Bevezetés a matematikába

Járai Antal

Ezek a programok csak szemléltetésre szolgálnak.

1. Halmazok

2. Természetes számok

3. A számfogalom bővítése

4. Véges halmazok

5. Végtelen halmazok

6. Számelmélet

6.1. Oszthatóság

6.1.1. Oszthatóság a természetes számok körében.

```
> restart; 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*] (6.1.1.1)

```
> divisors(60);
```

{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60} (6.1.1.2)

->*6.1.2. Feladat.*

**6.1.3. Feladat.*

**6.1.4. Feladat.*

6.1.5. Az oszthatóság tulajdonságai a természetes számok

körében.

6.1.6. Törzsszámok és prímszámok.

```
> isprime(16); isprime(17); divisors(17); nextprime(15);
  prevprime(18);
```

false

true

$\{1, 17\}$

17

17 (6.1.6.1)

->6.1.7. Feladat.

6.1.8. Feladat.

6.1.9. Feladat.

->6.1.10. Feladat.

6.1.11. Feladat.

6.1.12. Oszthatóság egységelemes integritási tartományban.

6.1.13. Az oszthatóság tulajdonságai egységelemes integritási tartományban.

6.1.14. Asszociáltak és egységek.

6.1.15. Felbonthatatlan elem és prímelem.

6.1.16. Oszthatóság az egész számok körében.

```
> divisors(-60); igcd(12,18); igcd(-12,18); ilcm(12,18); ilcm
  (-12,-18);
```

$\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$

6

6

36

36 (6.1.16.1)

6.1.17. Példa: Gauss-egészek.

```
> with(GaussInt); GInormal(2-3*I);
```

[*GIbasis*, *GIchrem*, *GIdivisor*, *GIfacpoly*, *GIfacset*, *GIfactor*, *GIfactors*, *GIgcd*, *GIgcdex*, *GIhermite*, *GIissqr*, *GIlcm*, *GImcmbine*, *GImod*, *GInearest*, *GInodiv*, *GInorm*, *GInormal*, *GIorder*, *GIphi*, *GIprime*, *GIquadres*, *GIquo*, *GIrem*, *GIroots*, *GIsieve*, *GIsmith*, *GIsqrfree*,

GIsqrt, GIunitnormal]

$$3 + 2\,I \qquad (6.1.17.1)$$

6.1.18. Legnagyobb közös osztó, legkisebb közös többszörös, relativ primek.

->6.1.19. Feladat.

->6.1.20. Feladat.

->6.1.21. Feladat.

->6.1.22. Feladat.

6.1.23. Feladat.

6.1.24. Legnagyobb közös osztó, legkisebb közös többszörös az egész számok körében.

6.1.25. Bővített euklidészi algoritmus.

```
> exgcd:=proc(a::integer,b::integer) local n,x,y,r,q;
  x[0]:=1;y[0]:=0;r[0]:=a;x[1]:=0;y[1]:=1;r[1]:=b;n:=0;
  do if r[n+1]=0 then return x[n],y[n],r[n] fi;
    q[n+1]:=floor(r[n]/r[n+1]);r[n+2]:=r[n]-q[n+1]*r[n+1];
    x[n+2]:=x[n]-q[n+1]*x[n+1];y[n+2]:=y[n]-q[n+1]*y[n+1];
    n:=n+1;
  od; end;
```

```
exgcd := proc(a::integer, b::integer)
    local n, x, y, r, q;
    x[0] := 1;
    y[0] := 0;
    r[0] := a;
    x[1] := 0;
    y[1] := 1;
    r[1] := b;
    n := 0;
    do
        if r[n+1] = 0 then
            return x[n], y[n], r[n]
        end if;
        q[n+1] := floor(r[n] / r[n+1]);
        r[n+2] := r[n] - q[n+1]*r[n+1];
        x[n+2] := x[n] - q[n+1]*x[n+1];
        y[n+2] := y[n] - q[n+1]*y[n+1];
        n := n+1
```

(6.1.25.1)

```
    end do
end proc
```

```
> exgcd(12,18); exgcd(-12,-18); igcdex(12,18,'x','y'); x; y;
```

$$-1,\ 1,\ 6$$

$$-1,\ 1,\ -6$$

$$6$$

$$-1$$

$$1 \qquad (6.1.25.2)$$

6.1.26. *Megjegyzés.*

```
> exgcd:=proc(a::integer,b::integer) local x0,x1,x2,y0,y1,y2,
  r0,r1,r2,q;
  x0:=1;y0:=0;r0:=a;x1:=0;y1:=1;r1:=b;
  do if r1=0 then return x0,y0,r0 fi;
    q:=floor(r0/r1);r2:=r0-q*r1;
    x2:=x0-q*x1;y2:=y0-q*y1;
    r0:=r1;r1:=r2;x0:=x1;x1:=x2;y0:=y1;y1:=y2;
  od; end;
```

$$exgcd := \mathbf{proc}(a::integer,\ b::integer) \qquad (6.1.26.1)$$

$$\mathbf{local}\ x0,\ x1,\ x2,\ y0,\ y1,\ y2,\ r0,\ r1,\ r2,\ q;$$

$$x0 := 1;$$

$$y0 := 0;$$

$$r0 := a;$$

$$x1 := 0;$$

$$y1 := 1;$$

$$r1 := b;$$

$$\mathbf{do}$$

$$\quad \mathbf{if}\ r1 = 0\ \mathbf{then}$$

$$\quad\quad \mathbf{return}\ x0,\ y0,\ r0$$

$$\quad \mathbf{end\ if};$$

$$\quad q := \mathrm{floor}(r0 / r1);$$

$$\quad r2 := r0 - q * r1;$$

$$\quad x2 := x0 - q * x1;$$

$$\quad y2 := y0 - q * y1;$$

$$\quad r0 := r1;$$

$$\quad r1 := r2;$$

$$\quad x0 := x1;$$

$$\quad x1 := x2;$$

$$\quad y0 := y1;$$

```
        y1 := y2
    end do
end proc
```

```
> exgcd(12,18);
```

$$-1,\ 1,\ 6 \qquad (6.1.26.2)$$

6.1.27. Példa: bővített euklideszi algoritmus.

