Komputeralgebrai algoritmusok

Járai Antal

Ezek a programok csak szemléltetésre szolgálnak.

1. Történet

2. Algebrai alapok

3. Normál formák, reprezentáció

4. Aritmetika

5. Kínai maradékolás

```
> restart;
```

E 5.1. Példa.

E 5.2. Példa.

```
> a:=-30*x^3*y+90*x^2*y^2+15*x^2-60*x*y+45*y^2;
```

$$a := -30\,x^3\,y + 90\,x^2\,y^2 + 15\,x^2 - 60\,x\,y + 45\,y^2 \quad (5.2.1)$$

```
> collect(a,[x,y],`distributed`);
```

$$-30\,x^3\,y + 90\,x^2\,y^2 + 15\,x^2 - 60\,x\,y + 45\,y^2 \quad (5.2.2)$$

```
> collect(a,x);
```

$$-30\,x^3\,y + \left(90\,y^2 + 15\right)x^2 - 60\,x\,y + 45\,y^2 \quad (5.2.3)$$

```
> collect(a,y);
```

$$\left(90\,x^2 + 45\right)y^2 + \left(-30\,x^3 - 60\,x\right)y + 15\,x^2 \quad (5.2.4)$$

E 5.3. Példa.

```
> 3/1;
```

$$3 \quad (5.3.1)$$

E 5.4. Példa.

```
> [i$i=-8..8]; map(x->x mod 6,%);
```

$$[-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8]$$

$$[4, 5, 0, 1, 2, 3, 4, 5, 0, 1, 2, 3, 4, 5, 0, 1, 2] \quad (5.4.1)$$

E 5.5. Példa.

```
> subs(x=5,a); subs(y=2,a);
```

$$-4050\, y + 2295\, y^2 + 375$$

$$-60\, x^3 + 375\, x^2 - 120\, x + 180 \quad (5.5.1)$$

E 5.6. Példa.

```
> a:=3*x^2*y^2-x^2*y+5*x^2+x*y^2-3*x*y; b:=2*x*y+7*x+y^2-2;
```

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

$$b := 2\, x\, y + 7\, x + y^2 - 2 \quad (5.6.1)$$

```
> a mod 5; b mod 5;
```

$$3\, x^2\, y^2 + 4\, x^2\, y + x\, y^2 + 2\, x\, y$$

$$2\, x\, y + 2\, x + y^2 + 3 \quad (5.6.2)$$

```
> a mod 7; b mod 7;
```

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

$$2\, x\, y + y^2 + 5 \quad (5.6.3)$$

E 5.7. Példa.

```
> a:=7*x+5; b:=2*x-3; c:=expand(a*b);
```

$$a := 7\, x + 5$$

$$b := 2\, x - 3$$

$$c := 14\, x^2 - 11\, x - 15 \quad (5.7.1)$$

```
> subs(x=0,a) mod 5; subs(x=0,b) mod 5; subs(x=0,c) mod 5;
```

$$0$$

$$2$$

$$0 \quad (5.7.2)$$

```
> subs(x=1,a) mod 5; subs(x=1,b) mod 5; subs(x=1,c) mod 5;
```

$$2$$

$$4$$
$$3 \quad (5.7.3)$$

```
> subs(x=2,a) mod 5; subs(x=2,b) mod 5; subs(x=2,c) mod 5;
```

$$4$$
$$1$$
$$4 \quad (5.7.4)$$

```
> subs(x=0,a) mod 7; subs(x=0,b) mod 7; subs(x=0,c) mod 7;
```

$$5$$
$$4$$
$$6 \quad (5.7.5)$$

```
> subs(x=1,a) mod 7; subs(x=1,b) mod 7; subs(x=1,c) mod 7;
```

$$5$$
$$6$$
$$2 \quad (5.7.6)$$

```
> subs(x=2,a) mod 7; subs(x=2,b) mod 7; subs(x=2,c) mod 7;
```

$$5$$
$$1$$
$$5 \quad (5.7.7)$$

```
> c mod 7; c mod 5;
```

$$3\,x+6$$
$$4\,x^2+4\,x \quad (5.8.8)$$

E 5.8. Példa.

```
> m*i$i=-infinity..infinity;
```

$$m\,i\$\left(i=-\infty..\infty\right) \quad (5.8.1)$$

E 5.9. Példa.

```
> p:=5*x+2; p*d;
```

$$p := 5\,x+2$$
$$\left(5\,x+2\right)\,d \quad (5.9.1)$$

E 5.10. Példa.

```
> p1:=x; p2:=y;
```

$$p1 := x$$
(5.10.1)

