Számítógépes számelmélet

Járai Antal

Ezek a programok csak szemléltetésre szolgálnak

▶ 1. A prímek eloszlása, szitálás

▶ 2. Egyszerű faktorizálási módszerek

▶ 3. Egyszerű prímtesztelési módszerek

▶ 4. Lucas-sorozatok

▶ 5. Alkalmazások

▶ 6. Számok és polinomok

▶ 7. Gyors Fourier-transzformáció

▶ 8. Elliptikus függvények

▶ 9. Számolás elliptikus görbéken

▶ 10. Faktorizálás elliptikus gürbékkel

▶ 11. Prímteszt elliptikus görbékkel

▼ 12. Polinomfaktorizálás

```
> restart; with(PolynomialTools);
```

[CoefficientList, CoefficientVector, GcdFreeBasis, GreatestFactorialFactorization, Hurwitz, IsSelfReciprocal, MinimalPolynomial, PDEToPolynomial, PolynomialToPDE, ShiftEquivalent, ShiftlessDecomposition, Shorten, Shorter, Sort, Split, Splits, Translate] (12.1)

▶ 12.1. Polinomfaktorizálás modulo egy prím.

▼ 12.2. Visszavezetés négyzetmentes esetre.

```
> SquareFree:=proc(a,x,p) local i,out,b,c,y,z,w;
  i:=1; out:=[]; b:=diff(a,x) mod p;
  if b=0 then error "zero derivative; substitute x^p with p";
  fi;
  c:=Gcd(a,b) mod p; w:=Quo(a,c,x) mod p;
  while degree(c)<>0 do
    y:=Gcd(w,c) mod p;
    z:=Quo(w,y,x) mod p;
    out:=[op(out),z];
    i:=i+1;
    w:=y; c:=Quo(c,y,x) mod p;
  od; out:=[c,op(out),w]; end;
```

SquareFree := **proc**(*a*, *x*, *p*) (12.2.1)

```
    local i, out, b, c, y, z, w;
    i := 1;
    out := [ ];
    b := mod(diff(a, x), p);
    if b = 0 then
        error "zero derivative; substitute x^p with p"
    end if;
    c := mod(Gcd(a, b), p);
    w := mod(Quo(a, c, x), p);
    while degree(c) <> 0 do
        y := mod(Gcd(w, c), p);
        z := mod(Quo(w, y, x), p);
        out := [op(out), z];
        i := i + 1;
        w := y;
        c := mod(Quo(c, y, x), p)
    end do;
    out := [c, op(out), w]
end proc
```

```
> `mod`:=mods; x:='x'; a:=x^15-1; debug(SquareFree); SquareFree
```

```
(a,x,5);
```

$$mod := mods$$

$$x := x$$

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

$$SquareFree$$

```
{--> enter SquareFree, args = x^15-1, x, 5
```

$$i := 1$$

$$out := [\,]$$

$$b := 0$$

```
<-- ERROR in SquareFree (now at top level) = zero derivative;
substitute x^p with p}
Error, (in SquareFree) zero derivative; substitute x^p with p
> SquareFree(a,x,11);
{--> enter SquareFree, args = x^15-1, x, 11
```

$$i := 1$$

$$out := [\,]$$

$$b := 4\,x^{14}$$

$$c := 1$$

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

$$out := \left[1,\, x^{15} - 1\right]$$

```
<-- exit SquareFree (now at top level) = [1, x^15-1]}
```

$$\left[1,\, x^{15} - 1\right] \tag{12.2.2}$$

```
> SquareFree(x^3+3*x^2+3*x+1,x,11);
{--> enter SquareFree, args = x^3+3*x^2+3*x+1, x, 11
```

$$i := 1$$

$$out := [\,]$$

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

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

$$w := x + 1$$

$$y := x + 1$$

$$z := 1$$

$$out := [1]$$

$$i := 2$$

$$w := x + 1$$

$$c := x + 1$$

$$y := x + 1$$

$$z := 1$$

$$out := [1, 1]$$

$$i := 3$$

$$w := x + 1$$

$$c := 1$$

$$out := [1, 1, 1, x + 1]$$

```
<-- exit SquareFree (now at top level) = [1, 1, 1, x+1]}
```

$$[1, 1, 1, x + 1] \tag{12.2.3}$$

12.3. Véges testek.

```
> n:=8; RijndaelPoly:=Nextprime(Z^n,Z) mod 2; alpha:=Z;
```

$$n := 8$$

$$RijndaelPoly := Z^8 + Z^4 + Z^3 + Z + 1$$

$$\alpha := Z \tag{12.3.1}$$

```
> x:=234; xx:=convert(x,base,2); xxx:=add(xx[i]*Z^(i-1),i=1..
  nops(xx));
```

