Komputeralgebrai algoritmusok

Járai Antal

Ezek a programok csak szemléltetésre szolgálnak.

▶ 1. Történet

▶ 2. Algebrai alapok

▶ 3. Normál formák, reprezentáció

▼ 4. Aritmetika

```
> restart;
```

▼ A 4.1. Algoritmus.

```
> BigIntegerMultiply:=proc(a,b,B) local c,t,i,j,carry;
    c:=[]; for i from 0 to nops(a)-1 do c:=[op(c),0] od;
    for j from 0 to nops(b)-1 do
      carry:=0;
      for i from 0 to nops(a)-1 do
        t:=a[i+1]*b[j+1]+c[i+j+1]+carry;
        carry:=iquo(t,B);
        c[i+j+1]:=irem(t,B)
      od;
      c:=[op(c),carry];
    od; c;
  end;
```

$$BigIntegerMultiply := \mathbf{proc}(a, b, B) \quad (4.1.1)$$

$\mathbf{local}\ c, t, i, j, carry;$
$c := [\,];$
$\mathbf{for}\ i\ \mathbf{from}\ 0\ \mathbf{to}\ nops(a) - 1\ \mathbf{do}$
$c := [op(c), 0]$
$\mathbf{end\ do};$
$\mathbf{for}\ j\ \mathbf{from}\ 0\ \mathbf{to}\ nops(b) - 1\ \mathbf{do}$
$carry := 0;$

```
        for i from 0 to nops(a) - 1 do
            t := a[i+1]*b[j+1] + c[i+j+1] + carry;
            carry := iquo(t, B);
            c[i+j+1] := irem(t, B)
        end do;
        c := [op(c), carry]
    end do;
    c
end proc
```

```
> a:=floor(evalf(10^10*Pi,20)); b:=floor(evalf(10^10*exp(1)));
  c:=a*b;
  a:=convert(a,base,10^4); b:=convert(b,base,10^4); c:=convert
  (c,base,10^4);
```

$$a := 31415926535$$

$$b := 27182818280$$

$$c := 853973422098735059800$$

$$a := [6535, 1592, 314]$$

$$b := [8280, 8281, 271]$$

$$c := [9800, 3505, 987, 3422, 5397, 8] \tag{4.1.2}$$

```
> BigIntegerMultiply(a,b,10^4);
```

$$[9800, 3505, 987, 3422, 5397, 8] \tag{4.1.3}$$

E 4.1. Példa.

```
> with(powseries);
```

$$[compose, evalpow, inverse, multconst, multiply, negative, powadd, powcos, powcreate, powdiff, powexp, powint, powlog, powpoly, powsin, powsolve, powsqrt, quotient, reversion, subtract, tpsform] \tag{4.2.1}$$

```
> a:=powpoly((1-x)^5,x); tpsform(a,x,8);
```

$$a := \mathbf{proc}(powparm) \ldots \mathbf{end\ proc}$$

$$1 - 5x + 10x^2 - 10x^3 + 5x^4 - x^5 \tag{4.2.2}$$

```
> b:=inverse(a); tpsform(b,x,8);
```

$$b := \mathbf{proc}(powparm) \ldots \mathbf{end\ proc}$$

$$1 + 5x + 15x^2 + 35x^3 + 70x^4 + 126x^5 + 210x^6 + 330x^7 + O(x^8) \tag{4.2.3}$$

E 4.2. Példa.

```
> a:=powpoly(x,x); b:=powsin(a); tpsform(b,x,8);
```

$$a := \mathbf{proc}(powparm) \ldots \mathbf{end\ proc}$$
$$b := \mathbf{proc}(powparm) \ldots \mathbf{end\ proc}$$
$$x - \frac{1}{6}x^3 + \frac{1}{120}x^5 - \frac{1}{5040}x^7 + O(x^8) \tag{4.3.1}$$

```
> c:=reversion(b); tpsform(c,x,8);
```

$$c := \mathbf{proc}(powparm) \ldots \mathbf{end\ proc}$$
$$x + \frac{1}{6}x^3 + \frac{3}{40}x^5 + \frac{5}{112}x^7 + O(x^8) \tag{4.3.2}$$

```
>
```

A 4.2. Algoritmus.

```
> Karatsuba:=proc(a,b,n,B) local aa,bb,a1,a2,b1,b2,n1,n2,c1,c2,
  c3,c,t;
    c:=sign(a)*sign(b);
    aa:=abs(a); bb:=abs(b);
    if n=1 then
      t:=BigIntegerMultiply([aa],[bb],B);
      return c*(t[2]*B+t[1])
    fi;
    n1:=floor(n/2); n2:=n-n1;
    a1:=iquo(aa,B^n1); a2:=irem(aa,B^n1);
    b1:=iquo(bb,B^n1); b2:=irem(bb,B^n2);
    c1:=Karatsuba(a1,b1,n1,B);
    c2:=Karatsuba(a1-a2,b2-b1,n2,B);
    c3:=Karatsuba(a2,b2,n2,B);
    c*(c1*B^(2*n1)+(c1+c2+c3)*B^n1+c3);
  end;
```