$$p2 := y \quad (5.10.1)$$

```
> p1*a1+p2*a2;
```

$$x\, a1 + y\, a2 \quad (5.10.2)$$

E 5.11. Példa.

```
> [i$i=-8..8]; map(x->x mod 6,%);
```

$$[-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8]$$

$$[4, 5, 0, 1, 2, 3, 4, 5, 0, 1, 2, 3, 4, 5, 0, 1, 2] \quad (5.11.1)$$

E 5.12. Példa.

```
> p:=x^2+1;
```

$$p := x^2 + 1 \quad (5.12.1)$$

```
> a:=x^2+8*x+4; rem(a,p,x); b:=2*x^2+8*x+5; rem(b,p,x);
```

$$a := x^2 + 8\, x + 4$$

$$3 + 8\, x$$

$$b := 2\, x^2 + 8\, x + 5$$

$$3 + 8\, x \quad (5.12.2)$$

```
> p:=x-2; rem(a,p,x); subs(x=2,a); rem(b,p,x); subs(x=2,b);
```

$$p := x - 2$$

$$24$$

$$24$$

$$29$$

$$29 \quad (5.12.3)$$

E 5.13. Példa.

```
> a:=-30*x^3*y+90*x^2*y^2+15*x^2-60*x*y+45*y^2; a mod 7; subs
(y=3,a);
```

$$a := -30\, x^3\, y + 90\, x^2\, y^2 + 15\, x^2 - 60\, x\, y + 45\, y^2$$

$$5\, x^3\, y + 6\, x^2\, y^2 + x^2 + 3\, x\, y + 3\, y^2$$

$$-90\, x^3 + 825\, x^2 - 180\, x + 405 \quad (5.13.1)$$

E 5.14. Példa.

```
> m0:=3; m1:=5; m:=m0*m1; 11=2+3*3; -4=-1+(-1)*3;
```

$$m0 := 3$$

$$m1 := 5$$

$$m := 15$$

$$11 = 11$$

$$-4 = -4 \qquad (5.14.1)$$

A 5.1. Algoritmus.

```
> IntegerCRA:=proc(M,U) local G,N,n,i,j,t;
    n:=nops(M)-1;
    G:=[0$i=1..n];
    N:=[0$i=0..n];
    for j to n do
      t:=M[1] mod M[j+1];
      for i to j-1 do
        t:=t*M[i+1] mod M[j+1];
      od;
      G[j]:=1/t mod M[j+1];
    od;
    N[1]:=U[1];
    for j to n do
      t:=N[j];
      for i from j-2 to 0 by -1 do
        t:=t*M[i+1]+N[i+1] mod M[j+1];
      od;
      N[j+1]:=(U[j+1]-t)*G[j] mod M[j+1];
    od;
    t:=N[n+1];
    for j from n-1 to 0 by -1 do
      t:=t*M[j+1]+N[j+1];
    od; t;
  end;
```

IntegerCRA := **proc**(*M*, *U*) (5.15.1)

local *G*, *N*, *n*, *i*, *j*, *t*;

$n := nops(M) - 1;$

$G := [\ `\$`(0, i = 1..n)];$

$N := [\ `\$`(0, i = 0..n)];$

for *j* **to** *n* **do**

$t := mod(M[1], M[j+1]);$

for *i* **to** $j - 1$ **do**

$t := mod(t * M[i+1],$

$M[j+1])$

end do;

$G[j] := mod(1 / t, M[j+1])$

end do;

$N[1] := U[1]$;

for j **to** n **do**

$t := N[j]$;

for i **from** $j-2$ **by** -1 **to** 0 **do**

$t := mod(t^* M[i+1] + N[i+1], M[j+1])$

end do;

$N[j+1] := mod((U[j+1] - t) * G[j], M[j+1])$

end do;

$t := N[n+1]$;

for j **from** $n-1$ **by** -1 **to** 0 **do**

$t := t^* M[j+1] + N[j+1]$

end do;

t

end proc

E 5.15. Példa.

```
> `mod`:=mods; debug(IntegerCRA); IntegerCRA([99,97,95],[49,
  -21,-30]);
```

$$mod := mods$$

$$IntegerCRA$$

```
{--> enter IntegerCRA, args = [99, 97, 95], [49, -21, -30]
```

$$n := 2$$

$$G := [0, 0]$$

$$N := [0, 0, 0]$$

$$t := 2$$

$$G_1 := -48$$

$$t := 4$$

$$t := 8$$

$$G_2 := 12$$

$$N_1 := 49$$

$$t := 49$$

$$N_2 := -35$$

$$t := -35$$
$$t := 4$$
$$N_3 := -28$$
$$t := -28$$
$$t := -2751$$
$$t := -272300$$
$$-272300$$

```
<-- exit IntegerCRA (now at top level) = 272300}
```

$$-272300 \tag{5.16.1}$$

A 5.2. Algoritmus.

```
> NewtonInterp:=proc(a,u,x,p) local i,j,t,n,G,N;
    n:=nops(a)-1;
    G:=[0$i=1..n];
    N:=[0$i=0..n];
    for j to n do
      t:=a[j+1]-a[1] mod p;
      for i to j-1 do
        t:=t*(a[j+1]-a[i+1]) mod p;
      od;
      G[j]:=1/t mod p;
    od;
    N[1]:=u[1];
    for j to n do
      t:=N[j];
      for i from j-2 to 0 by -1 do
        t:=t*(a[j+1]-a[i+1])+N[i+1] mod p;
      od;
      N[j+1]:=(u[j+1]-t)*G[j] mod p;
    od;
    t:=N[n+1];
    for j from n-1 to 0 by -1 do
      t:=t*(x-a[j+1])+N[j+1] mod p;
    od; t;
  end;
```

