

Matematikai problémák vizsgálata a Maple programcsomag segítségével

Tengely Szabolcs

tengely@science.unideb.hu

<http://www.math.unideb.hu/~tengely>

Áttekintés

Maple és a gráfelmélet

Maple és lineáris algebra

Maple és az LLL-algoritmus

Index kalkulus Maple segítségével

Elliptikus görbék és a Maple

Feszítőfák keresése - Kruskal

Adott $G(V, E)$ gráf és egy $s : E \rightarrow \mathbb{R}_+$ súlyfüggvény.

Keresünk olyan feszítőfát, amelyben az élek súlya minimális.

Kruskal algoritmus: rendezzük az éleket növekvő sorrendbe a súlyok szerint, addig választunk be éleket, amíg fát nem kapunk.

Delete-reverse algoritmus: csökkenő sorrendbe rendezzük az éleket és addig törlünk, amíg összefüggő gráf marad.

Feszítőfák keresése - Kruskal

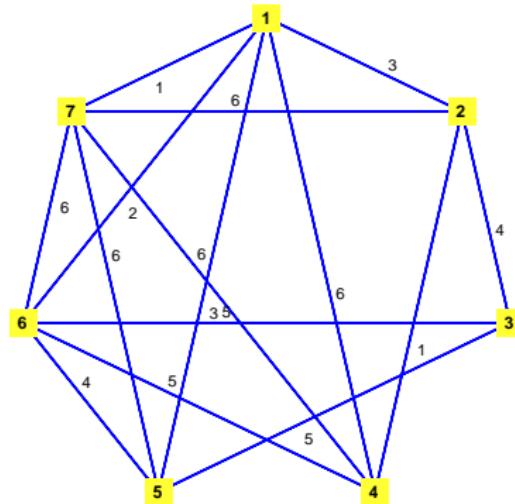
```
> FeszitoPal:=proc(G)
> local g0,f,eG,l;
> g0:=Graph(NumberVertices(G),'weighted');
> f:=(x,y)->if x[2]<y[2] then true; else false; end if;
> eG:=sort([op(Edges(G,weights))],f);
> l:=1; while not IsTree(g0) do
> if IsForest(AddEdge(g0,eG[l][1],inplace=false)) then g0:=AddEdge
> (g0,eG[l]); end if;
> l:=l+1;
> end do;
> g0;
> end proc;
FeszitoPal := proc(G)
local g0,f,eG,l;
g0 := GraphTheory:-Graph(GraphTheory:-NumberVertices(G), 'weighted');
f:=(x,y)->if x[2]<y[2] then true else false end if;
eG:=sort([op(GraphTheory:-Edges(G, weights))],f);
l:=1;
while not GraphTheory:-IsTree(g0) do
if GraphTheory:-IsForest(GraphTheory:-AddEdge(g0, eG[l][1], inplace = false)) then
g0 := GraphTheory:-AddEdge(g0, eG[l]);
end if;
l:=l+1;
end do;
g0
end proc;
```

(1)


```
> with(GraphTheory);
> with(RandomGraphs):
> Graf:=RandomGraph(7,1,connected, weights=1..6);
Graf:= Graph 1: an undirected weighted graph with 7 vertices and 15 edges
> DrawGraph(Graf);
```

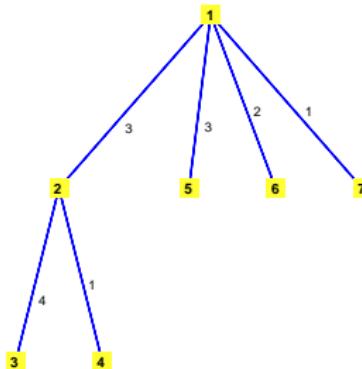
(2)

Feszítőfák keresése - Kruskal



```
> DrawGraph(FeszitoFal(Graf));
```

Feszítőfák keresése - Reverse-Delete



```

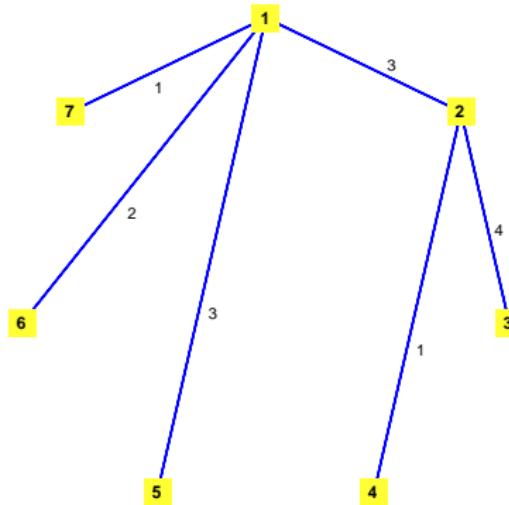
> FeszitoFa2:=proc(G)
> local f,eG,H,l; f:=(x,y)->if x[2]>y[2] then true; else false; end
> if;
> eG:=sort([op(Edges(G,weights))],f);
> H:=G; l:=1;
> while not IsTree(H) do
> if IsConnected(DeleteEdge(H,eG[l][1],inplace=false)) then
> DeleteEdge(H,eG[l]);
> l:=l+1; end do;
> H;
> end proc;
FeszitoFa2 := proc(G)
local f, eG, H, l;
f:=(x,y)->if y[2]<x[2] then true else false end if;
eG:=sort([op(GraphTheory:-Edges(G,weights))],f);
H:=G;
  