$$Karatsuba := \mathbf{proc}(a, b, n, B) \tag{4.4.1}$$
$$\mathbf{local}\ aa, bb, a1, a2, b1, b2, n1, n2, c1, c2, c3, c, t;$$
$$c := sign(a) * sign(b);$$
$$aa := \mathrm{abs}(a);$$
$$bb := \mathrm{abs}(b);$$
$$\mathbf{if}\ n = 1\ \mathbf{then}$$
$$t := BigIntegerMultiply([aa], [bb], B);$$
$$\mathbf{return}\ c * (t[2] * B + t[1])$$
$$\mathbf{end\ if};$$
$$n1 := \mathrm{floor}(1 / 2 * n);$$
$$n2 := n - n1;$$
$$a1 := iquo(aa, B\hat{}n1);$$

```
    a2 := irem(aa, B^n1);
    b1 := iquo(bb, B^n1);
    b2 := irem(bb, B^n2);
    c1 := Karatsuba(a1, b1, n1, B);
    c2 := Karatsuba(a1 - a2, b2 - b1,
    n2, B);
    c3 := Karatsuba(a2, b2, n2, B);
    c*(c1*B^(2*n1) + (c1 + c2 + c3)*B^n1 + c3)
end proc
> a:=floor(evalf(10^10*Pi,20)); b:=floor(evalf(10^10*exp(1)));
  c:=a*b;
  debug(Karatsuba); Karatsuba(a,b,3,10^4);
                        a := 31415926535
                        b := 27182818280
                  c := 853973422098735059800
                          Karatsuba
{--> enter Karatsuba, args = 31415926535, 27182818280, 3,
10000
                             c := 1
                        aa := 31415926535
                        bb := 27182818280
                             n1 := 1
                             n2 := 2
                          a1 := 3141592
                            a2 := 6535
                          b1 := 2718281
                          b2 := 82818280
{--> enter Karatsuba, args = 3141592, 2718281, 1, 10000
                             c := 1
                          aa := 3141592
                          bb := 2718281
                      t := [3352, 853972984]
<-- exit Karatsuba (now in Karatsuba) = 8539729843352}
                       c1 := 8539729843352
{--> enter Karatsuba, args = 3135057, 80099999, 2, 10000
                             c := 1
                          aa := 3135057
                          bb := 80099999
                             n1 := 1
```

$$n2 := 1$$
$$a1 := 313$$
$$a2 := 5057$$
$$b1 := 8009$$
$$b2 := 9999$$

```
{--> enter Karatsuba, args = 313, 8009, 1, 10000
```

$$c := 1$$
$$aa := 313$$
$$bb := 8009$$
$$t := [6817, 250]$$

```
<-- exit Karatsuba (now in Karatsuba) = 2506817}
```

$$c1 := 2506817$$

```
{--> enter Karatsuba, args = 4744, 1990, 1, 10000
```

$$c := -1$$
$$aa := 4744$$
$$bb := 1990$$
$$t := [560, 944]$$

```
<-- exit Karatsuba (now in Karatsuba) = 9440560}
```

$$c2 := -9440560$$

```
{--> enter Karatsuba, args = 5057, 9999, 1, 10000
```

$$c := 1$$
$$aa := 5057$$
$$bb := 9999$$
$$t := [4943, 5056]$$

```
<-- exit Karatsuba (now in Karatsuba) = 50564943}
```

$$c3 := 50564943$$
$$251118062564943$$

```
<-- exit Karatsuba (now in Karatsuba) = 251118062564943}
```

$$c2 := 251118062564943$$

```
{--> enter Karatsuba, args = 6535, 82818280, 2, 10000
```

$$c := 1$$
$$aa := 6535$$
$$bb := 82818280$$
$$n1 := 1$$
$$n2 := 1$$
$$a1 := 0$$
$$a2 := 6535$$
$$b1 := 8281$$
$$b2 := 8280$$

```
{--> enter Karatsuba, args = 0, 8281, 1, 10000
```
$$c := 1$$
$$aa := 0$$
$$bb := 8281$$
$$t := [0, 0]$$
```
<-- exit Karatsuba (now in Karatsuba) = 0}
```
$$c1 := 0$$
```
{--> enter Karatsuba, args = 6535, 1, 1, 10000
```
$$c := 1$$
$$aa := 6535$$
$$bb := 1$$
$$t := [6535, 0]$$
```
<-- exit Karatsuba (now in Karatsuba) = 6535}
```
$$c2 := 6535$$
```
{--> enter Karatsuba, args = 6535, 8280, 1, 10000
```
$$c := 1$$
$$aa := 6535$$
$$bb := 8280$$
$$t := [9800, 5410]$$
```
<-- exit Karatsuba (now in Karatsuba) = 54109800}
```
$$c3 := 54109800$$
$$541217459800$$
```
<-- exit Karatsuba (now in Karatsuba) = 541217459800}
```
$$c3 := 541217459800$$
$$856574974975098409800$$
```
<-- exit Karatsuba (now at top level) =
856574974975098409800}
```
$$856574974975098409800 \qquad (4.4.2)$$

