Komputeralgebrai algoritmusok

Járai Antal

Ezek a programok csak szemléltetésre szolgálnak.

▶ 1. Történet

▶ 2. Algebrai alapok

▶ 3. Normál formák, reprezentáció

▶ 4. Aritmetika

▶ 5. Kínai maradékolás

▼ 6. Newton–iteráció, Hensel–felemelés

```
> restart;
```

▼ E 6.1. Példa.

```
> `mod`:=mods; p:=97; u:=-272300; u0:=u mod p; u1:=(u-u0)/p mod
  p;
  u2:=(u-(u0+u1*p))/p^2 mod p; u-(u0+u1*p+u2*p^2);
```

$$mod := mods$$
$$p := 97$$
$$u := -272300$$
$$u0 := -21$$
$$u1 := 6$$
$$u2 := -29$$
$$0 \qquad (6.1.1)$$

▼ E 6.2. Példa.

```
> p:=5; u:=14*x^2-11*x-15; u0:=u mod p; u1:=(u-u0)/p mod p;
  u2:=(u-(u0+u1*p))/p^2 mod p; u-(u0+u1*p+u2*p^2);
```

$$p := 5$$

$$u := 14\,x^2 - 11\,x - 15$$
$$u0 := -x^2 - x$$
$$u1 := -2\,x^2 - 2\,x + 2$$
$$u2 := x^2 - 1$$
$$0 \tag{6.2.1}$$

E 6.3. Példa.

```
> u:='u'; a:=36*x^4-180*x^3+93*x^2+330*x+121;
  F:=a-u^2; Fp:=diff(F,u);
```

$$u := u$$
$$a := 36\,x^4 - 180\,x^3 + 93\,x^2 + 330\,x + 121$$
$$F := 36\,x^4 - 180\,x^3 + 93\,x^2 + 330\,x + 121 - u^2$$
$$Fp := -2\,u \tag{6.3.1}$$

```
> a mod p;
```

$$x^4 - 2\,x^2 + 1 \tag{6.3.2}$$

```
> u0:=x^2-1; u[1]:=u0; d:=subs(u=u[1],Fp);
```

$$u0 := x^2 - 1$$
$$u_1 := x^2 - 1$$
$$d := -2\,x^2 + 2 \tag{6.3.3}$$

```
> u1:=-expand(subs(u=u[1],F)/p); u1:=Quo(u1,d,x) mod p;
```

$$u1 := -7\,x^4 + 36\,x^3 - 19\,x^2 - 66\,x - 24$$
$$u1 := x^2 + 2\,x - 2 \tag{6.3.4}$$

```
> u[2]:=u0+5*u1; u2:=-expand(subs(u=u[2],F)/p^2); u2:=Quo(u2,d,
  x) mod p;
```

$$u_2 := 6\,x^2 - 11 + 10\,x$$
$$u2 := 12\,x^3 - 5\,x^2 - 22\,x$$
$$u2 := -x \tag{6.3.5}$$

```
> u[3]:=u0+5*u1+5^2*u2; expand(subs(u=u[3],F));
```

$$u_3 := 6\,x^2 - 11 - 15\,x$$
$$0 \tag{6.3.6}$$

E 6.4. Példa.

```
> p:=5; `mod`:=mods;
  a:=x^4+x^3*y^2-x^2*y^4+x^2*y*z+2*x^2*z-2*x^2-2*x*y^3*z+x*y^2*
  z-x*y^2-y^2*z^2+y*z^2-y*z+z^2-2*z+1 mod p;
```

```
a:=collect(a,[y,z],`distributed`); sort(a,[y,z],tdeg);
F:=a-u^2; Fp:=diff(F,u);
```

$$p := 5$$

$$mod := mods$$

$$a := x^4 + x^3 y^2 - x^2 y^4 + x^2 y z + 2 x^2 z - 2 x^2 - 2 x y^3 z + x y^2 z - x y^2 - y^2 z^2 + y z^2 - y z + z^2 - 2 z + 1$$

$$a := x^4 - 2 x^2 + 1 - 2 x y^3 z + x y^2 z - y^2 z^2 + y z^2 + \left(x^2 - 1\right) y z + \left(2 x^2 - 2\right) z + \left(-x + x^3\right) y^2 + z^2 - x^2 y^4$$

$$-x^2 y^4 - 2 x y^3 z - y^2 z^2 + x y^2 z + y z^2 + \left(-x + x^3\right) y^2 + \left(x^2 - 1\right) y z + z^2 + \left(2 x^2 - 2\right) z + x^4 - 2 x^2 + 1$$

$$F := -x^2 y^4 - 2 x y^3 z - y^2 z^2 + x y^2 z + y z^2 + \left(-x + x^3\right) y^2 + \left(x^2 - 1\right) y z + z^2 + \left(2 x^2 - 2\right) z + x^4 - 2 x^2 + 1 - u^2$$

$$Fp := -2 u \tag{6.4.1}$$

```
> subs(y=0,z=0,a); u[1]:=x^2-1;
```

$$x^4 - 2 x^2 + 1$$

$$u_1 := x^2 - 1 \tag{6.4.2}$$

```
> d:=subs(u=u[1],Fp) mod p;
```

$$d := -2 x^2 + 2 \tag{6.4.3}$$

```
> FF:=expand(subs(u=u[1],F)) mod p;
  FF:=collect(%,[y,z],`distributed`);
  sort(%,[y,z],tdeg);
  u2:=0; u3:=-Quo(2*x^2-2,d,x) mod p;
  du[2]:=u2*y+u3*z; u[2]:=u[1]+du[2];
```

$$FF := -x^2 y^4 - 2 x y^3 z - y^2 z^2 + x y^2 z + y z^2 - x y^2 + x^3 y^2 + x^2 y z - y z + z^2 + 2 x^2 z - 2 z$$

$$FF := -2 x y^3 z + x y^2 z - y^2 z^2 + y z^2 + \left(x^2 - 1\right) y z + \left(2 x^2 - 2\right) z + \left(-x + x^3\right) y^2 + z^2 - x^2 y^4$$

$$-x^2 y^4 - 2 x y^3 z - y^2 z^2 + x y^2 z + y z^2 + \left(-x + x^3\right) y^2 + \left(x^2 - 1\right) y z + z^2 + \left(2 x^2 - 2\right) z$$