```
> exgcd(172,62);
```

$$-9,\ 25,\ 2 \qquad (6.1.27.1)$$

6.1.28. Következmény.

```
> igcd(12,18,10);
```

$$2 \qquad (6.1.28.1)$$

6.1.29. Tétel.

6.1.30. Megjegyzés.

6.1.31. A számelmélet alaptétele.

```
> ifactor(720);
```

$$(2)^4\,(3)^2\,(5) \qquad (6.1.31.1)$$

6.1.32. Feladat.

6.1.33. Feladat.

6.1.34. Feladat.

6.1.35. Feladat.

6.1.36. Feladat.

6.1.37. Feladat.

6.1.38. Feladat.

6.1.39. Feladat.

6.1.40. Feladat.

->6.1.41. Feladat.

6.1.42. Feladat: Lamé tétele.

6.1.43. Feladat.

6.1.44. Feladat.

6.1.45. Feladat: bináris lnko.

6.1.46. Euklidész tétele.

```
> P:=2; ifactor(P+1); P:=P*3; ifactor(P+1); P:=P*5; ifactor
  (P+1); P:=P*7; ifactor(P+1); P:=P*11; ifactor(P+1); P:=P*
  13; ifactor(P+1);
```

$$P := 2$$
$$(3)$$
$$P := 6$$
$$(7)$$
$$P := 30$$
$$(31)$$
$$P := 210$$
$$(211)$$
$$P := 2310$$
$$(2311)$$
$$P := 30030$$
$$(59)\,(509) \qquad (6.1.46.1)$$

6.1.47. Megjegyzés.

```
> ifactor(P+2); ifactor(P+3); ifactor(P+4); ifactor(P+5);
  ifactor(P+6); ifactor(P+7);
```

$$(2)^4\,(1877)$$
$$(3)^2\,(47)\,(71)$$
$$(2)\,(15017)$$
$$(5)\,(6007)$$
$$(2)^2\,(3)\,(2503)$$
$$(7)^2\,(613) \qquad (6.1.47.1)$$

6.1.48. Megjegyzés.

```
> N:=6; for n to N do s:=0: for i from 2 to 10^n do if
  isprime(i) then s:=s+1 fi; od; s,10^n/ln(10.^n); od;
```

$$N := 6$$
$$s := 0$$
$$4,\ 4.342944819$$
$$s := 0$$
$$25,\ 21.71472410$$
$$s := 0$$

168, 144.7648273

$s := 0$

1229, 1085.736205

$s := 0$

9592, 8685.889642

$s := 0$

78498, 72382.41364 (6.1.48.1)

```
> N:=25;for n to N do n,pi(10^n),10^n/ln(10.^n) od;
```

$N := 25$

1, 4, 4.342944819

2, 25, 21.71472410

3, 168, 144.7648273

4, 1229, 1085.736205

5, 9592, 8685.889642

6, 78498, 72382.41364

7, 664579, $6.204206885\ 10^{5}$

8, 5761455, $5.428681025\ 10^{6}$

9, 50847534, $4.825494243\ 10^{7}$

10, 455052511, $4.342944819\ 10^{8}$

11, 4118054813, $3.948131654\ 10^{9}$

12, 37607912018, $3.619120682\ 10^{10}$

13, 346065536839, $3.340726784\ 10^{11}$

14, 3204941750802, $3.102103442\ 10^{12}$

15, 29844570422669, $2.895296546\ 10^{13}$

16, 279238341033925, $2.714340512\ 10^{14}$

17, 2623557157654233, $2.554673423\ 10^{15}$

18, 24739954287740860, $2.412747122\ 10^{16}$

19, 234057667276344607, $2.285760431\ 10^{17}$

20, 2220819602560918840, $2.171472410\ 10^{18}$

21, 21127269486018731928, $2.068068962\ 10^{19}$

```
Warning,  computation interrupted
```

6.1.49. Kanonikus alak.

```
> ifactor(-720); ifactors(-720);
```

$-(2)^4 (3)^2 (5)$

$[-1, [[2, 4], [3, 2], [5, 1]]]$ (6.1.49.1)

▶ *6.1.50. Következmény.*

▶ *6.1.51. Következmény.*

▶ *6.1.52. Következmény.*

▶ *6.1.53. Következmény.*

▶ *6.1.54. Megjegyzés.*

▼ *6.1.55. Erathoszthenész szitája.*

```
> N:=1000; B:=Array(1..N,1);

  sieve:=proc() local p,i; global N,B; B[1]:=0; p:=1;
  do while B[p]=0 do p:=p+1; od; if p^2>N then return fi;
    i:=p^2; while i<=N do B[i]:=0; i:=i+p; od; p:=p+1;
  od; end;

  sieve(); ArrayElems(B);
```

$$N := 1000$$

$$B := \begin{bmatrix} 1 \text{ .. } 1000 \text{ Array} \\ \text{Data Type: anything} \\ \text{Storage: rectangular} \\ \text{Order: Fortran\_order} \end{bmatrix}$$

```
sieve := proc()
    local p, i;
    global N, B;
    B[1] := 0;
    p := 1;
    do
        while B[p] = 0 do
            p := p + 1
        end do;
        if N < p^2 then
            return
        end if;
        i := p^2;
        while i <= N do
            B[i] := 0;
            i := i + p
        end do;
```