A 4.3. Algoritmus.

```
> with(CurveFitting);
```
$$[BSpline, BSplineCurve, Interactive, LeastSquares, PolynomialInterpolation, RationalInterpolation, Spline, ThieleInterpolation] \qquad (4.5.1)$$

```
> TrialDivision:=proc(a,b,x,L) local i,c,y,La,Lb;
    La:=map(y->subs(x=y,a),L);
    Lb:=map(y->subs(x=y,b),L);
    for i to nops(L) do
      if Lb[i]=0 then
```

```
        if La[i]<>0 then return FAIL else La[i]=0 fi;
      else La[i]:=La[i]/Lb[i] fi;
    od;
    c:=PolynomialInterpolation(L,La,x);
    if degree(c,x)=degree(a,x)-degree(b,x) then c else FAIL fi;
  end;
```

$$TrialDivision := \mathbf{proc}(a, b, x, L) \tag{4.5.2}$$

```
  local i, c, y, La, Lb;
  La := map(proc(y)
      option operator, arrow;
      subs(x = y, a)
    end proc, L);
  Lb := map(proc(y)
      option operator, arrow;
      subs(x = y, b)
    end proc,
  L);
  for i to nops(L) do
    if Lb[i] = 0 then
      if La[i] <> 0 then
        return FAIL
      else
        La[i] = 0
      end if
    else
      La[i] := La[i] / Lb[i]
    end if
  end do;
  c := CurveFitting:-PolynomialInterpolation(L, La, x);
  if degree(c, x) = degree(a, x) - degree(b, x) then
    c
  else
    FAIL
  end if
end proc
```

```
> b:=3*x^3-4*x^2+x-3; c:=6*x^2+2*x-7; a:=expand(b*c); L:=[i$i=
  0..5];
```

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

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

$$a := 18x^5 - 18x^4 - 23x^3 + 12x^2 - 13x + 21$$
$$L := [0, 1, 2, 3, 4, 5] \tag{4.5.3}$$

```
> debug(TrialDivision); TrialDivision(a,b,x,L);
```

TrialDivision

```
{--> enter TrialDivision, args = 18*x^5-18*x^4-23*x^3+12*
x^2-13*x+21, 3*x^3-4*x^2+x-3, x, [0, 1, 2, 3, 4, 5]
```

$$La := [21, -3, 147, 2385, 12513, 42381]$$
$$Lb := [-3, -3, 7, 45, 129, 277]$$
$$La_1 := -7$$
$$La_2 := 1$$
$$La_3 := 21$$
$$La_4 := 53$$
$$La_5 := 97$$
$$La_6 := 153$$
$$c := 6x^2 + 2x - 7$$
$$6x^2 + 2x - 7$$

```
<-- exit TrialDivision (now at top level) = 6*x^2+2*x-7}
```

$$6x^2 + 2x - 7 \tag{4.5.4}$$

```
> a:=a-1; TrialDivision(a,b,x,L);
```

$$a := 18x^5 - 18x^4 - 23x^3 + 12x^2 - 13x + 18$$

```
{--> enter TrialDivision, args = 18*x^5-18*x^4-23*x^3+12*
x^2-13*x+18, 3*x^3-4*x^2+x-3, x, [0, 1, 2, 3, 4, 5]
```

$$La := [18, -6, 144, 2382, 12510, 42378]$$
$$Lb := [-3, -3, 7, 45, 129, 277]$$
$$La_1 := -6$$
$$La_2 := 2$$
$$La_3 := \frac{144}{7}$$
$$La_4 := \frac{794}{15}$$
$$La_5 := \frac{4170}{43}$$
$$La_6 := \frac{42378}{277}$$
$$c := \frac{241517}{3751965}x^5 - \frac{360901}{416885}x^4 + \frac{15463688}{3751965}x^3 - \frac{827249}{416885}x^2 + \frac{5000773}{750393}x - 6$$

$$FAIL$$

```
<-- exit TrialDivision (now at top level) = FAIL}
```

$$FAIL \tag{4.5.5}$$

E 4.3. Példa.

```
> omega:=(1+I)/sqrt(2); omega^8; omega^4;
```

$$\omega := \left(\frac{1}{2} + \frac{1}{2}\,\mathrm{I}\right)\sqrt{2}$$

$$1$$

$$-1 \tag{4.6.1}$$

```
> omega:=I; omega^8; omega^4;
```

$$\omega := \mathrm{I}$$

$$1$$

$$1 \tag{4.6.2}$$

E 4.4. Példa.

```
> 4^4 mod 17; [4^i$i=0..3] mod 17;
```

$$1$$

$$[1, 4, 16, 13] \tag{4.7.1}$$

```
> A:=Matrix(4,(i,j)->4^((i-1)*(j-1)) mod 17);
```

$$A := \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 16 & 13 \\ 1 & 16 & 1 & 16 \\ 1 & 13 & 16 & 4 \end{bmatrix} \tag{4.7.2}$$

E 4.5. Példa.

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

$$mod := mods \tag{4.8.1}$$

```
> 14&^8 mod 41;
```

$$1 \tag{4.8.2}$$

```
> [14&^i$i=0..7]; map(x->x mod 41,%);
```

$$[14\ \&^\wedge\ 0, 14\ \&^\wedge\ 1, 14\ \&^\wedge\ 2, 14\ \&^\wedge\ 3, 14\ \&^\wedge\ 4, 14\ \&^\wedge\ 5, 14\ \&^\wedge\ 6, 14\ \&^\wedge\ 7]$$

$$[1, 14, -9, -3, -1, -14, 9, 3] \tag{4.8.3}$$

```
> [(-9)&^i$i=0..3]; map(x->x mod 41,%);
```