$$u2 := 0$$

$$u3 := 1$$

$$du_2 := z$$

$$u_2 := x^2 - 1 + z \tag{6.4.4}$$

```
> FF:=expand(subs(u=u[2],F)) mod p;
  FF:=collect(%,[y,z],`distributed`);
  sort(%,[y,z],tdeg);
  u22:=-Quo(x^3-x,d,x) mod p; u23:=-Quo(x^2-1,d,x) mod p; u33:=
```

```
-Quo(0,d,x) mod p;
du[3]:=u22*y^2+u23*y*z+u33*z^2; u[3]:=u[2]+du[3];
```

$$FF := -x^2 y^4 - 2 x y^3 z - y^2 z^2 + x y^2 z + y z^2 - x y^2 + x^3 y^2 + x^2 y z - y z$$

$$FF := -2 x y^3 z + x y^2 z - y^2 z^2 + y z^2 + \left(x^2 - 1\right) y z + \left(-x + x^3\right) y^2 - x^2 y^4$$

$$-x^2 y^4 - 2 x y^3 z - y^2 z^2 + x y^2 z + y z^2 + \left(-x + x^3\right) y^2 + \left(x^2 - 1\right) y z$$

$$u22 := -2 x$$

$$u23 := -2$$

$$u33 := 0$$

$$du_3 := -2 x y^2 - 2 y z$$

$$u_3 := x^2 - 1 + z - 2 x y^2 - 2 y z \tag{6.4.5}$$

```
> FF:=expand(subs(u=u[3],F)) mod p;
```

$$FF := 0 \tag{6.4.6}$$

E 6.5. Példa.

```
> p:=5; m:=p; a:=x^3+10*x^2-432*x+5040; a mod p; u:=x; w:=x^2
  -2;
  e:=expand(a-u*w);
```

$$p := 5$$

$$m := 5$$

$$a := x^3 + 10 x^2 - 432 x + 5040$$

$$x^3 - 2 x$$

$$u := x$$

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

$$e := 10 x^2 - 430 x + 5040 \tag{6.5.1}$$

```
> Gcdex(u,w,x,'s','t') mod p; s; t;
```

$$1$$

$$-2 x$$

$$2 \tag{6.5.2}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := 2 x^2 - 86 x + 1008$$

$$\sigma := x^3 + 2 x^2 - x$$

$$\tau := -x^2 - 2 x + 1 \tag{6.5.3}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

$$\sigma := x - 1$$

$$x + 2$$

$$\tau := 1 \tag{6.5.4}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := x + 5$$
$$w := x^2 - 7 + 5\,x$$
$$e := -450\,x + 5075$$
$$m := 25 \tag{6.5.5}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := -18\,x + 203$$
$$\sigma := x^2 - x$$
$$\tau := -x + 1 \tag{6.5.6}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

$$\sigma := -x + 2$$
$$1$$
$$\tau := 1 \tag{6.5.7}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := x + 30$$
$$w := x^2 + 43 - 20\,x$$
$$e := 125\,x + 3750$$
$$m := 125 \tag{6.5.8}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := x + 30$$
$$\sigma := -2\,x^2$$
$$\tau := 2\,x \tag{6.5.9}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

$$\sigma := 1$$
$$-2$$
$$\tau := 0 \tag{6.5.10}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := x + 30$$
$$w := x^2 + 168 - 20\,x$$
$$e := 0$$
$$m := 625 \tag{6.5.11}$$

E 6.6. Példa.

```
> p:=5; m:=p; a:=x^4+1; a mod p; u:=x^2+2; w:=x^2-2; expand(u*
  w) mod p;
  e:=expand(a-u*w);
```

$$p := 5$$
$$m := 5$$
$$a := x^4 + 1$$
$$x^4 + 1$$
$$u := x^2 + 2$$
$$w := x^2 - 2$$
$$x^4 + 1$$
$$e := 5 \tag{6.6.1}$$

```
> Gcdex(u,w,x,'s','t') mod p; s; t;
```

$$1$$
$$-1$$
$$1 \tag{6.6.2}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := 1$$
$$\sigma := -1$$
$$\tau := 1 \tag{6.6.3}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

$$\sigma := -1$$
$$0$$
$$\tau := 1 \tag{6.6.4}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := x^2 + 7$$
$$w := x^2 - 7$$
$$e := 50$$
$$m := 25 \tag{6.6.5}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := 2$$
$$\sigma := -2$$
$$\tau := 2 \tag{6.6.6}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

$$\sigma := -2$$
$$0$$
$$\tau := 2 \tag{6.6.7}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := x^2 + 57$$
$$w := x^2 - 57$$
$$e := 3250$$
$$m := 125 \tag{6.6.8}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := 26$$
$$\sigma := -1$$
$$\tau := 1 \tag{6.6.9}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

$$\sigma := -1$$
$$0$$
$$\tau := 1 \tag{6.6.10}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := x^2 + 182$$
$$w := x^2 - 182$$
$$e := 33125$$
$$m := 625 \tag{6.6.11}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := 53$$
$$\sigma := 2$$
$$\tau := -2 \tag{6.6.12}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

$$\sigma := 2$$
$$0$$
$$\tau := -2 \tag{6.6.13}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := x^2 - 1068$$
$$w := x^2 + 1068$$
$$e := 1140625$$
$$m := 3125 \tag{6.6.14}$$

E 6.7. Példa.

```
> p:=5; m:=p; a:=expand((2*x+5)*(6*x^2-10*x+7)); a mod p; u:=2*
  x; w:=x^2+2;
  e:=expand(a-u*w);
```

$$p := 5$$

$$m := 5$$

$$a := 12\,x^3 + 10\,x^2 - 36\,x + 35$$

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

$$u := 2\,x$$

$$w := x^2 + 2$$

$$e := 10\,x^3 + 10\,x^2 - 40\,x + 35 \qquad (6.7.1)$$

```
> Gcdex(u,w,x,'s','t') mod p; s; t;
```

$$1$$

$$x$$

$$-2 \qquad (6.7.2)$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := 2\,x^3 + 2\,x^2 - 8\,x + 7$$

$$\sigma := 2\,x^4 + 2\,x^3 + 2\,x^2 + 2\,x$$

$$\tau := x^3 + x^2 + x + 1 \qquad (6.7.3)$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