```
        p := p + 1
    end do
end proc
```

$$\{2 = 1, 3 = 1, 7 = 1, 11 = 1, 5 = 1, 13 = 1, 19 = 1, 23 = 1, 29 = 1, \quad (6.1.55.1)$$
$$31 = 1, 37 = 1, 41 = 1, 43 = 1, 47 = 1, 53 = 1, 59 = 1, 61 = 1,$$
$$67 = 1, 71 = 1, 73 = 1, 79 = 1, 83 = 1, 89 = 1, 97 = 1, 101 = 1,$$
$$103 = 1, 107 = 1, 109 = 1, 113 = 1, 127 = 1, 131 = 1, 137 = 1,$$
$$139 = 1, 149 = 1, 151 = 1, 157 = 1, 163 = 1, 167 = 1, 173 = 1,$$
$$179 = 1, 181 = 1, 191 = 1, 193 = 1, 197 = 1, 199 = 1, 211 = 1,$$
$$223 = 1, 227 = 1, 233 = 1, 239 = 1, 241 = 1, 251 = 1, 257 = 1,$$
$$263 = 1, 269 = 1, 271 = 1, 17 = 1, 277 = 1, 283 = 1, 293 = 1,$$
$$307 = 1, 311 = 1, 313 = 1, 317 = 1, 331 = 1, 337 = 1, 347 = 1,$$
$$349 = 1, 353 = 1, 359 = 1, 367 = 1, 373 = 1, 379 = 1, 383 = 1,$$
$$389 = 1, 397 = 1, 401 = 1, 409 = 1, 419 = 1, 421 = 1, 431 = 1,$$
$$433 = 1, 439 = 1, 443 = 1, 449 = 1, 457 = 1, 461 = 1, 463 = 1,$$
$$467 = 1, 479 = 1, 487 = 1, 491 = 1, 499 = 1, 503 = 1, 509 = 1,$$
$$521 = 1, 523 = 1, 541 = 1, 547 = 1, 557 = 1, 563 = 1, 569 = 1,$$
$$571 = 1, 577 = 1, 587 = 1, 593 = 1, 599 = 1, 601 = 1, 281 = 1,$$
$$229 = 1, 607 = 1, 617 = 1, 619 = 1, 631 = 1, 641 = 1, 643 = 1,$$
$$653 = 1, 659 = 1, 661 = 1, 673 = 1, 677 = 1, 683 = 1, 691 = 1,$$
$$701 = 1, 709 = 1, 719 = 1, 727 = 1, 733 = 1, 739 = 1, 743 = 1,$$
$$751 = 1, 757 = 1, 761 = 1, 769 = 1, 773 = 1, 787 = 1, 797 = 1,$$
$$809 = 1, 811 = 1, 821 = 1, 823 = 1, 827 = 1, 829 = 1, 839 = 1,$$
$$853 = 1, 857 = 1, 859 = 1, 863 = 1, 877 = 1, 881 = 1, 883 = 1,$$
$$887 = 1, 907 = 1, 911 = 1, 919 = 1, 929 = 1, 937 = 1, 941 = 1,$$
$$947 = 1, 953 = 1, 967 = 1, 613 = 1, 647 = 1, 971 = 1, 983 = 1,$$
$$991 = 1, 997 = 1, 977 = 1\}$$

▼ ***->6.1.56. Feladat.***

▼ ***6.1.57. Feladat.***

▶ ***->6.1.58. Feladat.***

▼ ***->6.1.59. Feladat.***

▶ ***->6.1.60. Feladat.***

▶ ***->6.1.61. Feladat.***

▶ ***6.1.62. Feladat.***

▼ ***6.1.63. Feladat.***

▼ ***6.1.64. Feladat.***

▶ *6.1.65. Feladat.*
▼ *6.1.66. Feladat.*
▶ *6.1.67. Feladat.*
▶ *6.1.68. Feladat.*
▼ *6.1.69. Feladat.*
▶ *6.1.70. Feladat.*
▶ *6.1.71. Feladat.*
▶ *6.1.72. Feladat.*
▶ *6.1.73. Feladat.*
▶ *6.1.74. Feladat.*
▼ *6.1.75. Feladat.*
▶ *6.1.76. További feladatok megoldásokkal.*
▶ *6.1.77. További feladatok.*

▼ 6.2. Kongruenciák

```
> restart;
```

▼ *6.2.1. Kongruenciák.*

▼ *->6.2.2. Feladat.*

▼ *6.2.3. Maradékosztályok.*

```
> 13 mod 7; modp(13,7); `mod`(13,7); mods(13,7); `mod`:=mods;
  13 mod 7;
```

$$6$$
$$6$$
$$6$$
$$-1$$
$$mod := mods$$
$$-1 \qquad (6.2.3.1)$$

```
> `mod`:=modp; [2,10] mod 8; [2,8] mod 8; [8,1,10,19,4,29,
  -10,7] mod 8;
  mods(%,8); [1,19,29,7] mod 8;
```

$$mod := modp$$
$$[2, 2]$$
$$[2, 0]$$

$$[0, 1, 2, 3, 4, 5, 6, 7]$$
$$[0, 1, 2, 3, 4, -3, -2, -1]$$
$$[1, 3, 5, 7] \qquad (6.2.3.2)$$

6.2.4. Komplemens ábrázolás.

6.2.5. Tétel.

```
> 1/3 mod 8; 1/2 mod 8; 1/1 mod 5; 1/2 mod 5; 1/3 mod 5; 1/4
  mod 5;
```

$$3$$

```
Error, the modular inverse does not exist
```

$$1$$
$$3$$
$$2$$
$$4 \qquad (6.2.5.1)$$

->6.2.6. Feladat.

```
> 1/5 mod 17; 9*11 mod 17; (15+10)/(3+5) mod 17; mul(i,i=1.
  .16) mod 17;
```

$$7$$
$$14$$
$$1$$
$$16 \qquad (6.2.6.1)$$

6.2.7. Feladat.

6.2.8. Diszkrét logaritmus probléma.

*6.2.9. Gyors hatványozás.

```
> fastexp:=proc(g,n::posint,mult::procedure) local j,x,b;
  b:=convert(n,base,2); x:=g;
  for j from nops(b)-1 to 1 by -1 do
    x:=mult(x,x); if b[j]=1 then x:=mult(x,g) fi;
  od; x; end;
```

$$fastexp := \mathbf{proc}(g, n::posint, mult::procedure) \qquad (6.2.9.1)$$
$$\quad \mathbf{local}\ j, x, b;$$
$$\quad b := convert(n, base, 2);$$
$$\quad x := g;$$
$$\quad \mathbf{for}\ j\ \mathbf{from}\ nops(b) - 1\ \mathbf{by}\ -1\ \mathbf{to}\ 1\ \mathbf{do}$$
$$\qquad x := mult(x, x);$$

```
        if b[j] = 1 then
            x := mult(x, g)
        end if
    end do;
    x
end proc
```