$$[(-9)\,\&\hat{}\,0,\ (-9)\,\&\hat{}\,1,\ (-9)\,\&\hat{}\,2,\ (-9)\,\&\hat{}\,3]$$
$$[1, -9, -1, 9] \tag{4.8.4}$$

```
> [(-1)&^i$i=0..1]; map(x->x mod 41,%);
```

$$[(-1)\,\&\hat{}\,0,\ (-1)\,\&\hat{}\,1]$$
$$[1, -1] \tag{4.8.5}$$

E 4.6. Példa.

```
> a:=5*x^6+x^5+3*x^3+x^2-4*x+1;
```

$$a := 5\,x^6 + x^5 + 3\,x^3 + x^2 - 4\,x + 1 \tag{4.9.1}$$

```
> b:=5*y^3+y+1; c:=y^2+3*y-4; a=expand(subs(y=x^2,b+x*c));
```

$$b := 5\,y^3 + y + 1$$
$$c := y^2 + 3\,y - 4$$
$$5\,x^6 + x^5 + 3\,x^3 + x^2 - 4\,x + 1 = 5\,x^6 + x^5 + 3\,x^3 + x^2 - 4\,x + 1 \tag{4.9.2}$$

```
> d:=1; e:=5*z+1; b=expand(subs(z=y^2,d+y*e));
```

$$d := 1$$
$$e := 5\,z + 1$$
$$5\,y^3 + y + 1 = 5\,y^3 + y + 1 \tag{4.9.3}$$

```
> subs(z=1,d) mod 41; subs(z=1,e) mod 41;
```

$$1$$
$$6 \tag{4.9.4}$$

```
> subs(y=1,b) mod 41=1+1*6 mod 41; subs(y=-1,b) mod 41=1-1*6
  mod 41;
```

$$7 = 7$$
$$-5 = -5 \tag{4.9.5}$$

```
> subs(z=-1,d) mod 41; subs(z=-1,e) mod 41;
```

$$1$$
$$-4 \tag{4.9.6}$$

```
> subs(y=-9,b) mod 41=1+(-9)*(-4) mod 41; subs(y=9,b) mod 41=
  1+9*(-4) mod 41;
```

$$-4 = -4$$
$$6 = 6 \tag{4.9.7}$$

```
> subs(y=1,c) mod 41; subs(y=-1,c) mod 41;
  subs(y=-9,c) mod 41; subs(y=9,c) mod 41;
```

$$0$$
$$-6$$
$$9$$
$$-19 \tag{4.9.8}$$

```
> subs(x=3,a) mod 41=6+3*(-19) mod 41;
  subs(x=-3,a) mod 41=6+(-3)*(-19) mod 41;
```

$$-10 = -10$$

$$-19 = -19 \qquad (4.9.9)$$

```
> [14&^i$i=0..7]; map(x->x mod 41,%); map(y->subs(x=y,a) mod
  41,%);
```

$$[14 \&^\wedge 0,\ 14 \&^\wedge 1,\ 14 \&^\wedge 2,\ 14 \&^\wedge 3,\ 14 \&^\wedge 4,\ 14 \&^\wedge 5,\ 14 \&^\wedge 6,\ 14 \&^\wedge 7]$$

$$[1, 14, -9, -3, -1, -14, 9, 3]$$

$$[7, -1, 8, -19, 7, -7, -18, -10] \qquad (4.9.10)$$

A 4.4. Algoritmus.

```
> mFFT:=proc(a,x,omega,n,m) local A,B,C,b,c,i,j;
    if n=0 then return [a mod m] fi;
    b:=0; c:=0;
    for i from 0 to 2^(n-1)-1 do
      b:=b+coeff(a,x,2*i)*x^i;
      c:=c+coeff(a,x,2*i+1)*x^i;
    od;
    B:=mFFT(b,x,omega^2 mod m,n-1,m);
    C:=mFFT(c,x,omega^2 mod m,n-1,m);
    A:=[0$j=0..2^n-1];
    for i from 0 to 2^(n-1)-1 do
      A[i+1]:=B[i+1]+omega&^i*C[i+1] mod m;
      A[i+1+2^(n-1)]:=B[i+1]-omega&^i*C[i+1] mod m;
    od; A;
  end;
```

$mFFT := \mathbf{proc}(a, x, \text{omega}, n, m)$ (4.10.1)

$\mathbf{local}\ A, B, C, b, c, i, j;$

$\mathbf{if}\ n = 0\ \mathbf{then}$

$\mathbf{return}\ [mod(a, m)]$

$\mathbf{end\ if};$

$b := 0;$

$c := 0;$

$\mathbf{for}\ i\ \mathbf{from}\ 0\ \mathbf{to}\ 2\wedge(n-1)-1\ \mathbf{do}$

$b := b + coeff(a, x, 2*i)*x\wedge i;$

$c := c + coeff(a, x, 2*i+1)*x\wedge i$

$\mathbf{end\ do};$

$B := mFFT(b, x,$

$mod(\text{omega}\wedge 2, m), n-1, m);$

$C := mFFT(c, x, mod(\text{omega}\wedge 2, m),$

```
    n - 1, m);
    A := [ `$`(0, j = 0..2^n - 1)];
    for i from 0 to 2^(n - 1) - 1 do
        A[i + 1] := mod(B[i + 1] + omega &^ i * C[i + 1], m);
        A[i + 1 + 2^(n - 1)] := mod(B[i + 1] - omega &^ i * C[i + 1], m)
    end do;
    A
end proc
```

```
> debug(mFFT); mFFT(a,x,14,3,41); undebug(mFFT);
```