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

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

$$\tau := 2\,x + 1 \qquad (6.7.4)$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := 12\,x + 5$$

$$w := x^2 - 3 - 10\,x$$

$$e := 125\,x^2 + 50\,x + 50$$

$$m := 25 \qquad (6.7.5)$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := 5\,x^2 + 2\,x + 2$$

$$\sigma := 2\,x^2 + 2\,x$$

$$\tau := x + 1 \qquad (6.7.6)$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

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

$$2$$

$$\tau := 1 \qquad (6.7.7)$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := 12\,x + 30$$

$$w := x^2 + 22 + 40\,x$$

$$e := -500\,x^2 - 1500\,x - 625$$

$$m := 125 \tag{6.7.8}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := -4\,x^2 - 12\,x - 5$$

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

$$\tau := -2\,x^2 - x \tag{6.7.9}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

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

$$x - 2$$

$$\tau := 0 \tag{6.7.10}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := 12\,x + 30$$

$$w := x^2 - 103 - 210\,x$$

$$e := 2500\,x^2 + 7500\,x + 3125$$

$$m := 625 \tag{6.7.11}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := 4\,x^2 + 12\,x + 5$$

$$\sigma := -x^3 + 2\,x^2$$

$$\tau := 2\,x^2 + x \tag{6.7.12}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

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

$$-x + 2$$

$$\tau := 0 \tag{6.7.13}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); e:=expand(a-u*w);
  m:=m*p;
```

$$u := 12\,x + 30$$

$$w := x^2 + 522 + 1040\,x$$

$$e := -12500\,x^2 - 37500\,x - 15625$$

$$m := 3125 \tag{6.7.14}$$

E 6.8. Példa.

```
> p:=5; m:=p; a:=expand((2*x+5)*(6*x^2-10*x+7));
  a mod p; u:=2*x; w:=x^2+2;
  alpha:=lcoeff(a); mu:=lcoeff(u); nu:=lcoeff(w);
  aa:=alpha*a; u:=alpha*u/mu mod m; w:=alpha*w/nu mod m;
  e:=expand(aa-u*w);
```

$$p := 5$$

$$m := 5$$

$$a := 12\,x^3 + 10\,x^2 - 36\,x + 35$$

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

$$u := 2\,x$$

$$w := x^2 + 2$$

$$\alpha := 12$$

$$\mu := 2$$

$$\nu := 1$$

$$aa := 144\,x^3 + 120\,x^2 - 432\,x + 420$$

$$u := 2\,x$$

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

$$e := 140\,x^3 + 120\,x^2 - 430\,x + 420 \qquad (6.8.1)$$

```
> Gcdex(u,w,x,'s','t') mod p; s; t;
```

$$1$$

$$x$$

$$-1 \qquad (6.8.2)$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := 28\,x^3 + 24\,x^2 - 86\,x + 84$$

$$\sigma := -2\,x^4 - x^3 - x^2 - x$$

$$\tau := 2\,x^3 + x^2 + x + 1 \qquad (6.8.3)$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

$$\sigma := x - 1$$

$$-x^2 + 2\,x - 1$$

$$\tau := -x + 1 \qquad (6.8.4)$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); m:=m*p;
  mu:=lcoeff(u); nu:=lcoeff(w);
  u:=alpha*u/mu mod m; w:=alpha*w/nu mod m;
  e:=expand(aa-u*w);
```

$$u := -3\,x + 5$$

$$w := 2\,x^2 - 6 + 5\,x$$

$$m := 25$$

$$\mu := -3$$
$$\nu := 2$$
$$u := 12\,x + 5$$
$$w := 12\,x^2 - 11 + 5\,x$$
$$e := -325\,x + 475 \tag{6.8.5}$$

```
> c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
```

$$c := -13\,x + 19$$
$$\sigma := 2\,x^2 - x$$
$$\tau := -2\,x + 1 \tag{6.8.6}$$

```
> sigma:=Rem(sigma,w,x,'q') mod p; q; tau:=expand(tau+q*u) mod
  p;
```

$$\sigma := -x + 1$$
$$1$$
$$\tau := 1 \tag{6.8.7}$$

```
> u:=expand(u+tau*m); w:=expand(w+sigma*m); m:=m*p;
  mu:=lcoeff(u); nu:=lcoeff(w);
  u:=alpha*u/mu mod m; w:=alpha*w/nu mod m;
  e:=expand(aa-u*w);
```

$$u := 12\,x + 30$$
$$w := 12\,x^2 + 14 - 20\,x$$
$$m := 125$$
$$\mu := 12$$
$$\nu := 12$$
$$u := 12\,x + 30$$
$$w := 12\,x^2 + 14 - 20\,x$$
$$e := 0 \tag{6.8.8}$$

```
> mu:=igcd(coeffs(u)); u:=u/mu;
  nu:=igcd(coeffs(w)); w:=w/nu;
```

$$\mu := 6$$
$$u := 2\,x + 5$$
$$\nu := 2$$
$$w := 6\,x^2 - 10\,x + 7 \tag{6.8.9}$$