```

(3)

Feszítőfák keresése - Reverse-Delete

```
I:=1;  
while not GraphTheory:-IsTree(H) do  
    if GraphTheory:-IsConnected(GraphTheory:-DeleteEdge(H,eG[I][1],inplace  
=false)) then  
        GraphTheory:-DeleteEdge(H,eG[I])  
    end if;  
    I:=I+1  
end do;  
H  
end proc  
> DrawGraph(FeszitoFa2(Graf));
```

Feszítőfák keresése - Reverse-Delete



Sakktábla bejárása

$m \times n$ -es sakktábla bejárása

Adott $m \times n$ -es sakktábla esetén egy mezőről indulva lóugrással járjuk be a táblát úgy, hogy minden mezőt pontosan egyszer érintünk és a kiindulópontba jutunk vissza.

Gráfelméletre lehet visszavezetni. Csúcsok: $[a_1, a_2], [b_1, b_2], \dots$

$$|a_1 - b_1||a_2 - b_2| = 2.$$



Sakktábla bejárása

```
> with(GraphTheory):
> csucs:=(m,n)->{seq(seq([a,b],a=1..m),b=1..n)};
      csucs := (m, n) → {seq(seq([a, b]), a = 1 .. m), b = 1 .. n}

> f:=x->if abs(x[1,1]-x[2,1])*abs(x[1,2]-x[2,2])=2 then true; else false
      end if;
      f:=x→if |x1,1-x2,1| |x1,2-x2,2|=2 then true else false end if

> A:=(m,n)->select(f,{seq(seq([u,v],u=csucs(m,n)),v=csucs(m,n))});
      A := (m, n) → select(f, {seq(seq([u, v], u = csucs(m, n)), v = csucs(m, n))})

> B:=(m,n)->{seq({convert(k[1],string),convert(k[2],string)},k=A(m,n));
      B := (m, n) → {seq({convert(k1,string),convert(k2,string)},k = A(m, n))}

> Gsakk:=(m,n)->Graph(B(m,n));
      Gsakk := (m, n) → GraphTheory:-Graph(B(m, n))

> sakkgraf:=Gsakk(6,6);
      sakkgraf := Graph 1: an undirected unweighted graph with 36 vertices and 80 edge(s)

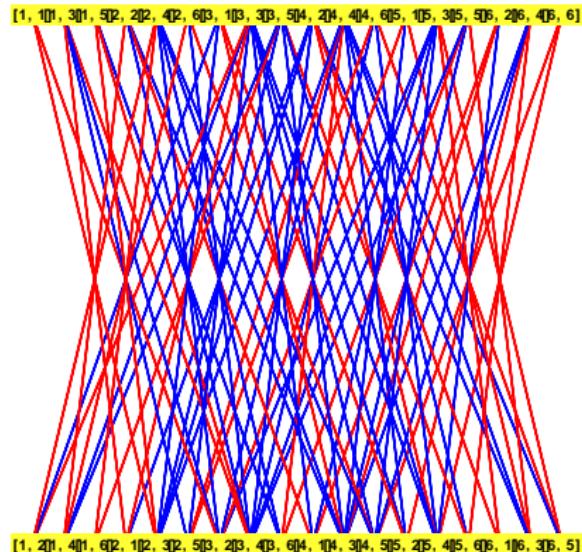
> IsHamiltonian(sakkgraf,'s');
      true

> s;
      ["[1, 1]", "[2, 3]", "[1, 5]", "[3, 4]", "[1, 3]", "[2, 1]", "[3, 3]", "[1, 2]", "[2, 4]", "[1, 6]", "[3, 5]", "[5, 6]",
      "[6, 4]", "[5, 2]", "[3, 1]", "[4, 3]", "[6, 2]", "[4, 1]", "[2, 2]", "[1, 4]", "[2, 6]", "[4, 5]", "[6, 6]", "[5, 4]",
      "[4, 2]", "[6, 1]", "[5, 3]", "[6, 5]", "[4, 6]", "[2, 5]", "[4, 4]", "[3, 6]", "[5, 5]", "[6, 3]", "[5, 1]", "[3, 2]",
      "[1, 1]"]

> HighlightTrail(sakkgraf,s,red);
> DrawGraph(sakkgraf);
```



Sakktábla bejárása



Gráfok színezése - algebrai út

Csúcsok színezése

k -színezés:

$$f(x) = x(x-1)(x-2)\cdots(x-k+1)$$

véges test feletti polinom.

$$f(x_1) = 0, \quad f(x_2) = 0, \dots, f(x_n) = 0$$

garantálja, hogy minden csúcsot kiszínezünk.