$$mFFT$$

```
{--> enter mFFT, args = 5*x^6+x^5+3*x^3+x^2-4*x+1, x, 14,
3, 41
```

$$b := 0$$

$$c := 0$$

$$b := 1$$

$$c := -4$$

$$b := 1 + x$$

$$c := -4 + 3\,x$$

$$b := 1 + x$$

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

$$b := 1 + x + 5\,x^3$$

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

```
{--> enter mFFT, args = 1+x+5*x^3, x, 9, 2, 41
```

$$b := 0$$

$$c := 0$$

$$b := 1$$

$$c := 1$$

$$b := 1$$

$$c := 1 + 5\,x$$

```
{--> enter mFFT, args = 1, x, 1, 1, 41
```

$$b := 0$$

$$c := 0$$

$$b := 1$$

$$c := 0$$

```
{--> enter mFFT, args = 1, x, 1, 0, 41
<-- exit mFFT (now in mFFT) = [1]}
```

$$B := [1]$$

```
{--> enter mFFT, args = 0, x, 1, 0, 41
<-- exit mFFT (now in mFFT) = [0]}
```

$$C := [0]$$
$$A := [0, 0]$$
$$A_1 := 1$$
$$A_2 := 1$$
$$[1, 1]$$

```
<-- exit mFFT (now in mFFT) = [1, 1]}
```

$$B := [1, 1]$$

```
{--> enter mFFT, args = 1+5*x, x, 1, 1, 41
```

$$b := 0$$
$$c := 0$$
$$b := 1$$
$$c := 5$$

```
{--> enter mFFT, args = 1, x, 1, 0, 41
<-- exit mFFT (now in mFFT) = [1]}
```

$$B := [1]$$

```
{--> enter mFFT, args = 5, x, 1, 0, 41
<-- exit mFFT (now in mFFT) = [5]}
```

$$C := [5]$$
$$A := [0, 0]$$
$$A_1 := 6$$
$$A_2 := -4$$
$$[6, -4]$$

```
<-- exit mFFT (now in mFFT) = [6, -4]}
```

$$C := [6, -4]$$
$$A := [0, 0, 0, 0]$$
$$A_1 := 7$$
$$A_3 := -5$$
$$A_2 := -4$$
$$A_4 := 6$$
$$[7, -4, -5, 6]$$

```
<-- exit mFFT (now in mFFT) = [7, -4, -5, 6]}
```

$$B := [7, -4, -5, 6]$$

```
{--> enter mFFT, args = -4+3*x+x^2, x, 9, 2, 41
```

$$b := 0$$
$$c := 0$$
$$b := -4$$
$$c := 3$$
$$b := x - 4$$

$$c := 3$$

```
{--> enter mFFT, args = x-4, x, 1, 1, 41
```

$$b := 0$$

$$c := 0$$

$$b := -4$$

$$c := 1$$

```
{--> enter mFFT, args = 4, x, 1, 0, 41
<-- exit mFFT (now in mFFT) = [-4]}
```

$$B := [-4]$$

```
{--> enter mFFT, args = 1, x, 1, 0, 41
<-- exit mFFT (now in mFFT) = [1]}
```

$$C := [1]$$

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

$$A_1 := -3$$

$$A_2 := -5$$

$$[-3, -5]$$

```
<-- exit mFFT (now in mFFT) = [-3, -5]}
```

$$B := [-3, -5]$$

```
{--> enter mFFT, args = 3, x, 1, 1, 41
```

$$b := 0$$

$$c := 0$$

$$b := 3$$

$$c := 0$$

```
{--> enter mFFT, args = 3, x, 1, 0, 41
<-- exit mFFT (now in mFFT) = [3]}
```

$$B := [3]$$

```
{--> enter mFFT, args = 0, x, 1, 0, 41
<-- exit mFFT (now in mFFT) = [0]}
```

$$C := [0]$$

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

$$A_1 := 3$$

$$A_2 := 3$$

$$[3, 3]$$

```
<-- exit mFFT (now in mFFT) = [3, 3]}
```

$$C := [3, 3]$$

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

$$A_1 := 0$$

$$A_3 := -6$$

$$A_2 := 9$$

$$A_4 := -19$$

$$[0, 9, -6, -19]$$

```
<-- exit mFFT (now in mFFT) = [0, 9, -6, -19]}
```

$$C := [0, 9, -6, -19]$$

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

$$A_1 := 7$$

$$A_5 := 7$$

$$A_2 := -1$$

$$A_6 := -7$$

$$A_3 := 8$$

$$A_7 := -18$$

$$A_4 := -19$$

$$A_8 := -10$$

$$[7, -1, 8, -19, 7, -7, -18, -10]$$

```
<-- exit mFFT (now at top level) = [7, -1, 8, -19, 7, -7,
-18, -10]}
```

$$[7, -1, 8, -19, 7, -7, -18, -10]$$

$$mFFT \tag{4.10.2}$$

E 4.7. Példa.

```
> `mod`:=modp;
```

$$mod := modp \tag{4.11.1}$$

```
> 4^4 mod 17; [4^i$i=0..3] mod 17;
```

$$1$$

$$[1, 4, 16, 13] \tag{4.11.2}$$

```
> A:=Matrix(4,(i,j)->4^((i-1)*(j-1)) mod 17);
```

$$A := \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 16 & 13 \\ 1 & 16 & 1 & 16 \\ 1 & 13 & 16 & 4 \end{bmatrix} \tag{4.11.3}$$

```
> B:=Matrix(4,(i,j)->4^(-((i-1)*(j-1))) mod 17);
```