```
> fastexp(2,11,(x,y)->x*y);
```

$$2048 \qquad (6.2.9.2)$$

6.2.10. Diffie-Hellmann-Merkle-kulcscsere.

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

$$[GIgcd, bigomega, cfrac, cfracpol, cyclotomic, divisors, factorEQ, factorset, fermat, imagunit, index, integral\_basis, invcfrac, invphi, issqrfree, jacobi, kronecker, \lambda, legendre, mcombine, mersenne, migcdex, minkowski, mipolys, mlog, mobius, mroot, msqrt, nearestp, nthconver, nthdenom, nthnumer, nthpow, order, pdexpand, \phi, \pi, pprimroot, primroot, quadres, rootsunity, safeprime, \sigma, sq2factor, sum2sqr, \tau, thue] \qquad (6.2.10.1)$$

```
> q:=safeprime
  (435987601265432789056687987654123456578909876542 60567);

  p:=(q-1)/2; isprime(p); g:=3;
```

$$q := 435987601265432789056687987654123456578909876542\backslash 60567$$

$$p := 217993800632716394528343993827061728289454938271\backslash 30283$$

$$true$$

$$g := 3 \qquad (6.2.10.2)$$

```
> T:=convert(floor(time()*1000)+3141592 mod (111^3),base,111)
  ;while nops(T)<3 do T:=[op(TT),0] od;
```

$$T := [105, 109, 32] \qquad (6.2.10.3)$$

```
> N:=3; T:=vector(N+3,T); n:=0; m:=0; c:="a";
```

$$N := 3$$

$$T := [105 \quad 109 \quad 32 \quad T_4 \quad T_5 \quad T_6]$$

$$n := 0$$

$$m := 0$$
$$c := \text{"a"} \tag{6.2.10.4}$$

```
> nexttime:=proc() local i,S; global T,TT,N,m,n,c;
    S:="0123456789-abcdefghijklmnopqrstuvwxyz";
    m:=1+(T[3+n] mod 3);
    i:=T[m] mod 37;
    if S[i+1]=c then
      n:=n+1; T[3+n]:=floor(time()*1000) mod 3*37*16; T[m]:=T
   [3+n]
    fi;
    if n=N then print(T); return fi;
    m:=1+(T[3+n] mod 3);
    i:=T[m] mod 37;
    print(T,S[i+1]);
    c:=readline(terminal);
    while true do i:=0 od;
  end;
```

```
nexttime := proc()
    local i, S;
    global T, TT, N, m, n, c;
    S := "0123456789-abcdefghijklmnopqrstuvwxyz";
    m := 1 + (mod(T[3 + n], 3));
    i := mod(T[m], 37);
    if S[i + 1] = c then
        n := n + 1;
        T[3 + n] := mod(floor(1000 * time()), 1776);
        T[m] := T[3 + n]
    end if;
    if n = N then
        print(T);
        return
    end if;
    m := 1 + (mod(T[3 + n], 3));
    i := mod(T[m], 37);
    print(T, S[i + 1]);
    c := readline(terminal);
    do
        i := 0
    end do
end proc
```

(6.2.10.5)

```
> nexttime();
```

(6.2.10.6)

$$[1271 \quad 110 \quad 1245 \quad 20 \quad 1245 \quad 1271] \tag{6.2.10.6}$$

```
>
> convert(T,list); %[4..N+3]; map(t->t mod 16,%);
  x:=add(%[i]*16^(i-1),i=1..nops(%)); X:=g&^x mod q;
```

$$[105, 109, 32, T_4, T_5, T_6]$$
$$[T_4, T_5, T_6]$$
$$[T_4, T_5, T_6]$$
$$x := T_4 + 16\,T_5 + 256\,T_6$$
$$X := 3\ \&^{\wedge}\ (T_4 + 16\,T_5 + 256\,T_6) \tag{6.2.10.7}$$

```
> x:=768134069215447386542317506798909232101649164367 39; X:=
  g&^x mod q;
  y:=476143609917846513247659876667890987665423334325 43; Y:=
  g&^y mod q;
```

$$x := 768134069215447386542317506798909232101649164367 39$$
$$X := 265122515504214772937605315507315212932802752207\ 44368$$
$$y := 476143609917846513247659876667890987665423334325 43$$
$$Y := 262064444478543486478696215091708772691198270 66\ 03926 \tag{6.2.10.8}$$

```
> X&^y mod q; Y&^x mod q;
```

$$2498399197399051233713151981063883280814367565528746$$
$$2498399197399051233713151981063883280814367565528746 \tag{6.2.10.9}$$

6.2.11. Feladat.

```
> [[3^i mod 17,i]$i=1..16]; sort(map(x->[x[1] mod 17,x[2]],%)
  ,(x,y)->x[1]<y[1]);
```

$$[[3, 1], [9, 2], [27, 3], [81, 4], [243, 5], [729, 6], [2187, 7], [6561, 8], [19683, 9], [59049, 10], [177147, 11], [531441, 12], [1594323, 13], [4782969, 14], [14348907, 15], [43046721, 16]]$$
$$[[1, 16], [2, 14], [3, 1], [4, 12], [5, 5], [6, 15], [7, 11], [8, 10], [9, 2], [10, 3], [11, 7], [12, 13], [13, 4], [14, 9], [15, 6], [16, 8]] \tag{6.2.11.1}$$

6.2.12. Az Euler-féle φ függvény.

```
> phi(1); phi(2); phi(3); phi(4); phi(5); phi(6); phi(7); phi
```

```
(8);
```

$$\begin{matrix}1\\1\\2\\2\\4\\2\\6\\4\end{matrix} \qquad (6.2.12.1)$$

▶ *6.2.13. Lemma.*

▶ *6.2.14. Euler–Fermat tétel.*

▶ *6.2.15. Következmény: Fermat-tétel.*

▶ *6.2.16. Lineáris kongruencia megoldása.*

▼ *6.2.17. Példa.*

```
> x:='x'; msolve(172*x=6,62);
```

$$x := x$$
$$\{x = 4\}, \{x = 35\} \qquad (6.2.17.1)$$

▼ *->6.2.18. Feladat.*

▼ *->6.2.19. Feladat.*

▼ *6.2.20. Feladat.*

▶ *6.2.21. Feladat.*

▶ *6.2.22. Feladat.*

▼ *6.2.23. Lineáris kongruenciarendszer megoldása.*