$$x := 234$$

$$xx := [0, 1, 0, 1, 0, 1, 1, 1]$$

$$xxx := Z + Z^3 + Z^5 + Z^6 + Z^7 \tag{12.3.2}$$

```
> y:=111; yy:=convert(y,base,2); yyy:=add(yy[i]*Z^(i-1),i=1..
  nops(yy));
```

$$y := 111$$

$$yy := [1, 1, 1, 1, 0, 1, 1]$$

$$yyy := 1 + Z + Z^2 + Z^3 + Z^5 + Z^6 \tag{12.3.3}$$

```
> zzz:=modpol(xxx+yyy,RijndaelPoly,Z,2); zz:=CoefficientList
  (zzz,Z);
  z:=add(zz[i]*2^(i-1),i=1..nops(zz));
```

$$zzz := Z^7 + 1 + Z^2$$

$$zz := [1, 0, 1, 0, 0, 0, 0, 1]$$

$$z := 133 \tag{12.3.4}$$

```
> zzz:=modpol(xxx*yyy,RijndaelPoly,Z,2); zz:=CoefficientList
  (zzz,Z);
  z:=add(zz[i]*2^(i-1),i=1..nops(zz));
```

$$zzz := Z^6 + Z^5 + Z^4 + Z^3 + Z^2 + 1$$

$$zz := [1, 0, 1, 1, 1, 1, 1]$$

$$z := 125 \quad (12.3.5)$$

```
> zzz:=modpol(1/xxx,RijndaelPoly,Z,2); zz:=CoefficientList(zzz,
  Z);
  z:=add(zz[i]*2^(i-1),i=1..nops(zz));
```

$$zzz := Z^7 + Z^6 + Z^4 + Z^2 + Z + 1$$

$$zz := [1, 1, 1, 0, 1, 0, 1, 1]$$

$$z := 215 \quad (12.3.6)$$

12.4. Faktorizálás különböző fokú faktorokra.

```
> 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 := **proc**(*a*, *x*, *p*) (12.4.1)

```
    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

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

$$mod := mods$$

$$x := x$$

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

$$PartialFactorDD$$

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

$$i := 1$$

$$w := x$$

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

$$L := []$$

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

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

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

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

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

$$i := 2$$

$$w := x$$

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

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

$$aa := 1$$

$$w := 0$$

$$i := 3$$

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

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

$$[x^5 - 1, x^{10} + x^5 + 1, 1] \qquad (12.4.2)$$

12.5. Hasítás.

```
> PartialFactorSplit:=proc(a,x,d,p) local t,i;
  t:=rand(); t:=convert(t,base,p); t:=add(t[i]*x^(i-1),i=1..
  nops(t));
  t:=modpol(t,a,x,p); t:=modpol(t^((p^d-1)/2)-1,a,x,p);
  t:=Gcd(t,a) mod p; [t,Quo(a,t,x) mod p]; end;
```

PartialFactorSplit := **proc**(*a*, *x*, *d*, *p*) (12.5.1)

```
    local t, i;
    t := rand();
    t := convert(t, base, p);
    t := add(t[i]*x^(i - 1), i = 1 ..nops(t));
    t := modpol(t, a, x, p);
    t := modpol(t^(1/2*p^d - 1/2) - 1, a, x, p);
    t := mod(Gcd(t, a), p);
    [t, mod(Quo(a, t, x), p)]
end proc
```

```
> debug(PartialFactorSplit); PartialFactorSplit(x^5-1,x,1,11);
```

PartialFactorSplit

```
{--> enter PartialFactorSplit, args = x^5-1, x, 1, 11
```

$$t := 395718860534$$

$$t := [8, 0, 10, 6, 8, 10, 6, 0, 9, 2, 4, 1]$$

$$t := 8 + 10 x^2 + 6 x^3 + 8 x^4 + 10 x^5 + 6 x^6 + 9 x^8 + 2 x^9 + 4 x^{10} + x^{11}$$

$$t := -x^2 + 4 x^3 - x^4 - 4 x$$

$$t := -5 x^4 + x^3 - 2 x^2 - 4 x - 1$$

$$t := x^2 - 5 x + 4$$

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

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

$$[x^2 - 5 x + 4, x^3 + 5 x^2 - x - 3] \quad (12.5.2)$$

```
> expand((x^2+2*x-2)*(x^3-2*x^2-5*x-5)) mod 11;
```