(4.11.4)

$$B := \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 13 & 16 & 4 \\ 1 & 16 & 1 & 16 \\ 1 & 4 & 16 & 13 \end{bmatrix} \tag{4.11.4}$$

```
> evalm(A&*B); map(x->x mod 17,%);
```

$$\begin{bmatrix} 4 & 34 & 34 & 34 \\ 34 & 361 & 289 & 442 \\ 34 & 289 & 514 & 289 \\ 34 & 442 & 289 & 361 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} \tag{4.11.5}$$

A 4.5. Algoritmus.

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

$$mod := mods \tag{4.12.1}$$

```
> mFFT_Multiply:=proc(a,b,x,omega,n,m) local A,B,c,C,i;
    A:=mFFT(a,x,omega,n,m);
    B:=mFFT(b,x,omega,n,m);
    c:=0;
    for i from 0 to 2^n-1 do
      c:=c+A[i+1]*B[i+1]*x^i mod m;
    od;
    C:=mFFT(c,x,omega,n,m);
    c:=0;
    for i from 0 to 2^n-1 do
      c:=c+C[i+1]/2^n*x^i mod m;
    od; c;
  end;
```

$$mFFT_Multiply := \mathbf{proc}(a, b, x, \text{omega}, n, m) \tag{4.12.2}$$
$$\quad \mathbf{local}\ A, B, c, C, i;$$
$$\quad A := mFFT(a, x, \text{omega}, n, m);$$
$$\quad B := mFFT(b, x, \text{omega}, n, m);$$
$$\quad c := 0;$$
$$\quad \mathbf{for}\ i\ \mathbf{from}\ 0\ \mathbf{to}\ 2\text{^}n - 1\ \mathbf{do}$$

```
        c := mod(c + A[i+1]*B[i+1]*x^i, m)
    end do;
    C := mFFT(c, x, omega, n, m);
    c := 0;
    for i from 0 to 2^n - 1 do
        c := mod(c + C[i+1]*x^i/2^n, m)
    end do;
    c
end proc
```

E 4.8. Példa.

```
> a:=3*x^3+x^2-4*x+1; b:=x^3+2*x^2+5*x-3;
```

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

$$b := x^3 + 2x^2 + 5x - 3 \tag{4.13.1}$$

```
> debug(mFFT_Multiply); mFFT_Multiply(a,b,x,14,3,41); expand(a*
  b);
```

mFFT_Multiply

```
{--> enter mFFT_Multiply, args = 3*x^3+x^2-4*x+1, x^3+2*
x^2+5*x-3, x, 14, 3, 41
```

$$A := [1, 9, -19, -18, 3, 16, 19, -3]$$

$$B := [5, 5, 0, 14, -7, -6, -10, 16]$$

$$c := 0$$

$$c := 5$$

$$c := 5 + 4x$$

$$c := 5 + 4x$$

$$c := 5 + 4x - 6x^3$$

$$c := 5 + 4x - 6x^3 + 20x^4$$

$$c := 5 + 4x - 6x^3 + 20x^4 - 14x^5$$

$$c := 5 + 4x - 6x^3 + 20x^4 - 14x^5 + 15x^6$$

$$c := 5 + 4x - 6x^3 + 20x^4 - 14x^5 + 15x^6 - 7x^7$$

$$C := [17, 0, -17, 15, -19, -6, -4, 13]$$

$$c := 0$$

$$c := -3$$

$$c := -3$$

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

$$c := -3 + 3x^2 + 7x^3$$

$$c := -3 + 3\,x^2 + 7\,x^3 + 13\,x^4$$

$$c := -3 + 3\,x^2 + 7\,x^3 + 13\,x^4 - 11\,x^5$$

$$c := -3 + 3\,x^2 + 7\,x^3 + 13\,x^4 - 11\,x^5 + 20\,x^6$$

$$c := -3 + 3\,x^2 + 7\,x^3 + 13\,x^4 - 11\,x^5 + 20\,x^6 + 17\,x^7$$

$$-3 + 3\,x^2 + 7\,x^3 + 13\,x^4 - 11\,x^5 + 20\,x^6 + 17\,x^7$$

```
<-- exit mFFT_Multiply (now at top level) = -3+3*x^2+7*
x^3+13*x^4-11*x^5+20*x^6+17*x^7}
```

