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

▶ 7. Legnagyobb közös osztó

▼ 8. Faktorizálás

```
> restart;
```

▼ A 8.1. Algoritmus.

```
> SquareFree:=proc(a,x) local i,out,b,c,y,z,w;
  i:=1; out:=1; b:=diff(a,x);
  c:=gcd(a,b); w:=quo(a,c,x);
  while c<>1 do
    y:=gcd(w,c);
    z:=quo(w,y,x);
    out:=out*z^i;
    i:=i+1;
    w:=y; c:=quo(c,y,x);
  od; out:=out*w^i; end;
```

$$SquareFree := \mathbf{proc}(a, x) \tag{8.1.1}$$

$\mathbf{local}\ i, out, b, c, y, z, w;$

$i := 1;$

```
    out := 1;
    b := diff(a, x);
    c := gcd(a, b);
    w := quo(a, c, x);
    while c <> 1 do
        y := gcd(w, c);
        z := quo(w, y, x);
        out := out * z^i;
        i := i + 1;
        w := y;
        c := quo(c, y, x)
    end do;
    out := out * w^i
end proc
```

E 8.1. Példa.

```
> a:=x^8-2*x^6+2*x^2-1;
```

$$a := x^8 - 2\,x^6 + 2\,x^2 - 1 \tag{8.2.1}$$

```
> debug(SquareFree); SquareFree(a,x);
```

SquareFree

```
{--> enter SquareFree, args = x^8-2*x^6+2*x^2-1, x
```

$$i := 1$$

$$out := 1$$

$$b := 8\,x^7 - 12\,x^5 + 4\,x$$

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

$$w := x^4 - 1$$

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

$$z := x^2 + 1$$

$$out := x^2 + 1$$

$$i := 2$$

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

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

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

$$z := 1$$

$$out := x^2 + 1$$

$$i := 3$$

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

$$c := 1$$

$$out := (x^2+1)(x^2-1)^3$$

```
<-- exit SquareFree (now at top level) = (x^2+1)*(x^2-1)^3}
```

$$(x^2+1)(x^2-1)^3 \tag{8.2.2}$$

A 8.2. Algoritmus.

```
>
```

E 8.2. Példa.

E 8.3. Példa.

```
> a:=x^13+1; diff(a,x) mod 13;
```

$$a := x^{13} + 1$$

$$0 \tag{8.5.1}$$

```
> (x+1)^13 mod 13; expand(%) mod 13;
```

$$(x+1)^{13}$$

$$x^{13} + 1 \tag{8.5.2}$$

A 8.3. Algoritmus.

```
> SquareFreeFF:=proc(a,x,p) local i,out,b,c,y,z,w;
```

E 8.4. Példa.

```
> a:=x^11+2*x^9+2*x^8+x^6+x^5+2*x^3+2*x^2+1;
```

$$a := x^{11} + 2x^9 + 2x^8 + x^6 + x^5 + 2x^3 + 2x^2 + 1 \tag{8.7.1}$$

```
> ap:=diff(a,x) mod 3;
```

$$ap := -x^{10} + x^7 - x^4 + x \tag{8.7.2}$$

```
> c:=Gcd(a,ap) mod 3;
```

$$c := x^9 - x^6 + x^3 - 1 \tag{8.7.3}$$

```
>
```

E 8.5. Példa.

```
>
```

▶ E 8.6. Példa.

▶ A 8.4. Algoritmus.

▶ A 8.5. Algoritmus.

▶ E 8.7. Példa.

▶ E 8.8. Példa.

▶ A 8.6. Algoritmus.

▶ E 8.9. Példa.

▶ E 8.10. Példa.

▶ E 8.11. Példa.

▶ E 8.12. Példa.

▶ E 8.13. Példa.

▶ A 8.7. Algoritmus.

▼ E 8.14. Példa.

```
> a:=x^63+1;
```

$$a := x^{63} + 1 \tag{8.21.1}$$

```
> a1:=Gcd(a,x^2-x) mod 2; a:=Quo(a,a1,x) mod 2;
```

$$a1 := x + 1$$

$$\begin{aligned} a := {} & 1 + x^{11} + x^{10} + x^4 + x^3 + x^7 + x^5 + x^{13} + x + x^{12} + x^8 + x^6 + x^2 + x^9 + x^{50} \\ & + x^{52} + x^{53} + x^{54} + x^{55} + x^{56} + x^{57} + x^{58} + x^{59} + x^{60} + x^{61} + x^{62} + x^{51} \\ & + x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{24} + x^{25} \\ & + x^{26} + x^{27} + x^{28} + x^{29} + x^{30} + x^{31} + x^{32} + x^{33} + x^{34} + x^{35} + x^{36} + x^{37} \\ & + x^{38} + x^{39} + x^{40} + x^{41} + x^{42} + x^{43} + x^{44} + x^{45} + x^{46} + x^{47} + x^{48} + x^{49} \end{aligned} \tag{8.21.2}$$

```
> a2:=Gcd(a,x^4-x) mod 2; a:=Quo(a,a2,x) mod 2;
```

$$a2 := x^2 + x + 1$$

$$\begin{aligned} a := {} & x^{60} + x^{57} + x^{54} + x^{51} + x^{48} + x^{45} + x^{42} + x^{39} + x^{36} + x^{33} + x^{30} + x^{27} + x^{24} \\ & + x^{21} + x^{18} + x^{15} + x^{12} + x^9 + x^6 + x^3 + 1 \end{aligned} \tag{8.21.3}$$

```
> a3:=Gcd(a,x^8-x) mod 2; a:=Quo(a,a3,x) mod 2;
```