A 6.1. Algoritmus.

```
> replace_lc:=proc(a,x,alpha) local aa,aalpha,t;
    aa:=expand(a);
    aalpha:=lcoeff(aa,x,'t');
    aa:=expand(aa-aalpha*t+alpha*t);
  end;
```

```
replace_lc := proc(a, x, alpha)                                   (6.9.1)
    local aa, aalpha, t;
    aa := expand(a);
    aalpha := lcoeff(aa, x, 't');
    aa := expand(aa - aalpha * t + alpha * t)
end proc
```

```
> UnivariateHensel:=proc(a,u1,w1,x,p,B,gamma)
    local aa,alpha,e,u,uu,w,ww,m,s,t,q,c,sigma,tau;
    aa:=expand(a); alpha:=lcoeff(aa); aa:=gamma*aa;
    uu:=expand(u1); uu:=uu/lcoeff(uu)*gamma mod p;
    ww:=expand(w1); ww:=ww/lcoeff(ww)*alpha mod p;
    Gcdex(uu,ww,x,'s','t') mod p;
    u:=replace_lc(uu,x,gamma); w:=replace_lc(ww,x,alpha);
    e:=expand(aa-u*w); m:=p;
    while e<>0 and m<2*B*gamma do
      c:=e/m; sigma:=expand(s*c) mod p; tau:=expand(t*c) mod p;
      sigma:=Rem(sigma,ww,x,'q') mod p;
      tau:=expand(tau+q*uu) mod p;
      u:=expand(u+tau*m); w:=expand(w+sigma*m);
      e:=expand(aa-u*w); m:=m*p;
    od;
    if e=0 then
      u:=u/igcd(coeffs(u)); w:=w/igcd(coeffs(w));
      [u,w];
    else FAIL fi;
  end;
```

```
UnivariateHensel := proc(a, u1, w1, x, p, B, gamma)               (6.9.2)
    local aa, alpha, e, u,
    uu, w, ww, m, s, t, q, c, sigma, tau;
    aa := expand(a);
    alpha := lcoeff(aa);
    aa := gamma * aa;
    uu := expand(u1);
    uu := mod(uu * gamma / lcoeff(uu), p);
    ww := expand(w1);
    ww := mod(ww * alpha / lcoeff(ww), p);
    mod(Gcdex(uu, ww, x, 's',
    't'), p);
    u := replace_lc(uu, x, gamma);
    w := replace_lc(ww, x, alpha);
    e := expand(aa - u * w);
    m := p;
```

```
    while e <> 0 and m < 2*B*gamma do
        c := e / m;
        sigma := mod(expand(s*c), p);
        tau := mod(expand(t*c), p);
        sigma := mod(Rem(sigma, ww, x, 'q'), p);
        tau := mod(expand(tau + q*uu), p);
        u := expand(u + tau*m);
        w := expand(w + sigma*m);
        e := expand(aa - u*w);
        m := m*p
    end do;
    if e = 0 then
        u := u / igcd(coeffs(u));
        w := w / igcd(coeffs(w));
        [u, w]
    else
        FAIL
    end if
end proc
```

E 6.9. Példa.

```
> debug(UnivariateHensel); debug(replace_lc);
```

$$\mathit{UnivariateHensel}$$

$$\mathit{replace_lc} \tag{6.10.1}$$

```
> UnivariateHensel(a,2*x,2*x^2-1,x,5,10000,2);
{--> enter UnivariateHensel, args = 12*x^3+10*x^2-36*x+35,
2*x, 2*x^2-1, x, 5, 10000, 2
```

$$aa := 12\,x^3 + 10\,x^2 - 36\,x + 35$$

$$\alpha := 12$$

$$aa := 24\,x^3 + 20\,x^2 - 72\,x + 70$$

$$uu := 2\,x$$

$$uu := 2\,x$$

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

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

$$1$$

```
{--> enter replace_lc, args = 2*x, x, 2
```

$$aa := 2\,x$$

$$aalpha := 2$$

$$aa := 2\,x$$

```
<-- exit replace_lc (now in UnivariateHensel) = 2*x}
```

$$u := 2\,x$$

```
{--> enter replace_lc, args = 2*x^2-1, x, 12
```

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

$$aalpha := 2$$

$$aa := 12\,x^2 - 1$$

```
<-- exit replace_lc (now in UnivariateHensel) = 12*x^2-1}
```

$$w := 12\,x^2 - 1$$

$$e := 20\,x^2 - 70\,x + 70$$

$$m := 5$$

$$c := 4\,x^2 - 14\,x + 14$$

$$\sigma := -x^3 + x^2 - x$$

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

$$\sigma := x - 2$$

$$\tau := 1$$

$$u := 2\,x + 5$$

$$w := 12\,x^2 - 11 + 5\,x$$

$$e := -50\,x^2 - 75\,x + 125$$

$$m := 25$$

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

$$\sigma := -2\,x^3 + 2\,x^2$$

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

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

$$\tau := 0$$

$$u := 2\,x + 5$$

$$w := 12\,x^2 + 14 - 20\,x$$

$$e := 0$$

$$m := 125$$

$$u := 2\,x + 5$$

$$w := 6\,x^2 - 10\,x + 7$$

$$\left[2\,x + 5,\ 6\,x^2 - 10\,x + 7\right]$$

```
<-- exit UnivariateHensel (now at top level) = [2*x+5, 6*
x^2-10*x+7]}
```

$$\left[2\,x + 5,\ 6\,x^2 - 10\,x + 7\right] \tag{6.10.2}$$

E 6.10. Példa.

```
> p:=5; l:=1; a:=x^2*y^4*z-x*y^9*z^2+x*y*z^3+2*x-y^6*z^4-2*y^5*
  z;
  subs(y=1,z=1,a) mod p^l;
```

$$p := 5$$

$$l := 1$$

$$a := x^2 y^4 z - x y^9 z^2 + x y z^3 + 2 x - y^6 z^4 - 2 y^5 z$$

$$x^2 + 2 x + 2 \tag{6.11.1}$$

```
> u[1]:=x-2; w[1]:=x-1; expand(u[1]*w[1]) mod p^l;
```

$$u_1 := x - 2$$

$$w_1 := x - 1$$

$$x^2 + 2 x + 2 \tag{6.11.2}$$

```
> aa:=expand(subs(y=Y+1,z=Z+1,a)) mod p^l;
```

$$aa := 2 + 2 x + x^2 - Y - Z + x^2 Y^4 Z - x^2 Y^3 Z + x^2 Y^2 Z - x^2 Y Z + Y Z \tag{6.11.3}$$
$$+ x^2 Y^4 - x^2 Y^3 + x^2 Y^2 - x^2 Y + x^2 Z - Z^2 - Y^6 Z^2$$
$$+ Y^6 Z - Y^5 Z^2 - Y^5 Z - Y Z^2 + 2 x Y + x Z + x Y^3 - x Y^2$$
$$+ 2 x Z^2 - x Y^4 - x Y^5 + x Y^6 - x Y^7 + x Y^8 - x Y^9 + Y Z^3 + x Z^3$$
$$+ 2 Y^5 - Y^6 + Z^3 + 2 x Y^3 Z - 2 x Y^2 Z - x Y^9 Z^2 - 2 x Y^9 Z$$
$$+ 2 x Y^8 Z - x Y^7 Z^2 - 2 x Y^7 Z + x Y^6 Z^2$$
$$+ 2 x Y^6 Z - x Y^5 Z^2 - 2 x Y^5 Z - x Y^4 Z^2$$
$$+ x Y^3 Z^2 - x Y^2 Z^2 - x Y Z^2 - 2 x Y^4 Z + x Y^8 Z^2 + x Y Z^3 + Y^6 Z^3 - Y^5 Z^4$$
$$+ Y^5 Z^3 - Y Z^4 - Z^4 - Y^6 Z^4$$

```
> collect(aa,[Y,Z],`distributed`): aa:=sort(%,[Y,Z],tdeg);
```