$$-3 + 3\,x^2 + 7\,x^3 + 13\,x^4 - 11\,x^5 + 20\,x^6 + 17\,x^7$$

$$3\,x^6 + 7\,x^5 + 13\,x^4 - 11\,x^3 - 21\,x^2 + 17\,x - 3 \qquad (4.13.2)$$

E 4.9. Példa.

```
> 14&^8 mod 41; 14&^4 mod 41;
```

$$1$$

$$-1 \qquad (4.14.1)$$

E 4.10. Példa.

```
> with(numtheory);
```

[*GIgcd*, *bigomega*, *cfrac*, *cfracpol*, *cyclotomic*, *divisors*, *factorEQ*, *factorset*, *fermat*, *imagunit*, *index*, *integral_basis*, *invcfrac*, *invphi*, *issqrfree*, *jacobi*, *kronecker*, λ, *legendre*, *mcombine*, *mersenne*, *migcdex*, *minkowski*, *mipolys*, *mlog*, *mobius*, *mroot*, *msqrt*, *nearestp*, *nthconver*, *nthdenom*, *nthnumer*, *nthpow*, *order*, *pdexpand*, ϕ, π, *pprimroot*, *primroot*, *quadres*, *rootsunity*, *safeprime*, σ, *sq2factor*, *sum2sqr*, τ, *thue*] (4.15.1)

```
> 2.^31/ln(2.^31)/phi(2^20);
```

$$190.6218996 \qquad (4.15.2)$$

E 4.11. Példa.

```
> 15&^8 mod 41; 15&^20 mod 41;
```

$$18$$

$$-1 \qquad (4.16.1)$$

```
> evalf(3./Pi^2);
```

$$0.3039635508 \qquad (4.16.2)$$

E 4.12. Példa.

```
> a:='a';
  powcreate(a(n)=1,a(0)=1,a(1)=-2,a(2)=3,a(3)=0,a(4)=1,a(5)=-1,
  a(6)=2);
  tpsform(a,x,8); convert(%,polynom);
```

$$a := a$$

$$1 - 2\,x + 3\,x^2 + x^4 - x^5 + 2\,x^6 + x^7 + \mathrm{O}\left(x^8\right)$$

$$1 - 2\,x + 3\,x^2 + x^4 - x^5 + 2\,x^6 + x^7 \tag{4.17.1}$$

```
> tpsform(a,x,1); convert(%,polynom); y:=powpoly(1/%,x); two:=
  powpoly(2,x);
```

$$1 + \mathrm{O}(x)$$

$$1$$

$$y := \mathbf{proc}(powparm)\ \ldots\ \mathbf{end\ proc}$$

$$two := \mathbf{proc}(powparm)\ \ldots\ \mathbf{end\ proc} \tag{4.17.2}$$

```
> multiply(y,subtract(two,multiply(y,a))); tpsform(%,x,2);
  convert(%,polynom); y:=powpoly(%,x);
```

$$\mathbf{proc}(powparm)\ \ldots\ \mathbf{end\ proc}$$

$$1 + 2\,x + \mathrm{O}\left(x^2\right)$$

$$1 + 2\,x$$

$$y := \mathbf{proc}(powparm)\ \ldots\ \mathbf{end\ proc} \tag{4.17.3}$$

```
> multiply(y,subtract(two,multiply(y,a))); tpsform(%,x,4);
  convert(%,polynom); y:=powpoly(%,x);
```

$$\mathbf{proc}(powparm)\ \ldots\ \mathbf{end\ proc}$$

$$1 + 2\,x + x^2 - 4\,x^3 + \mathrm{O}\left(x^4\right)$$

$$1 + 2\,x + x^2 - 4\,x^3$$

$$y := \mathbf{proc}(powparm)\ \ldots\ \mathbf{end\ proc} \tag{4.17.4}$$

```
> multiply(y,subtract(two,multiply(y,a))); tpsform(%,x,8);
  convert(%,polynom); y:=powpoly(%,x);
```

$$\mathbf{proc}(powparm)\ \ldots\ \mathbf{end\ proc}$$

$$1 + 2\,x + x^2 - 4\,x^3 - 12\,x^4 - 13\,x^5 + 9\,x^6 + 57\,x^7 + \mathrm{O}\left(x^8\right)$$

$$1 + 2\,x + x^2 - 4\,x^3 - 12\,x^4 - 13\,x^5 + 9\,x^6 + 57\,x^7$$

$$y := \mathbf{proc}(powparm)\ \ldots\ \mathbf{end\ proc} \tag{4.17.5}$$

```
> multiply(y,a); tpsform(%,x,8);
```

$$\mathbf{proc}(powparm)\ \ldots\ \mathbf{end\ proc}$$

$$1 + \mathrm{O}\left(x^8\right) \tag{4.17.6}$$

A 4.6. Algoritmus.

```
> FastNewtonInversion:=proc(a,x,n) local y,yy,k,two;
    tpsform(a,x,1); yy:=convert(1/%,polynom);
    y:=powpoly(yy,x); two:=powpoly(2,x);
    for k to n do
      multiply(y,subtract(two,multiply(y,a))); tpsform(%,x,2^k)
  ;
      yy:=convert(%,polynom); y:=powpoly(yy,x);
    od; yy;
  end;
```

$$FastNewtonInversion := \mathbf{proc}(a, x, n) \tag{4.18.1}$$

```
    local y, yy, k, two;
    powseries:-tpsform(a, x, 1);
    yy := convert(1 / `%`, polynom);
    y := powseries:-powpoly(yy, x);
    two := powseries:-powpoly(2, x);
    for k to n do
        powseries:-multiply(y, powseries:-subtract(two,
       powseries:-multiply(y, a)));
        powseries:-tpsform(`%`, x, 2^k);
        yy := convert(`%`, polynom);
        y := powseries:-powpoly(yy, x)
    end do;
    yy
end proc
```

```
> FastNewtonInversion(a,x,3);
```