```
> y:='y'; msolve({3*x-4*y=1,7*x+y=2},19);
```

$$y := y$$
$$\{y = 11, x = 15\} \qquad (6.2.23.1)$$

▼ *->6.2.24. Feladat.*

▼ *6.2.25. Diofantikus problémák.*

```
> isolve(x^2+y^2=z^2);
```

$$\left\{x = \frac{\_Z3\left(-\_Z1^2 + \_Z2^2\right)}{igcd\left(-\_Z1^2 + \_Z2^2, \_Z1^2 + \_Z2^2, -2\,\_Z1\,\_Z2\right)}, \right. \qquad (6.2.25.1)$$

$$z = \frac{\_Z3\left(\_Z1^2 + \_Z2^2\right)}{igcd\left(-\_Z1^2 + \_Z2^2,\ \_Z1^2 + \_Z2^2,\ -2\ \_Z1\ \_Z2\right)},$$

$$y = -\frac{2\ \_Z3\ \_Z1\ \_Z2}{igcd\left(-\_Z1^2 + \_Z2^2,\ \_Z1^2 + \_Z2^2,\ -2\ \_Z1\ \_Z2\right)}\Bigg\}$$

```
> isolve(x^3+y^3=z^3);
```

6.2.26. Feladat.

**6.2.27. Feladat.*

6.2.28. Kínai maradéktétel.

```
> chrem([1,2,2],[2,3,7]);
```

$$23 \qquad (6.2.28.1)$$

6.2.29. Megjegyzés.

6.2.30. Példa.

6.2.31. Feladat.

->6.2.32. Feladat.

```
> 42&^600 mod 13;
```

$$1 \qquad (6.2.32.1)$$

->6.2.33. Feladat.

->6.2.34. Feladat.

->6.2.35. Feladat.

6.2.36. Feladat.

6.2.37. Feladat.

6.2.38. Feladat.

6.2.39. Az RSA eljárás.

```
> p:=safeprime
  (156345678881425617888676566155526134298764532134566543212345678877209127512109876123212233332123343412343212334445432123432094872546784546778885981234236 5); log[2.](p);
  q:=safeprime
  (298415244751590016765614534678909876512342543214564909987676267881825143256789099872365142341542323965878747789933777220049883766678827671563638883776266777288 88); log[2.](q);
  n:=p*q;

  e:=28763541324536789099876534321234098876354231 25;
```

```
igcdex(e,(p-1)*(q-1),'d'); d; d*e mod (p-1)*(q-1);
```

$p :=$

1563456788814256178886765661555261342987645321345\
6654321234567887720912751210987612321223333212 3\
3434123432123344454321234320948725467845467788 8\
59812363179

508.8997379

$q :=$

2984152447515900167656145346789098765123425432 14\
5649099876762678818251432567890998723651423415 42\
3239658787477899337772200498837666788276715636 3\
888377626677803527

533.0858164

$n :=$

4665593402925412424182224876400472112892773327 81\
3449453351019945622674603742441009009573960222 11\
6531745940349543348422686605488315168714111637 1\
8915251508806678428043789500872863510643356826 92\
0817709316133372668676678694865105558712822167 10\
6575626216328755384345969767781305821261864036 6\
396927023748196137493113233 3

$e :=$ 28763541324536789099876534321234098876354231 25

1

–

1957129622478286376611572572501533489779239931 49\
7112164198867845520671251361820628354584152329 64\
0064971617786694234640440682214932084123273568 6\
3857893715807237232345759942482997119965921948 96\
5140136400026278153423494508152965571832240980 89\
5842023669648156871374368010120465251673272075 3\
179856008073268914420048383 1

1 (6.2.39.1)

```
> M:="Mint víz alatti, elmerült harangok
  hintáznak-e hajnalonként ágyadnál
  a tizennyolc éves iskolások
  kiket felakasztattál";

  convert(M,'bytes');
```

```
m:=sum(%[i]*256^(i-1),i=1..nops(%));

c:=m&^e mod n;
```

M:= "Mint víz alatti, elmerült harangok

hintáznak-e hajnalonként ágyadnál

a tizennyolc éves iskolások

kiket felakasztattál"

[77, 105, 110, 116, 32, 118, 195, 173, 122, 32, 97, 108, 97, 116, 116, 105, 44, 32, 101, 108, 109, 101, 114, 195, 188, 108, 116, 32, 104, 97, 114, 97, 110, 103, 111, 107, 10, 10, 104, 105, 110, 116, 195, 161, 122, 110, 97, 107, 45, 101, 32, 104, 97, 106, 110, 97, 108, 111, 110, 107, 195, 169, 110, 116, 32, 195, 161, 103, 121, 97, 100, 110, 195, 161, 108, 10, 10, 97, 32, 116, 105, 122, 101, 110, 110, 121, 111, 108, 99, 32, 195, 169, 118, 101, 115, 32, 105, 115, 107, 111, 108, 195, 161, 115, 111, 107, 10, 10, 107, 105, 107, 101, 116, 32, 102, 101, 108, 97, 107, 97, 115, 122, 116, 97, 116, 116, 195, 161, 108]

m:=

19528680046240611054074111890960392345823897844641211\
41211123261273221169061744378240835537054015631 3\
94774815478298280810507336262895468621974609594\
43059138312535255019845996711281074221991389403 1\
17085548216837925027178277690153125688091048976 5\
90489549780975327596948774377394853498167317079\
96530126168857916556188 93

c:= (6.2.39.2)

77524849422698264675685168880311738340989858492 5\
75204736838157266495122850646492987180503005220 4\
51702860034067164181214844639064979047472769226\
26874209747246992010527460796379302928687354533 5\
75986040206493447311162190731376406766176088155 9\
78629408505121905984327641729117414833323813226\
58648841543244889737553218

```
> c&^d mod n; convert(%,base,256); convert(%,'bytes');
```

19528680046240611054074111890960392345823897844641211\

```
123261273221169061744378240835537054015631394 77\
48154782982808105073362628954686219746095944 3059\
13831253525501984599671128107422199138940311 7085\
54821683792502717827769015312568809104897659 048\
95497809753275969487743773948534981673170799 6530\
12616885791655618893
```