$$aa := -x Y^9 Z^2 - 2 x Y^9 Z + x Y^8 Z^2 - Y^6 Z^4 - x Y^9 + 2 x Y^8 Z - x Y^7 Z^2 \tag{6.11.4}$$
$$+ Y^6 Z^3 - Y^5 Z^4 + x Y^8 - 2 x Y^7 Z + (x - 1) Y^6 Z^2 + Y^5 Z^3 - x Y^7 + (2 x$$
$$+ 1) Y^6 Z + (-1 - x) Y^5 Z^2 + (x - 1) Y^6 + (-2 x - 1) Y^5 Z - x Y^4 Z^2$$
$$+ (-x + 2) Y^5 + (x^2 - 2 x) Y^4 Z + x Y^3 Z^2 - Y Z^4 + (x^2 - x) Y^4$$
$$+ (2 x - x^2) Y^3 Z - x Y^2 Z^2 + (x + 1) Y Z^3 - Z^4 + (-x^2 + x) Y^3$$
$$+ (x^2 - 2 x) Y^2 Z + (-1 - x) Y Z^2 + (x + 1) Z^3 + (x^2 - x) Y^2$$
$$+ (1 - x^2) Y Z + (-1 + 2 x) Z^2 + (-x^2 + 2 x - 1) Y + (x^2 - 1 + x) Z$$
$$+ 2 x + x^2 + 2$$

```
> aa:=subs(Y=y-1,Z=z-1,aa) mod p^l;
  u[7]:=(x-2)+(-x+1)*(y-1)+(x-2)*(z-1)+x*(y-1)^2+(-x-2)*(y-1)*
  (z-1)+(-2)*(z-1)^2+(-x)*(y-1)^3+x*(y-1)^2*(z-1)+(-2)*(y-1)*(z
  -1)^2+(z-1)^3+x*(y-1)^4+(-x)*(y-1)^3*(z-1)+(y-1)*(z-1)^3+x*(y
  -1)^4*(z-1) mod p^l;
```

```
w[7]:=(x-1)+(-1)*(z-1)+(-1)*(y-1)^5+(-1)*(y-1)^5*(z-1) mod
p^l;
```

$$aa := 2 + 2x + x^2 + 2x(y-1)^8(z-1) + x(y-1)^8(z-1)^2 + (x + 1)(y-1)(z-1)^3 - x(y-1)^9 + x(y-1)^8 - x(y-1)^7 + (x-1)(y-1)^6 + (-x+2)(y-1)^5 + (x^2-x)(y-1)^4 + (-x^2 + x)(y-1)^3 + (x^2-x)(y-1)^2 + (-x^2+2x-1)(y-1) + (x^2-1 + x)(z-1) + (-1+2x)(z-1)^2 - (y-1)^6(z-1)^4 + (y-1)^6(z-1)^3 - (y-1)^5(z-1)^4 + (y-1)^5(z-1)^3 - (y-1)(z-1)^4 + (x+1)(z-1)^3 - (z-1)^4 + (1-x^2)(y-1)(z-1) + (x-1)(y-1)^6(z-1)^2 + (2x-x^2)(y-1)^3(z-1) - x(y-1)^9(z-1)^2 - 2x(y-1)^9(z-1) - x(y-1)^7(z-1)^2 - 2x(y-1)^7(z-1) + (2x+1)(y-1)^6(z-1) + (-1-x)(y-1)^5(z-1)^2 + (-2x-1)(y-1)^5(z-1) - x(y-1)^4(z-1)^2 + (x^2-2x)(y-1)^4(z-1) + x(y-1)^3(z-1)^2 - x(y-1)^2(z-1)^2 + (x^2-2x)(y-1)^2(z-1) + (-1-x)(y-1)(z-1)^2$$

$$u_7 := x - 2 + (-x+1)(y-1) + (x-2)(z-1) + x(y-1)^2 + (-x-2)(y-1)(z-1) - 2(z-1)^2 - x(y-1)^3 + x(y-1)^2(z-1) - 2(y-1)(z-1)^2 + (z-1)^3 + x(y-1)^4 - x(y-1)^3(z-1) + (y-1)(z-1)^3 + x(y-1)^4(z-1)$$

$$w_7 := x - z - (y-1)^5 - (y-1)^5(z-1) \tag{6.11.5}$$

```
> expand(u[7]) mod  p^l; expand(w[7]) mod p^l; expand(aa-u[7]*w
[7]) mod p^l;
```

$$2 + xy^4z + yz^3$$

$$x - y^5z$$

$$0 \tag{6.11.6}$$

A 6.2. Algoritmus.

```
> MultivariateDiophant:=proc(a,c,E,d,p,k)
    local sigma,r,nu,i,A,aa,b,cc,EE,e,monom,m,x,y,ee,cm,ds,
  alpha;
    r:=nops(a); nu:=nops(E);
    if nu>1 then
      x:=op(1,E[nu]); alpha:=op(2,E[nu]);
```

```
      A:=mul(a[i],i=1..r);
      for i to r do b[i]:=A/a[i] od;
      aa:=subs(E[nu],a);
      cc:=subs(E[nu],c);
      EE:=E[1..nu-1];
      sigma:=MultivariateDiophant(aa,cc,EE,d,p,k);
      e:=mods(expand(c-add(sigma[i]*b[i],i=1..r)),p^k);
      monom:=1;
      for m to d while e<>0 do
        monom:=monom*(x-alpha);
        ee:=diff(e,[x$m]);
        cm:=subs(x=alpha,ee)/m!;
        if cm<>0 then
          ds:=MultivariateDiophant(aa,cm,EE,d,p,k);
          for i to r do sigma[i]:=expand(sigma[i]+ds[i]*monom)
od;
          e:=mods(expand(e-add(ds[i]*monom*b[i],i=1..r)),p^k);
        fi;
      od;
    else
      x:=E[1];
      sigma:=[0$i=1..r];
      for m from 0 to d do
        cm:=coeff(c,x,m);
        if cm<>0 then
          ds:=UnivariateDiophant(a,x,m,p,k);
          for i to r do sigma[i]:=expand(sigma[i]+ds[i]*cm) od;
        fi;
      od;
    fi;
    map((x,y)->mods(x,y),sigma,p^k);
  end;
```

$$MultivariateDiophant := \mathbf{proc}(a, c, E, d, p, k) \tag{6.12.1}$$

local sigma, r, nu, i, A, aa, b, cc, EE, e, $monom$, m, x, y, ee, cm, ds, alpha;