$$x^5 - 1 \quad (12.5.3)$$

```
> PartialFactorSplit(x^2+2*x-2,x,1,11);
  PartialFactorSplit(x^3-2*x^2-5*x-5,x,1,11);
{--> enter PartialFactorSplit, args = x^2+2*x-2, x, 1, 11
```

$$t := 193139816415$$

$$t := [7, 9, 7, 3, 3, 4, 1, 0, 10, 4, 7]$$

$$t := 7 + 9x + 7x^2 + 3x^3 + 3x^4 + 4x^5 + x^6 + 10x^8 + 4x^9 + 7x^{10}$$

$$t := -2 - 5x$$

$$t := -x + 3$$

$$t := 1$$

$$[1, x^2 + 2x - 2]$$

```
<-- exit PartialFactorSplit (now at top level) = [1,
x^2+2*x-2]}
```

$$[1, x^2 + 2x - 2]$$

```
{--> enter PartialFactorSplit, args = x^3-2*x^2-5*x-5, x,
1, 11
```

$$t := 22424170465$$

$$t := [4, 9, 1, 0, 5, 9, 7, 6, 5, 9]$$

$$t := 4 + 9x + x^2 + 5x^4 + 9x^5 + 7x^6 + 6x^7 + 5x^8 + 9x^9$$

$$t := -2x + 2$$

$$t := -2x^2 + 2x - 1$$

$$t := 1$$

$$[1, x^3 - 2x^2 - 5x - 5]$$

```
<-- exit PartialFactorSplit (now at top level) = [1, x^3
-2*x^2-5*x-5]}
```

$$[1, x^3 - 2x^2 - 5x - 5] \quad (12.5.4)$$

```
> expand((x-4)*(x-5)) mod 11; expand((x+2)*(x^2-4*x+3)) mod 11;
```

$$x^2 + 2x - 2$$

$$x^3 - 2x^2 - 5x - 5 \quad (12.5.5)$$

```
> PartialFactorSplit(x^2-4*x+3,x,1,11);
{--> enter PartialFactorSplit, args = x^2-4*x+3, x, 1, 11
```

$$t := 800187484459$$

$$t := [0, 3, 6, 9, 7, 10, 2, 10, 3, 9, 8, 2]$$

$$t := 3x + 6x^2 + 9x^3 + 7x^4 + 10x^5 + 2x^6 + 10x^7 + 3x^8 + 9x^9 + 8x^{10} + 2x^{11}$$

$$t := -2x + 5$$

$$t := -x + 1$$

$$t := x - 1$$

$$[x - 1, x - 3]$$

```
<-- exit PartialFactorSplit (now at top level) = [x-1, x
-3]}
```

$$[x - 1, x - 3] \quad (12.5.6)$$

```
> PartialFactorSplit(x^2-4*x+3,x,1,11);
{--> enter PartialFactorSplit, args = x^2-4*x+3, x, 1, 11
```

$$t := 427552056869$$

$$t := [3, 3, 5, 8, 9, 10, 1, 6, 3, 5, 5, 1]$$

$$t := 3 + 3x + 5x^2 + 8x^3 + 9x^4 + 10x^5 + x^6 + 6x^7 + 3x^8 + 5x^9 + 5x^{10} + x^{11}$$

$$t := 4x$$

$$t := 0$$

$$t := x^2 - 4x + 3$$

$$[x^2 - 4x + 3, 1]$$

```
<-- exit PartialFactorSplit (now at top level) = [x^2-4*
x+3, 1]}
```

$$[x^2 - 4x + 3, 1] \quad (12.5.7)$$

```
> expand((x-3)*(x-1)) mod 11;
```

$$x^2 - 4x + 3 \quad (12.5.8)$$

```
> PartialFactorSplit(x^10+x^5+1,x,2,11);
{--> enter PartialFactorSplit, args = x^10+x^5+1, x, 2, 11
```

$$t := 842622684442$$

$$t := [0, 4, 4, 1, 10, 5, 9, 9, 3, 5, 10, 2]$$

$$t := 4x + 4x^2 + x^3 + 10x^4 + 5x^5 + 9x^6 + 9x^7 + 3x^8 + 5x^9 + 10x^{10} + 2x^{11}$$