$$1 + 2\,x + x^2 - 4\,x^3 - 12\,x^4 - 13\,x^5 + 9\,x^6 + 57\,x^7 \tag{4.18.2}$$

E 4.13. Példa.

```
> G:=(1-2*t*x+x^2)^(-1/2); series(G,x);
```

$$G := \frac{1}{\sqrt{1 - 2\,t\,x + x^2}}$$

$$1 + t\,x + \left(-\frac{1}{2} + \frac{3}{2}\,t^2\right)x^2 + \left(-\frac{3}{2}\,t + \frac{5}{2}\,t^3\right)x^3 + \left(\frac{3}{8} - \frac{15}{4}\,t^2 + \frac{35}{8}\,t^4\right)x^4 + \left(\frac{15}{8}\,t - \frac{35}{4}\,t^3 + \frac{63}{8}\,t^5\right)x^5 + O(x^6) \tag{4.19.1}$$

E 4.14. Példa.

```
> P:=(1-2*t*x+x^2)*y^2-1; PP:=diff(P,y); y0:=1;
```

$$P := \left(1 - 2\,t\,x + x^2\right) y^2 - 1$$

$$PP := 2\left(1 - 2\,t\,x + x^2\right) y$$

$$y0 := 1 \tag{4.20.1}$$

```
> y1:=series(y0-subs(y=y0,P)/subs(y=y0,PP),x,2);
  y1:=convert(y1,polynom);
```

$$y1 := 1 + t\,x + \mathrm{O}\left(x^2\right)$$

$$y1 := 1 + t\,x \tag{4.20.2}$$

```
> y2:=series(y1-subs(y=y1,P)/subs(y=y1,PP),x,4);
  y2:=convert(y2,polynom);
```

$$y2 := 1 + t\,x + \left(-\frac{1}{2} + \frac{3}{2}\,t^2\right) x^2 + \left(t^3 - t + \frac{1}{2}\left(3\,t^2 - 1\right) t\right) x^3 + \mathrm{O}\left(x^4\right)$$

$$y2 := 1 + t\,x + \left(-\frac{1}{2} + \frac{3}{2}\,t^2\right) x^2 + \left(t^3 - t + \frac{1}{2}\left(3\,t^2 - 1\right) t\right) x^3 \tag{4.20.3}$$

E 4.15. Példa.

```
> a:=4+x+2*x^2+3*x^3;
```

$$a := 4 + x + 2\,x^2 + 3\,x^3 \tag{4.21.1}$$

```
> P:=y^2-a; y0:=-2; y0:=2;
```

$$P := y^2 - 4 - x - 2\,x^2 - 3\,x^3$$

$$y0 := -2$$

$$y0 := 2 \tag{4.21.2}$$

```
> yy:=series(2-(4-a)/4,x,2); yy:=convert(yy,polynom);
```

$$yy := 2 + \frac{1}{4}\,x + \mathrm{O}\left(x^2\right)$$

$$yy := 2 + \frac{1}{4}\,x \tag{4.21.3}$$

```
> yy:=series(yy-(yy^2-a)/2/yy,x,4); yy:=convert(yy,polynom);
```

$$yy := 2 + \frac{1}{4}\,x + \frac{31}{64}\,x^2 + \frac{353}{512}\,x^3 + \mathrm{O}\left(x^4\right)$$

$$yy := 2 + \frac{1}{4}\,x + \frac{31}{64}\,x^2 + \frac{353}{512}\,x^3 \tag{4.21.4}$$

```
> series(yy^2,x,4);
```

$$4 + x + 2\,x^2 + 3\,x^3 + \mathrm{O}\left(x^4\right) \tag{4.21.5}$$

A 4.7. Algoritmus.

```
> NewtonSolve:=proc(P,y,x,y0,n) local yy,k,PP;
    PP:=diff(P,y); yy:=y0;
    for k to n do
      yy:=series(yy-subs(y=yy,P)/subs(y=yy,PP),x,2^k);
      yy:=convert(yy,polynom);
    od; yy;
  end;
```

$$NewtonSolve := \mathbf{proc}(P, y, x, y0, n) \tag{4.22.1}$$

$$\mathbf{local}\ yy,\ k,\ PP;$$
$$PP := diff(P, y);$$
$$yy := y0;$$
$$\mathbf{for}\ k\ \mathbf{to}\ n\ \mathbf{do}$$
$$yy := series(yy - subs(y = yy, P) / subs(y = yy, PP), x, 2\text{^}k);$$
$$yy := convert(yy, polynom)$$
$$\mathbf{end\ do};$$
$$yy$$
$$\mathbf{end\ proc}$$

```
> NewtonSolve(P,y,x,2,3);
```

$$2 + \frac{1}{4}x + \frac{31}{64}x^2 + \frac{353}{512}x^3 - \frac{2373}{16384}x^4 - \frac{19513}{131072}x^5 - \frac{136629}{2097152}x^6 + \frac{1579201}{16777216}x^7 \tag{4.22.2}$$

```
> series(%^2,x,8);
```

$$4 + x + 2x^2 + 3x^3 + O(x^8) \tag{4.22.3}$$

5. Kínai maradékolás

6. Newton–iteráció, Hensel–felemelés

7. Legnagyobb közös osztó

8. Faktorizálás

9. Egyenletrendszerek

10. Gröbner–bázisok

▶ 11. Racionális törtfüggvények integrálása

▶ 12. A Risch–algoritmus.