$r := nops(a)$;

nu $:= nops(E)$;

if $1 <$ nu **then**

$x := op(1, E[\text{nu}])$;

alpha $:= op(2, E[\text{nu}])$;

$A := mul(a[i], i = 1..r)$;

for i **to** r **do**

$b[i] := A / a[i]$

end do;

```
        aa := subs(E[nu], a);
        cc := subs(E[nu], c);
        EE := E[1 ..nu - 1];
        sigma := MultivariateDiophant(aa, cc, EE, d, p, k);
        e := mods(expand(c - add(sigma[i] * b[i], i = 1 ..r)), p^k);
        monom := 1;
        for m to d while e <> 0 do
            monom := monom * (x - alpha);
            ee := diff(e, [ `$`(x, m)]);
            cm := subs(x = alpha, ee) / factorial(m);
            if cm <> 0 then
                ds := MultivariateDiophant(aa, cm, EE, d, p, k);
                for i to r do
                    sigma[i] := expand(sigma[i] + ds[i] * monom)
                end do;
                e := mods(expand(e - add(ds[i] * monom * b[i], i = 1 ..r)),
                p^k)
            end if
        end do
    else
        x := E[1];
        sigma := [ `$`(0,
        i = 1 ..r)];
        for m from 0 to d do
            cm := coeff(c, x, m);
            if cm <> 0 then
                ds := UnivariateDiophant(a, x, m, p, k);
                for i to r do
                    sigma[i] := expand(sigma[i] + ds[i] * cm)
                end do
            end if
        end do
    end if;
    map(proc(x, y)
        option operator, arrow;
        mods(x, y)
    end proc, sigma, p^k)
end proc
```

A 6.3. Algoritmus.

```
> UnivariateDiophant:=proc(a,x,m,p,k)
    local i,sigma,r,s,R,q;
    r:=nops(a);
    if r>2 then
      s:=MultiTermEEAlift(a,x,p,k); R:=[];
      for i to r do R:=[op(R),mods(rem(x^m*s[i],a[i],x),p^k)]
  od;
    else
      s:=EEAlift(a[2],a[1],x,p,k);
      q:=mods(quo(x^m*s[1],a[1],x),p^k);
      R:=[mods(expand(x^m*s[1]-q*a[1]),p^k),
        mods(expand(x^m*s[2]+q*a[2]),p^k)];
    fi; R;
  end;
```

$$UnivariateDiophant := \mathbf{proc}(a, x, m, p, k) \tag{6.13.1}$$

$\mathbf{local}\ i, \mathrm{sigma}, r, s, R, q;$
$r := nops(a);$
$\mathbf{if}\ 2 < r\ \mathbf{then}$
$s := MultiTermEEAlift(a, x, p, k);$
$R := [\,];$
$\mathbf{for}\ i\ \mathbf{to}\ r\ \mathbf{do}$
$R := [op(R), mods(rem(x\hat{}m * s[i], a[i], x), p\hat{}k)]$
$\mathbf{end\ do}$
$\mathbf{else}$
$s := EEAlift(a[2], a[1], x, p, k);$
$q := mods(quo(x\hat{}m * s[1], a[1], x), p\hat{}k);$
$R := [mods(expand(x\hat{}m * s[1] - q * a[1]), p\hat{}k),$
$mods(expand(x\hat{}m * s[2] + q * a[2]), p\hat{}k)]$
$\mathbf{end\ if};$
R
$\mathbf{end\ proc}$

```
> MultiTermEEAlift:=proc(a,x,p,k) local i,r,s,beta,sigma;
    r:=nops(a); s:=[0$i=1..r];
    s[r-1]:=a[r];
    for i from r-2 by -1 to 1 do s[i]:=expand(a[i+1]*s[i+1])
  od;
    beta:=1;
    for i to r-1 do
      sigma:=MultivariateDiophant([s[i],a[i]],beta,[x],0,p,k);
      beta:=sigma[1]; s[i]:=sigma[2];
    od; s[r]:=beta;
```

```
    s;
  end;
```

```
MultiTermEEAlift := proc(a, x, p, k)                                    (6.13.2)
    local i, r, s, beta, sigma;
    r := nops(a);
    s := [ `$`(0, i = 1 ..r) ];
    s[r - 1] := a[r];
    for i from r - 2 by -1 to 1 do
        s[i] := expand(a[i + 1] * s[i + 1])
    end do;
    beta := 1;
    for i to r - 1 do
        sigma := MultivariateDiophant([s[i], a[i]], beta, [x], 0, p, k);
        beta := sigma[1];
        s[i] := sigma[2]
    end do;
    s[r] := beta;
    s
end proc
```

```
> EEAlift:=proc(a,b,x,p,k) local ap,bp,s,t,sp,tp,i,m,e,c,q,
  sigma,tau;
    ap:=mods(a,p); bp:=mods(b,p);
    mods(Gcdex(ap,bp,x,'s','t'),p);
    sp:=mods(s,p); tp:=mods(t,p); m:=p;
    for i to k-1 do
      e:=expand(1-s*a-t*b); c:=mods(e/m,p);
      sigma:=mods(expand(sp*c),p); tau:=mods(expand(tp*c),p);
      q:=mods(Quo(sigma,bp,x),p);
      sigma:=mods(expand(sigma-q*bp),p);
      tau:=mods(expand(tau+q*ap),p);
      s:=expand(s+sigma*m); t:=expand(t+tau*m);
      m:=m*p;
    od; [s,t];
  end;
```

```
EEAlift := proc(a, b, x, p, k)                                          (6.13.3)
    local ap, bp, s, t, sp, tp, i, m, e, c, q, sigma,
    tau;
    ap := mods(a, p);
    bp := mods(b, p);
    mods(Gcdex(ap, bp, x, 's',
    't'), p);
```

```
    sp := mods(s, p);
    tp := mods(t, p);
    m := p;
    for i to k - 1 do
        e := expand(1 - s*a - t*b);
        c := mods(e / m, p);
        sigma := mods(expand(sp*c), p);
        tau := mods(expand(tp*c),
       p);
        q := mods(Quo(sigma, bp, x), p);
        sigma := mods(expand(sigma - q*bp), p);
        tau := mods(expand(tau + q*ap), p);
        s := expand(s + sigma*m);
        t := expand(t + tau*m);
        m := m*p
    end do;
    [s, t]
end proc
```