```
[77, 105, 110, 116, 32, 118, 195, 173, 122, 32, 97, 108, 97, 116, 116,
   105, 44, 32, 101, 108, 109, 101, 114, 195, 188, 108, 116, 32, 104,
   97, 114, 97, 110, 103, 111, 107, 10, 10, 104, 105, 110, 116, 195,
   161, 122, 110, 97, 107, 45, 101, 32, 104, 97, 106, 110, 97, 108,
   111, 110, 107, 195, 169, 110, 116, 32, 195, 161, 103, 121, 97,
   100, 110, 195, 161, 108, 10, 10, 97, 32, 116, 105, 122, 101, 110,
   110, 121, 111, 108, 99, 32, 195, 169, 118, 101, 115, 32, 105, 115,
   107, 111, 108, 195, 161, 115, 111, 107, 10, 10, 107, 105, 107,
   101, 116, 32, 102, 101, 108, 97, 107, 97, 115, 122, 116, 97, 116,
   116, 195, 161, 108]
```

"Mint víz alatti, elmerült harangok (6.2.39.3)

hintáznak–e hajnalonként ágyadnál

a tizennyolc éves iskolások

kiket felakasztattál"

▶ *6.2.40. Feladat.*

▼ **6.2.41. A Miller–Rabin–féle valószínűségi teszt.*

```
> millerrabin:=proc(n::posint,a::posint) local j,k,q,b;
  if n=2 or n=3 or n=5 or n=7 then return true fi;
  if n<9 then return false fi;
  b:=a mod n; if b=0 or b=1 then return FAIL fi;
  k:=0; q:=n-1; while type(q,even) do k:=k+1; q:=q/2; od;
  b:=b&^q mod n; j:=0; if b=1 then return true fi;
  while j<k do if b=n-1 then return true fi; b:=b^2 mod n;
  j:=j+1; od;
  false; end;
```

millerrabin := **proc**(*n*::*posint*, *a*::*posint*) (6.2.41.1)

local *j*, *k*, *q*, *b*;

if $n = 2$ **or** $n = 3$ **or** $n = 5$ **or** $n = 7$ **then**

```
        return true
    end if;
    if n < 9 then
        return false
    end if;
    b := mod(a, n);
    if b = 0 or b = 1 then
        return FAIL
    end if;
    k := 0;
    q := n - 1;
    while type(q, even) do
        k := k + 1;
        q := 1 / 2 * q
    end do;
    b := mod(b &^ q, n);
    j := 0;
    if b = 1 then
        return true
    end if;
    while j < k do
        if b = n - 1 then
            return true
        end if;
        b := mod(b^2, n);
        j := j + 1
    end do;
    false
end proc
```

```
> millerrabin(9,2); millerrabin(11,2);
```

$$false$$

$$true \tag{6.2.41.2}$$

```
> for n do if millerrabin(n,2)<>isprime(n) then print(n) fi;
  od;
```

2047

3277

4033

4681

```
                                8321
                               15841
                               29341
                               42799
                               49141
                               52633
                               65281
                               74665
                               80581
                               85489
                               88357
                               90751
Warning,  computation interrupted
> for n do if millerrabin(n,2)<>isprime(n) and millerrabin(n,
  3)<> isprime(n) then print(n) fi; od;
                             1373653
                             1530787
                             1987021
                             2284453
                             3116107
Warning,  computation interrupted
> n;
```

*6.2.42. Digital Signature Standard.

```
> StringTools[Hash](M); h:=convert(%,decimal,hex);

                    "6848b65ee408b7eccb7521a7f2588895"
```

$$h := 138617255852014021523097242608084748437 \qquad (6.2.42.1)$$

```
> q:=nextprime(convert
  ("97654376ad4efcbe43598123daf56c7b386acbda",decimal,hex));

  for i from convert
  ("ffffffffeeeeeeeedddddddcccccccbbbbbbbbaaaaaaaa9999999988
  88888877777777666666665555555544444444333333332222222211111
  1100000000ffffffffeeeeeeeedddddddcccccccbbbbbbbbaaaaaaaa99
  99999988888888777777776666666655555555",decimal,hex) do
    p:=i*q+1; if isprime(p) then break fi; od: p;

  log[2.](q); log[2.](p);

  a:=2; g:=a&^((p-1)/q) mod p;
```

```
x:=432765098765765432112456567309098091230938 75;

y:=g&^x mod p;
```

$$q := 864315858566294654370934705973723661658370001937$$
$$106313578143555908193656524587783721879547904624578 33\$$
$$130069413327928644326946425031737102999365056 40\$$
$$271962547356723295866698603992186811777359562971\$$
$$254163849217237516060097946895282298434278542582\$$
$$250436151580275599006065350711272677355075705 52\$$
$$985057458719816664605555247261677413470590270624\$$
$$190328222921189037$$

$$159.2421791$$

$$1023.242179$$

$$a := 2$$

$$g := 757750019886573043307612954520709662085091310554\$$
$$514197301205855784338691968693512594733942988371\$$
$$954911402859211642463188487606860219250663414 14\$$
$$147740924796514244633388296050188360754537007695\$$
$$324727487262333108782394914497524065099285706905\$$
$$884886671476441207585293706805965362112752699 63\$$
$$2147115415465005025014$$

$$x := 432765098765765432112456567309098091230938 75$$

$$y := 327308886371736794899881276576203313917926736196\$$
$$875145942776348076911935071613009133484100855648\$$
$$241063626188651147340187263200362093402622935 93\$$
$$239339209741693845114667218485058840139845712324\$$
$$416996800406457483697570302049615890139408757511\$$
$$818780279319140308745369583476548875855538393 89\$$
$$043270025023387055939 1 \qquad (6.2.42.2)$$

```
> k:=980456321127654327890654327 8;

r:=(g&^k mod p) mod q;

s:=(h+x*r)/k mod q;
```

$$k := 980456321127654327890654327 8$$

$$r := 323275151680357711465404903685369497578574921 53$$

$s := 462328210683602561450626062330893104370385503881$ (6.2.42.3)