$$t := 5x^9 + 3x^8 - 2x^7 - 4x^6 - 5x^5 - x^4 + x^3 + 4x^2 + 2x + 1$$

$$t := -3x^9 - 3x^7 - 4x^6 + x^3 - 3x^2 + 1$$

$$t := x^4 - 2x^3 - 5x^2 + 4x + 4$$

$$[x^4 - 2x^3 - 5x^2 + 4x + 4, x^6 + 2x^5 - 2x^4 + 2x^3 + 4x^2 - 3x + 3]$$

```
<-- exit PartialFactorSplit (now at top level) = [x^4-2*
x^3-5*x^2+4*x+4, x^6+2*x^5-2*x^4+2*x^3+4*x^2-3*x+3]}
```

$$[x^4 - 2x^3 - 5x^2 + 4x + 4, x^6 + 2x^5 - 2x^4 + 2x^3 + 4x^2 - 3x + 3] \quad (12.5.9)$$

```
> expand((x^6-2*x^5+3*x^4+x^3-2*x^2+4*x+5)*(x^4+2*x^3+x^2-5*x
  -2)) mod 11;
```

$$x^{10} + x^5 + 1 \quad (12.5.10)$$

```
> PartialFactorSplit(x^6-2*x^5+3*x^4+x^3-2*x^2+4*x+5,x,2,11);
  PartialFactorSplit(x^4+2*x^3+x^2-5*x-2,x,2,11);
{--> enter PartialFactorSplit, args = x^6-2*x^5+3*x^4+x^3
-2*x^2+4*x+5, x, 2, 11
```

$$t := 412286285840$$

$$t := [0, 4, 8, 0, 5, 9, 8, 3, 9, 9, 4, 1]$$

$$t := 4x + 8x^2 + 5x^4 + 9x^5 + 8x^6 + 3x^7 + 9x^8 + 9x^9 + 4x^{10} + x^{11}$$

$$t := 3\,x^5 - 4\,x^4 - 4\,x^3 + 4\,x^2 + 1$$

$$t := 5\,x^5 - 2\,x^4 - x^3 + 5\,x^2 + x$$

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

$$\left[x^4 + 4\,x^3 + 2\,x^2 + x - 2,\ x^2 + 5\,x + 3\right]$$

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

$$\left[x^4 + 4\,x^3 + 2\,x^2 + x - 2,\ x^2 + 5\,x + 3\right]$$

```
{--> enter PartialFactorSplit, args = x^4+2*x^3+x^2-5*x
-2, x, 2, 11
```

$$t := 996417214180$$

$$t := [3, 8, 9, 4, 10, 5, 10, 3, 6, 4, 5, 3]$$

$$t := 3 + 8\,x + 9\,x^2 + 4\,x^3 + 10\,x^4 + 5\,x^5 + 10\,x^6 + 3\,x^7 + 6\,x^8 + 4\,x^9 + 5\,x^{10} + 3\,x^{11}$$

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

$$t := -2$$

$$t := 1$$

$$\left[1,\ x^4 + 2\,x^3 + x^2 - 5\,x - 2\right]$$

```
<-- exit PartialFactorSplit (now at top level) = [1,
x^4+2*x^3+x^2-5*x-2]}
```

$$\left[1,\ x^4 + 2\,x^3 + x^2 - 5\,x - 2\right] \qquad (12.5.11)$$

```
> expand((x^2+3*x-2)*(x^4-5*x^3-2*x^2-3*x+3)) mod 11;
```

$$x^6 - 2\,x^5 + 3\,x^4 + x^3 - 2\,x^2 + 4\,x + 5 \qquad (12.5.12)$$

```
> PartialFactorSplit(x^4-5*x^3-2*x^2-3*x+3,x,2,11);
  PartialFactorSplit(x^4+2*x^3+x^2-5*x-2,x,2,11);
{--> enter PartialFactorSplit, args = x^4-5*x^3-2*x^2-3*
x+3, x, 2, 11
```

$$t := 386408307450$$

$$t := [0, 4, 6, 3, 6, 4, 9, 6, 9, 9, 3, 1]$$

$$t := 4\,x + 6\,x^2 + 3\,x^3 + 6\,x^4 + 4\,x^5 + 9\,x^6 + 6\,x^7 + 9\,x^8 + 9\,x^9 + 3\,x^{10} + x^{11}$$