A 6.4. Algoritmus.

```
> MultivariateHensel:=proc(a,E,p,l,u,lcU)
    local nu,A,i,x,alpha,U,UU,n,monom,maxdeg,aa,e,ee,co,oco,t,
  xx,m,j,c,dU;
    aa:=expand(a);
    nu:=nops(E); A:=[0$i=1..nu]; n:=nops(u);
    A[nu]:=aa; maxdeg:=-1;
    for i from nu by -1 to 2 do
      x:=op(1,E[i]); alpha:=op(2,E[i]);
      A[i-1]:=subs(E[i],A[i]);
      if degree(a,x)>maxdeg then maxdeg:=degree(a,x) fi;
    od;
    U:=u; xx:=E[1];
    for i from 2 to nu do
      UU:=U; monom:=1;
      x:=op(1,E[i]); alpha:=op(2,E[i]);
      for m to n do
        if lcU[m]<>1 then
          co:=mods(subs(E[i+1..nu],lcU[m]),p^l);
          oco:=lcoeff(collect(U[m],xx),xx,'t');
          U[m]:=expand(U[m]-oco*t+co*t);
        fi;
```

```
      od;
      e:=expand(A[i]-mul(U[j],j=1..n));
      for j to degree(A[i],x) while e<>0 do
        monom:=monom*(x-alpha);
        c:=subs(E[i],diff(e,[x$j]))/j!;
        if c<>0 then
          dU:=MultivariateDiophant(UU,c,E[1..i-1],maxdeg,p,l);
          for m to n do U[m]:=mods(expand(U[m]+dU[m]*monom),
  p^l) od;
          e:=mods(expand(A[i]-mul(U[m],m=1..n)),p^l);
        fi;
      od;
    od;
    if a=expand(mul(U[m],m=1..n)) then U else FAIL fi;
  end;
```

$$MultivariateHensel := \mathbf{proc}(a, E, p, l, u, lcU) \tag{6.14.1}$$

local nu, A, i, x, alpha, U,
UU, n, $monom$, $maxdeg$, aa, e, ee, co, oco, t, xx, m, j, c, dU;
$aa := expand(a)$;
nu $:= nops(E)$;
$A := [\ `\$`(0, i = 1..\text{nu})\ ]$;
$n := nops(u)$;
$A[\text{nu}] := aa$;
$maxdeg := -1$;
for i **from** nu **by** -1 **to** 2 **do**
  $x := op(1, E[i])$;
  alpha $:= op(2, E[i])$;
  $A[i-1] := subs(E[i], A[i])$;
  if $maxdeg < degree(a, x)$ **then**
    $maxdeg := degree(a, x)$
  end if
end do;
$U := u$;
$xx := E[1]$;
for i **from** 2 **to** nu **do**
  $UU := U$;
  $monom := 1$;
  $x := op(1, E[i])$;
  alpha $:= op(2, E[i])$;
  for m **to** n **do**
    if $lcU[m] <> 1$ **then**
```
```

```
            co := mods(subs(E[i+1..nu], lcU[m]), p^l);
            oco := lcoeff(collect(U[m], xx), xx, 't');
            U[m] := expand(U[m] - oco*t + co*t)
        end if
    end do;
    e := expand(A[i] - mul(U[j], j = 1..n));
    for j to degree(A[i],
    x) while e <> 0 do
        monom := monom*(x - alpha);
        c := subs(E[i], diff(e, [`$`(x, j)])) / factorial(j);
        if c <> 0 then
            dU := MultivariateDiophant(UU, c, E[1..i-1],
            maxdeg, p, l);
            for m to n do
                U[m] := mods(expand(U[m] + dU[m]*monom), p^l)
            end do;
            e := mods(expand(A[i] - mul(U[m],
            m = 1..n)), p^l)
        end if
    end do
end do;
if a = expand(mul(U[m], m = 1..n)) then
    U
else
    FAIL
end if
end proc
```

```
> a; factor(a); collect(a,x); coeffs(%,x); gcd(%[1],%[2]);
```

$$x^2 y^4 z - x y^9 z^2 + x y z^3 + 2x - y^6 z^4 - 2 y^5 z$$

$$(x - y^5 z)(y^4 z x + y z^3 + 2)$$

$$x^2 y^4 z + (y z^3 + 2 - y^9 z^2) x - y^6 z^4 - 2 y^5 z$$

$$-y^6 z^4 - 2 y^5 z,\ y z^3 + 2 - y^9 z^2,\ y^4 z$$

$$1 \qquad (6.14.2)$$

```
> E:=[x,z=1,y=1]; subs(E[2..3],a);
```

$$E := [x,\ z = 1,\ y = 1]$$

$$x^2 + 2x - 3 \qquad (6.14.3)$$

```
> debug(MultivariateHensel);
```

$$(6.14.4)$$

```
> MultivariateHensel(a,E,5,2,[x-1,x+3],[1,y^4*z]);
{--> enter MultivariateHensel, args = x^2*y^4*z-x*y^9*z^2+
x*y*z^3+2*x-y^6*z^4-2*y^5*z, [x, z = 1, y = 1], 5, 2, [x
-1, x+3], [1, y^4*z]
```

