 - 2x - 1$$

```
> u0 := 2*x+2;
```

$$u0 := 2x + 2$$

```
> expand( amod5 - u0^2 ) mod p;
```

$$0$$

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

$$u := 2x + 2$$

```
> e1 := expand( a - u^2 );
```

$$e1 := 5x^2 + 10x + 20$$

```
> e1/p;
```

$$x^2 + 2x + 4$$

```
> d1 := Quo(e1/p,2*u0,x,'r') mod p;
```

$$d1 := -x - 1$$

```
> r;
```

$$-2$$

Since $r \neq 0$ we conclude sqrt(a) is not a polynomial