NewtonInterp := **proc**(*a*, *u*, *x*, *p*) (5.17.1)

local *i*, *j*, *t*, *n*, *G*, *N*;

$n := nops(a) - 1;$

$G := [\ `\$`(0, i = 1 .. n)];$

$N := [\ `\$`(0, i = 0 .. n)];$

for *j* **to** *n* **do**

```
            t := mod(a[j+1] - a[1], p);
            for i to j - 1 do
                t := mod(t*(a[j+1] - a[i+1]), p)
            end do;
            G[j] := mod(1 / t, p)
        end do;
        N[1] := u[1];
        for j to n do
            t := N[j];
            for i from j - 2 by -1 to 0 do
                t := mod(t*(a[j+1] - a[i+1]) + N[i+1], p)
            end do;
            N[j+1] := mod((u[j+1] - t)*G[j], p)
        end do;
        t := N[n+1];
        for j from n - 1 by -1 to 0 do
            t := mod(t*(x - a[j+1]) + N[j+1],
            p)
        end do;
        t
    end proc
```

E 5.16. Példa.

```
> u0:=NewtonInterp([0,1],[-21,-30],y,97);
```

$$u0 := -9\,y - 21 \quad (5.18.1)$$

```
> u1:=NewtonInterp([0,1],[20,17],y,97);
```

$$u1 := -3\,y + 20 \quad (5.18.2)$$

```
> u2:=NewtonInterp([0,1],[-36,-31],y,97);
```

$$u2 := 5\,y - 36 \quad (5.18.3)$$

```
> u:=NewtonInterp([0,1,2],[u0,u1,u2],x,97); expand(u);
```

$$u := \left(y\left(x-1\right) + 6\,y + 41\right)x - 9\,y - 21$$

$$x^2\,y + 5\,x\,y + 41\,x - 9\,y - 21 \quad (5.18.4)$$

E 5.17. Példa.

```
> a:=7*x+5; b:=2*x-3; c:=expand(a*b);
```

$$a := 7\,x + 5$$
$$b := 2\,x - 3$$
$$c := 14\,x^2 - 11\,x - 15 \tag{5.19.1}$$

```
> c5:=expand(NewtonInterp([0,1,2],[0,-2,-1],x,5)) mod 5;
```

$$c5 := -x^2 - x \tag{5.19.2}$$

```
> c7:=expand(NewtonInterp([0,1,2],[-1,2,-2],x,7)) mod 7;
```

$$c7 := 3\,x - 1 \tag{5.19.3}$$

```
> c3:=expand(NewtonInterp([0,1,-1],[0,0,1],x,3)) mod 3;
```

$$c3 := -x^2 + x \tag{5.19.4}$$

```
> expand(IntegerCRA([5,7,3],[-x^2-x,3*x-1,-x^2+x])) mod 105;
{--> enter IntegerCRA, args = [5, 7, 3], [-x^2-x, 3*x-1, -
x^2+x]
```

$$n := 2$$
$$G := [0, 0]$$
$$N := [0, 0, 0]$$
$$t := -2$$
$$G_1 := 3$$
$$t := -1$$
$$t := -1$$
$$G_2 := -1$$
$$N_1 := -x^2 - x$$
$$t := -x^2 - x$$
$$N_2 := -2\,x - 3 + 3\,x^2$$
$$t := -2\,x - 3 + 3\,x^2$$
$$t := -x^2 + x$$
$$N_3 := 0$$
$$t := 0$$
$$t := -2\,x - 3 + 3\,x^2$$
$$t := 14\,x^2 - 11\,x - 15$$
$$14\,x^2 - 11\,x - 15$$

```
<-- exit IntegerCRA (now at top level) = 14*x^2-11*x-15}
```

$$14\,x^2 - 11\,x - 15 \tag{5.19.5}$$

▶ 6. Newton-iteráció, Hensel-felemelés

- **7. Legnagyobb közös osztó**
- **8. Faktorizálás**
- **9. Egyenletrendszerek**
- **10. Gröbner–bázisok**
- **11. Racionális törtfüggvények integrálása**
- **12. A Risch–algoritmus.**