$$aa := x^2 y^4 z - x y^9 z^2 + x y z^3 + 2 x - y^6 z^4 - 2 y^5 z$$

$$\nu := 3$$

$$A := [0, 0, 0]$$

$$n := 2$$

$$A_3 := x^2 y^4 z - x y^9 z^2 + x y z^3 + 2 x - y^6 z^4 - 2 y^5 z$$

$$maxdeg := -1$$

$$x := y$$

$$\alpha := 1$$

$$A_2 := x^2 z - x z^2 + x z^3 + 2 x - z^4 - 2 z$$

$$maxdeg := 9$$

$$x := z$$

$$\alpha := 1$$

$$A_1 := x^2 + 2 x - 3$$

$$U := [x - 1, x + 3]$$

$$xx := x$$

$$UU := [x - 1, x + 3]$$

$$monom := 1$$

$$x := z$$

$$\alpha := 1$$

$$co := z$$

$$oco := 1$$

$$U_2 := 3 + z x$$

$$e := -x z^2 + x z^3 - x - z^4 - 2 z + 3 + z x$$

$$monom := z - 1$$

$$c := 2 x - 6$$

$$dU := [-1, 3]$$

$$U_1 := x - z$$

$$U_2 := z x + 3 z$$

$$e := x z^3 + 2 x - z^4 - 2 z - 3 z x + 3 z^2$$

$$monom := (z - 1)^2$$

$$c := 3 x - 3$$

$$dU := [0, 3]$$

$$U_1 := x - z$$

$$U_2 := z\,x - 3\,z + 3\,z^2 + 3$$

$$e := -3\,x\,z^2 + x\,z^3 - x - z^4 + z + 3\,z\,x - 3\,z^2 + 3\,z^3$$

$$monom := (z-1)^3$$

$$c := x - 1$$

$$dU := [0,\ 1]$$

$$U_1 := x - z$$

$$U_2 := z\,x + 2 + z^3$$

$$e := 0$$

$$UU := [x - z,\ z\,x + 2 + z^3]$$

$$monom := 1$$

$$x := y$$

$$\alpha := 1$$

$$co := y^4\,z$$

$$oco := z$$

$$U_2 := 2 + z^3 + y^4\,z\,x$$

$$e := -x\,y^9\,z^2 + x\,y\,z^3 - y^6\,z^4 - 2\,y^5\,z - x\,z^3 + 2\,z + z^4 + y^4\,z^2\,x$$

$$monom := y - 1$$

$$c := -5\,x\,z^2 + x\,z^3 - 6\,z^4 - 10\,z$$

$$dU := [-5\,z,\ z^3]$$

$$U_1 := x + 4\,z - 5\,y\,z$$

$$U_2 := y^4\,z\,x + y\,z^3 + 2$$

$$e := -x\,y^9\,z^2 - y^6\,z^4 - 2\,y^5\,z - 4\,y^4\,z^2\,x - 4\,y\,z^4 - 8\,z + 5\,y^5\,z^2\,x + 5\,y^2\,z^4 + 10\,y\,z$$

$$monom := (y-1)^2$$

$$c := -10\,x\,z^2 - 10\,z^4 - 20\,z$$

$$dU := [-10\,z,\ 0]$$

$$U_1 := x - 6\,z - 10\,y\,z - 10\,z\,y^2$$

$$U_2 := y^4\,z\,x + y\,z^3 + 2$$

$$e := -x\,y^9\,z^2 - y^6\,z^4 - 2\,y^5\,z + 6\,y^4\,z^2\,x + 6\,y\,z^4 + 12\,z + 10\,y^5\,z^2\,x + 10\,y^2\,z^4 - 5\,y\,z + 10\,z^2\,y^6\,x + 10\,z^4\,y^3 - 5\,z\,y^2$$

$$monom := (y-1)^3$$

$$c := 240\,x\,z^2 - 10\,z^4 - 20\,z$$

$$dU := [-10\,z,\ 0]$$

$$U_1 := x + 4\,z + 10\,y\,z - 5\,z\,y^2 - 10\,y^3\,z$$

$$U_2 := y^4\,z\,x + y\,z^3 + 2$$

$$e := -x\,y^9\,z^2 - y^6\,z^4 - 2\,y^5\,z - 4\,y^4\,z^2\,x - 4\,y\,z^4 - 8\,z - 10\,y^5\,z^2\,x - 10\,y^2\,z^4 + 5\,y\,z + 5\,z^2\,y^6\,x + 5\,z^4\,y^3 + 10\,z\,y^2 + 10\,x\,y^7\,z^2 + 10\,y^4\,z^4 - 5\,y^3\,z$$

$$monom := (y-1)^4$$

$$c := 245\,x\,z^2 - 5\,z^4 - 10\,z$$

$$dU := [-5\,z,\ 0]$$

$$U_1 := x - z + 5\,y\,z - 10\,z\,y^2 + 10\,y^3\,z - 5\,y^4\,z$$

$$U_2 := y^4\,z\,x + y\,z^3 + 2$$

$$e := -x\,y^9\,z^2 - y^6\,z^4 - 2\,y^5\,z + y^4\,z^2\,x + y\,z^4 + 2\,z - 5\,y^5\,z^2\,x - 5\,y^2\,z^4 - 10\,y\,z + 10\,z^2\,y^6\,x + 10\,z^4\,y^3 - 5\,z\,y^2 - 10\,x\,y^7\,z^2 - 10\,y^4\,z^4 + 5\,y^3\,z + 5\,x\,y^8\,z^2 + 5\,y^5\,z^4 + 10\,y^4\,z$$

$$monom := (y-1)^5$$

$$c := -x\,z^2 - z^4 - 2\,z$$

$$dU := [-z,\ 0]$$

$$U_1 := x - y^5\,z$$

$$U_2 := y^4\,z\,x + y\,z^3 + 2$$

$$e := 0$$

$$[x - y^5\,z,\ y^4\,z\,x + y\,z^3 + 2]$$

```
<-- exit MultivariateHensel (now at top level) = [x-y^5*z,
y^4*z*x+y*z^3+2]}
```

$$[x - y^5\,z,\ y^4\,z\,x + y\,z^3 + 2] \qquad (6.14.5)$$

▶ 7. Legnagyobb közös osztó

▶ 8. Faktorizálás

▶ 9. Egyenletrendszerek

▶ 10. Gröbner-bázisok

▶ 11. Racionális törtfüggvények integrálása

▶ 12. A Risch-algoritmus.