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

$$t := 0$$

$$t := x^4 - 5\,x^3 - 2\,x^2 - 3\,x + 3$$

$$\left[x^4 - 5\,x^3 - 2\,x^2 - 3\,x + 3,\ 1\right]$$

```
<-- exit PartialFactorSplit (now at top level) = [x^4-5*
x^3-2*x^2-3*x+3, 1]}
```

$$\left[x^4 - 5\,x^3 - 2\,x^2 - 3\,x + 3,\ 1\right]$$

```
{--> enter PartialFactorSplit, args = x^4+2*x^3+x^2-5*x
-2, x, 2, 11
```

$$t := 694607189265$$

$$t := [0, 2, 1, 7, 1, 7, 3, 4, 6, 8, 4, 2]$$

$$t := 2\,x + x^2 + 7\,x^3 + x^4 + 7\,x^5 + 3\,x^6 + 4\,x^7 + 6\,x^8 + 8\,x^9 + 4\,x^{10} + 2\,x^{11}$$

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

$$t := -2$$

$$t := 1$$

$$\left[1,\ x^4 + 2\,x^3 + x^2 - 5\,x - 2\right]$$

```
<-- exit PartialFactorSplit (now at top level) = [1,
x^4+2*x^3+x^2-5*x-2]}
```

$$\left[1,\ x^4 + 2\,x^3 + x^2 - 5\,x - 2\right] \tag{12.5.13}$$

```
> expand((x^2+4*x+5)*(x^2-2*x+4)) mod 11;
```

$$x^4 + 2\,x^3 + x^2 - 5\,x - 2 \tag{12.5.14}$$

```
> PartialFactorSplit(x^4-5*x^3-2*x^2-3*x+3,x,2,11);
{--> enter PartialFactorSplit, args = x^4-5*x^3-2*x^2-3*
x+3, x, 2, 11
```

$$t := 773012980023$$

$$t := [9, 10, 1, 7, 4, 7, 8, 1, 9, 8, 7, 2]$$

$$t := 9 + 10\,x + x^2 + 7\,x^3 + 4\,x^4 + 7\,x^5 + 8\,x^6 + x^7 + 9\,x^8 + 8\,x^9 + 7\,x^{10} + 2\,x^{11}$$

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

$$t := -2$$

$$t := 1$$

$$\left[1,\ x^4 - 5\,x^3 - 2\,x^2 - 3\,x + 3\right]$$

```
<-- exit PartialFactorSplit (now at top level) = [1, x^4
-5*x^3-2*x^2-3*x+3]}
```

$$\left[1,\ x^4 - 5\,x^3 - 2\,x^2 - 3\,x + 3\right] \tag{12.5.15}$$

```
> PartialFactorSplit(x^4-5*x^3-2*x^2-3*x+3,x,2,11);
{--> enter PartialFactorSplit, args = x^4-5*x^3-2*x^2-3*
x+3, x, 2, 11
```

$$t := 730616292946$$

$$t := [1, 4, 7, 9, 3, 9, 1, 4, 9, 1, 6, 2]$$

$$t := 1 + 4\,x + 7\,x^2 + 9\,x^3 + 3\,x^4 + 9\,x^5 + x^6 + 4\,x^7 + 9\,x^8 + x^9 + 6\,x^{10} + 2\,x^{11}$$

$$t := 4+4\,x-5\,x^3+3\,x^2$$

$$t := -3\,x^3+1$$

$$t := x^2+5\,x+3$$

$$\left[x^2+5\,x+3,\ x^2+x+1\right]$$

```
<-- exit PartialFactorSplit (now at top level) = [x^2+5*
x+3, x^2+x+1]}
```

$$\left[x^2+5\,x+3,\ x^2+x+1\right] \tag{12.5.16}$$

```
> PartialFactorSplit(x^4-5*x^3-2*x^2-3*x+3,x,2,11);
{--> enter PartialFactorSplit, args = x^4-5*x^3-2*x^2-3*
x+3, x, 2, 11
```

$$t := 106507053657$$

$$t := [4,\ 10,\ 8,\ 0,\ 0,\ 5,\ 5,\ 9,\ 1,\ 1,\ 4]$$

$$t := 4+10\,x+8\,x^2+5\,x^5+5\,x^6+9\,x^7+x^8+x^9+4\,x^{10}$$

$$t := -1+5\,x-4\,x^2+4\,x^3$$

$$t := 3\,x^3-3$$

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

$$\left[x^2+x+1,\ x^2+5\,x+3\right]$$

```
<-- exit PartialFactorSplit (now at top level) = [x^2+
x+1, x^2+5*x+3]}
```

$$\left[x^2+x+1,\ x^2+5\,x+3\right] \tag{12.5.17}$$

```
> expand((x^2+x+1)*(x^2+5*x+3)) mod 11;
```

$$x^4-5\,x^3-2\,x^2-3\,x+3 \tag{12.5.18}$$

▶ 13. Az AKS teszt

▶ 14. A szita módszerek alapjai