```
> w:=1/s mod q;

  u1:=h*w mod q;

  u2:=r*w mod q;

  v:=(g&^u1*y&^u2 mod p) mod q;
```

$w := 588921630297228603369981871409526163667934121061$

$u1 := 193709789008006978900495659899438140098738778246$

$u2 := 144419026006865696101856654631833819951577769549$

$v := 323275151680357711465404903685369497578574921 53$ (6.2.42.4)

▼ *6.2.43. Feladat: álprímek.*

▼ *6.2.44. Feladat: Carmichel-számok.*

▶ *->6.2.45. Feladat.*

▶ *6.2.46. Feladat: pitagoraszi számhármasok.*

▶ *6.2.47. Feladat.*

▶ *6.2.48. Feladat.*

▶ *6.2.49. Feladat.*

▶ *6.2.50. Feladat.*

▶ *6.2.51. További feladatok megoldásokkal.*

▶ *6.2.52. További feladatok.*

▼ 6.3. Számelméleti függvények

```
>  restart: with(numtheory);
```

[*GIgcd*, *bigomega*, *cfrac*, *cfracpol*, *cyclotomic*, *divisors*, *factorEQ*, *factorset*, (6.3.1)
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]

▶ *6.3.1. Számelméleti függvények.*

▶ *6.3.2. Tétel.*

▼ *6.3.3. Példák.*

```
> divisors(60); tau(60); sigma[0](60); sigma(60);
  sigma[1](60); sigma[2](60);
```

$$\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$
$$12$$
$$12$$
$$168$$
$$168$$
$$5460 \qquad (6.3.3.1)$$

```
> mobius(1); mobius(2); mobius(4); mobius(20); mobius(21);
```

$$1$$
$$-1$$
$$0$$
$$0$$
$$1 \qquad (6.3.3.2)$$

```
> kappa:=proc(n::posint) nops(ifactors(n)[2]) end; kappa(1);
  kappa(2); kappa(3); kappa(4); kappa(5); kappa(6);
```

$$\kappa := \mathbf{proc}(n::posint)\ nops(ifactors(n)[2])\ \mathbf{end\ proc}$$
$$0$$
$$1$$
$$1$$
$$1$$
$$1$$
$$2 \qquad (6.3.3.3)$$

```
> nu:=proc(n::posint) nops(factorset(n)) end; factorset(60);
  nu(60);
```

$$\nu := \mathbf{proc}(n::posint)\ nops(numtheory:-factorset(n))\ \mathbf{end\ proc}$$
$$\{2, 3, 5\}$$
$$3 \qquad (6.3.3.4)$$

6.3.4. Tétel.

```
> phi(60); invphi(16);
```

$$16$$
$$[17, 32, 34, 40, 48, 60] \qquad (6.3.4.1)$$

6.3.5. Példa.

```
> phi(5500);
```

$$2000 \qquad (6.3.5.1)$$

▼ *->6.3.6. Feladat.*
▼ *->6.3.7. Feladat.*
▼ *->6.3.8. Feladat.*
▼ *->6.3.9. Feladat.*
▶ *6.3.10. Feladat.*
▶ *6.3.11. Feladat.*
▶ *6.3.12. Feladat.*
▼ *->6.3.13. Feladat.*
▼ *->6.3.14. Feladat.*
▼ *->6.3.15. Feladat.*
▶ *6.3.16. Feladat.*
▶ *6.3.17. Feladat.*
▼ *6.3.18. Feladat.*
▼ *6.3.19. Feladat.*
▶ **6.3.20. Konvolúció.*
▶ **6.3.21. Tétel.*
▶ **6.3.22. Összegzési függvény.*
▶ **6.3.23 Möbius-féle inverziós formula.*
▶ **6.3.24. Példa.*
▶ **6.3.25. Tétel.*
▶ **6.3.26. Tétel.*
▶ *6.3.27. Feladat.*
▶ **6.3.28. Feladat.*
▶ *6.3.29. További feladatok megoldásokkal.*
▶ *6.3.30. További feladatok.*

▼ 6.4. Lánctörtek

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

[*GIgcd*, *bigomega*, *cfrac*, *cfracpol*, *cyclotomic*, *divisors*, *factorEQ*, *factorset*, (6.4.1)
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*]

*6.4.1. Lánctörtek.

```
> nextcfrac:=proc(L::list) local a,q,j; j:=nops(L);
  if j=0 then return FAIL fi; a:=L[j];
  if type(a,integer) then return(L) fi;
  q:=floor(a); a:=a-q; a:=simplify(expand(1/a)); [op(L[1..j
  -1]),q,a]; end;

  [19/7]; nextcfrac(%); nextcfrac(%); nextcfrac(%); nextcfrac
  (%);

  cfrac(19/7); cfrac(19/7,quotients);
```

```
nextcfrac := proc(L::list)
    local a, q, j;
    j := nops(L);
    if j = 0 then
        return FAIL
    end if;
    a := L[j];
    if type(a, integer) then
        return L
    end if;
    q := floor(a);
    a := a - q;
    a := simplify(expand(1 / a));
    [op(L[1 .. j - 1]), q, a]
end proc
```

$$\left[\frac{19}{7}\right]$$

$$\left[2, \frac{7}{5}\right]$$

$$\left[2, 1, \frac{5}{2}\right]$$

$$[2, 1, 2, 2]$$

$$[2, 1, 2, 2]$$

$$2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2}}}$$

$$[2, 1, 2, 2] \tag{6.4.1.1}$$

*6.4.2. Példák.

```
> [172/62]; nextcfrac(%); nextcfrac(%); nextcfrac(%);
  nextcfrac(%);

  cfrac(172/62);
```

$$\left[\frac{86}{31}\right]$$

$$\left[2, \frac{31}{24}\right]$$

$$\left[2, 1, \frac{24}{7}\right]$$

$$\left[2, 1, 3, \frac{7}{3}\right]$$

$$[2, 1, 3, 2, 3]$$

$$2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{3}}}} \tag{6.4.2.1}$$