$$a3 := x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$a := 1 + x^{11} + x^4 + x^3 + x + x^{12} + x^8 + x^6 + x^9 + x^{50} + x^{53} + x^{54} + x^{51} + x^{21} + x^{22} + x^{24} + x^{25} + x^{27} + x^{29} + x^{30} + x^{32} + x^{33} + x^{42} + x^{43} + x^{45} + x^{46} + x^{48} \quad (8.21.4)$$

```
> a4:=Gcd(a,x^16-x) mod 2; a:=Quo(a,a4,x) mod 2;
```

$$a4 := 1$$

$$a := 1 + x^{11} + x^4 + x^3 + x + x^{12} + x^8 + x^6 + x^9 + x^{50} + x^{53} + x^{54} + x^{51} + x^{21} + x^{22} + x^{24} + x^{25} + x^{27} + x^{29} + x^{30} + x^{32} + x^{33} + x^{42} + x^{43} + x^{45} + x^{46} + x^{48} \quad (8.21.5)$$

```
> a5:=Gcd(a,x^32-x) mod 2; a:=Quo(a,a5,x) mod 2;
```

$$a5 := 1$$

$$a := 1 + x^{11} + x^4 + x^3 + x + x^{12} + x^8 + x^6 + x^9 + x^{50} + x^{53} + x^{54} + x^{51} + x^{21} + x^{22} + x^{24} + x^{25} + x^{27} + x^{29} + x^{30} + x^{32} + x^{33} + x^{42} + x^{43} + x^{45} + x^{46} + x^{48} \quad (8.21.6)$$

```
> a6:=Gcd(a,x^64-x) mod 2; a:=Quo(a,a6,x) mod 2;
```

$$a6 := 1 + x^{11} + x^4 + x^3 + x + x^{12} + x^8 + x^6 + x^9 + x^{50} + x^{53} + x^{54} + x^{51} + x^{21} + x^{22} + x^{24} + x^{25} + x^{27} + x^{29} + x^{30} + x^{32} + x^{33} + x^{42} + x^{43} + x^{45} + x^{46} + x^{48}$$

$$a := 1 \quad (8.21.7)$$

A 8.8. Algoritmus.

```
> PartialFactorDD:=proc(a,x,p) local aa,L,aaa,w,i;
  i:=1; w:=x; aa:=a; L:=[];
  while i<=degree(aa)/2 do
    w:=Rem(w^p,aa,x) mod p;
    aaa:=Gcd(aa,w-x) mod p;
    L:=[op(L),aaa];
    if aaa<>1 then
      aa:=Quo(aa,aaa,x) mod p:
      w:=Rem(w,aa,x) mod p;
    fi; i:=i+1;
  od; L:=[op(L),aa]; end;
```

$$PartialFactorDD := \mathbf{proc}(a, x, p) \quad (8.22.1)$$

$$\mathbf{local}\ aa, L, aaa, w, i;$$

$$i := 1;$$

$$w := x;$$

$$aa := a;$$

$$L := [\,];$$

```
    while i <= 1 / 2 * degree(aa) do
        w := mod(Rem(w^p, aa, x), p);
        aaa := mod(Gcd(aa, w - x), p);
        L := [op(L), aaa];
        if aaa <> 1 then
            aa := mod(Quo(aa, aaa, x), p);
            w := mod(Rem(w, aa, x), p)
        end if;
        i := i + 1
    end do;
    L := [op(L), aa]
end proc
```

E 8.15. Példa.

```
> `mod`:=mods; a:=x^15-1; debug(PartialFactorDD);
  PartialFactorDD(a,x,11);
```

$$mod := mods$$

$$a := x^{15} - 1$$

$$PartialFactorDD$$

```
{--> enter PartialFactorDD, args = x^15-1, x, 11
```

$$i := 1$$

$$w := x$$

$$aa := x^{15} - 1$$

$$L := [\,]$$

$$w := x^{11}$$

$$aaa := x^5 - 1$$

$$L := [x^5 - 1]$$

$$aa := x^{10} + x^5 + 1$$

$$w := -x^6 - x$$

$$i := 2$$

$$w := x$$

$$aaa := x^{10} + x^5 + 1$$

$$L := [x^5 - 1, x^{10} + x^5 + 1]$$

$$aa := 1$$

$$w := 0$$

$$i := 3$$

$$L := \left[x^5 - 1,\ x^{10} + x^5 + 1,\ 1\right]$$

```
<-- exit PartialFactorDD (now at top level) = [x^5-1,
x^10+x^5+1, 1]}
```

$$\left[x^5 - 1,\ x^{10} + x^5 + 1,\ 1\right] \tag{8.23.1}$$

A 8.9. Algoritmus.

>

E 8.16. Példa.

>

E 8.17. Példa.

>

E 8.18. Példa.

>

E 8.19. Példa.

>

E 8.20. Példa.

>

A 8.10. Algoritmus.

>

E 8.21. Példa.

>

9. Egyenletrendszerek

10. Gröbner–bázisok

11. Racionális törtfüggvények integrálása

▶ 12. A Risch–algoritmus.