```
> a:=(sqrt(5)+1)/2; nextcfrac([a]); nextcfrac(%); nextcfrac
  (%);

  cfrac(a); cfrac(a,periodic); cfrac(a,periodic,quotients);
```

$$a := \frac{1}{2}\sqrt{5} + \frac{1}{2}$$

$$\left[1, \frac{2}{\sqrt{5} - 1}\right]$$

$$\left[1, 1, -\frac{\sqrt{5} - 1}{-3 + \sqrt{5}}\right]$$

$$\left[1, 1, 1, -\frac{1}{2}\ \frac{-3 + \sqrt{5}}{\sqrt{5} - 2}\right]$$

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{

$$\left(\frac{1}{3+\frac{1}{1+\frac{1}{1+\frac{1}{10+\frac{1}{1+\frac{1}{1+\frac{1}{3+\frac{1}{5+\frac{1}{3+\frac{1}{1+\frac{1}{1+\frac{1}{10+\ldots}}}}}}}}}}}}\right)$$

$$\sqrt{31}$$

$$[[5],[1, 66, 2, 2, 5, 10, 1, 1, 2, 2, 3, 2, 1, 1, 1, 268, 1, 1, 1, 2, 3, 2, 2, 1, 1, 10, 5, 2, 2, 66, 1, 9, 1, 3, 1, 1, 1, 8, 1, 1, 1, 3, 1, 9]]$$

$$\frac{3}{5}+\sqrt{29} \qquad (6.4.2.3)$$

*6.4.3. Feladat.

*6.4.4. Feladat.

*6.4.5. Feladat.

*6.4.6. Feladat.

*6.4.7. Lánctörtközelítések zárt alakja.

```
> cfrac(3/5+sqrt(29)); nthconver(%,7); nthnumer(%%,7);
  nthdenom(%%%,7);
```

$$5+\cfrac{1}{1+\cfrac{1}{66+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{5+\cfrac{1}{10+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{2+\ldots}}}}}}}}}}$$

$$\frac{121840}{20357}$$

$$121840$$

$$20357 \qquad (6.4.7.1)$$

*6.4.8. Példa.

```
> cfrac(172/62); nthconver(%,4); nthnumer(%%,4); nthdenom
  (%%%,4);
```

$$2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{3}}}}$$

$$\frac{86}{31}$$

$$86$$

$$31 \qquad (6.4.8.1)$$

*6.4.9. Megjegyzés.

```
> for n from 0 do expand(1/sqrt(5)*(((1+sqrt(5))/2)^n-((1-
  sqrt(5))/2)^n)) od;
```

$$0$$

$$1$$

1
2
3
5
8
13
21
34
55
89
144
233
377
610
987
1597
2584
4181
6765
10946
17711
28657
46368
75025
121393
196418
317811
514229
832040
1346269
2178309
3524578
5702887
9227465
14930352
24157817
39088169
63245986

```
                                102334155
                                165580141
                                267914296
                                433494437
                                701408733
                               1134903170
                               1836311903
                               2971215073
                               4807526976
                               7778742049
Warning,  computation interrupted
```

▶ *6.4.10. Megjegyzés.

▶ *6.4.11. Tétel.

▼ *6.4.12. Példa.

```
> nextrangecfrac:=proc(L::list) local a,a1,a2,j,q1,q2; j:=
  nops(L);
  if j=0 then return FAIL fi; a:=L[j];
  a1:=op(1,a); a2:=op(2,a); q1:=floor(a1); q2:=floor(a2);
  if q1<>q2 then return L fi;
  [op(L[1..j-1]),q1,1/(a2-q2)..1/(a1-q1)] end;

  [314159265/10^8..314159266/10^8]; nextrangecfrac(%);
  nextrangecfrac(%); nextrangecfrac(%); nextrangecfrac(%);
  nextrangecfrac(%); nextrangecfrac(%);

  evalf(355/113);
```

```
nextrangecfrac := proc(L::list)
    local a, a1, a2, j, q1, q2;
    j := nops(L);
    if j = 0 then
        return FAIL
    end if;
    a := L[j];
    a1 := op(1, a);
    a2 := op(2, a);
    q1 := floor(a1);
    q2 := floor(a2);
    if q1 <> q2 then
```

```
        return L
    end if;
    [op(L[1..j-1]), q1, 1/(a2-q2)..1/(a1-q1)]
end proc
```

$$\left[\frac{62831853}{20000000}..\frac{157079633}{50000000}\right]$$

$$\left[3, \frac{50000000}{7079633}..\frac{20000000}{2831853}\right]$$

$$\left[3, 7, \frac{2831853}{177029}..\frac{7079633}{442569}\right]$$

$$\left[3, 7, 15, \frac{442569}{441098}..\frac{177029}{176418}\right]$$

$$\left[3, 7, 15, 1, \frac{176418}{611}..\frac{441098}{1471}\right]$$

$$\left[3, 7, 15, 1, \frac{176418}{611}..\frac{441098}{1471}\right]$$

$$\left[3, 7, 15, 1, \frac{176418}{611}..\frac{441098}{1471}\right]$$

$$3.141592920 \qquad (6.4.12.1)$$

```
> cfrac(Pi,100,quotients);
```

[3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13, 1, 4, 2, 6, 6, 99, 1, 2, 2, 6, 3, 5, 1, 1, 6, 8, 1, 7, 1, 2, 3, 7, 1, 2, 1, 1, 12, 1, 1, 1, 3, 1, 1, 8, 1, 1, 2, 1, 6, 1, 1, 5, 2, 2, 3, 1, 2, 4, 4, 16, 1, 161, 45, 1, 22, 1, 2, 2, 1, 4, 1, 2, 24, 1, 2, 1, 3, 1, 2, 1, 1, 10, 2, ...] (6.4.12.2)

▼ ***6.4.13. Intervallumaritmetika.***

▶ ****6.4.14. Feladat.***

▶ ****6.4.15. Feladat.***

▶ ****6.4.16. Feladat.***

▼ ****6.4.17. Feladat.***

▼ ****6.4.18. Feladat.***

▶ ****6.4.19. Feladat.***

▶ ****6.4.20. Feladat.***

▶ ****6.4.21. Feladat.***

▶ ****6.4.22. Feladat.***

▼ ***6.4.23. Feladat.***

▼ *6.4.24. Feladat.*
▼ *6.4.25. Feladat.*
▼ *6.4.26. Feladat.*
▼ *6.4.27. Feladat.*

▶ **6.4.28. További feladatok megoldásokkal.*
▶ **6.4.29. További feladatok.*

▶ 7. Gráfelmélet

▶ 8. Algebra

▶ 9. Kódolás

▶ 10. Algoritmusok