Gráfok színezése - algebrai út

Csúcsok színezése

$$f(x_i) - f(x_j)$$

osztható $x_i - x_j$ -vel.

$$g(x_i, x_j) = \frac{f(x_i) - f(x_j)}{x_i - x_j}.$$

Minden $x_i x_j \in E$ esetében $g(x_i, x_j) = 0$.

Gráfok színezése - algebrai út

```

> sain:=proc(G,k)
local f,g,n,renderer, el,T,t; f:=x->x-expand(product(x-a,a=0..k-1));
g:=f*(x-y)-simplify((f(x)-f(y))/(x-y));
n:=NumberOfVertices(G);
renderer:=seq({x||1..n}) union seq(f(x||j),j=2..n)};
el:=Edges(G);
for T in el do t:=op(T);
renderer:=renderer union {g(x||T[1]),x||T[2])};
end do;
renderer;
end proc;
sain:=proc(G,k)
local f,g,n,renderer, el,T,t;
f:=x->x-expand(product(x-a,a=0..k-1));
g:=x||y->simplify((f(x)-f(y))/(x-y));
n:=GraphTheory:-NumberOfVertices(G);
renderer:=union({x||1..n}, seq(f(x||j),j=2..n));
el:=GraphTheory:-Edges(G);
for T in el do t:=op(T);
renderer:=union(renderer, {g(x||T[1]),x||T[2])});
end do;
renderer;
end proc;

> with(GraphTheory):
K3:=CompleteGraph(3);
K3:= Graph 2: an undirected unweighted graph with 3 vertices and 3 edge(s)

> ssin(K3,2);
{ $x_1, x_1^2 - x_2 x_3^2 - x_2, x_1 + x_2 - 1, x_1 + x_3 - 1, x_2 + x_3 - 1$ }

> [msolve(ssin(K3,2),3)];
[]

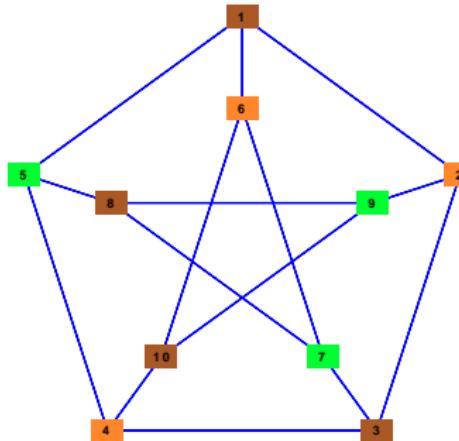
> [msolve(ssin(K3,3),3)];
{ $\{x_1 = 0, x_2 = 1, x_3 = 2\}, \{x_1 = 0, x_2 = 2, x_3 = 1\}$ }

> with(SpecialGraphs):
P:=PetersenGraph();
P:= Graph 3: an undirected unweighted graph with 10 vertices and 15 edge(s)

> A:=[msolve(ssin(P,3),5)];
d:=x->x^5-x_1^5-x_2^5-x_3^5-x_4^5-x_5^5;
x1:=x||1,x2:=x||2,x3:=x||3,x4:=x||4,x5:=x||5;
x6:=x||6,x7:=x||7,x8:=x||8,x9:=x||9,x10:=x||10;
x11:=x||11,x12:=x||12,x13:=x||13,x14:=x||14,x15:=x||15;
x16:=x||16,x17:=x||17,x18:=x||18,x19:=x||19,x20:=x||20;
x21:=x||21,x22:=x||22,x23:=x||23,x24:=x||24,x25:=x||25;
x26:=x||26,x27:=x||27,x28:=x||28,x29:=x||29,x30:=x||30;
x31:=x||31,x32:=x||33,x33:=x||34,x34:=x||35,x35:=x||36;
x36:=x||37,x37:=x||38,x38:=x||39,x39:=x||40,x40:=x||41;
x41:=x||42,x42:=x||43,x43:=x||44,x44:=x||45,x45:=x||46;
x46:=x||47,x47:=x||48,x48:=x||49,x49:=x||50,x50:=x||51;
x51:=x||52,x52:=x||53,x53:=x||54,x54:=x||55,x55:=x||56;
x56:=x||57,x57:=x||58,x58:=x||59,x59:=x||60,x60:=x||61;
x61:=x||62,x62:=x||63,x63:=x||64,x64:=x||65,x65:=x||66;
x66:=x||67,x67:=x||68,x68:=x||69,x69:=x||70,x70:=x||71;
x71:=x||72,x72:=x||73,x73:=x||74,x74:=x||75,x75:=x||76;
x76:=x||77,x77:=x||78,x78:=x||79,x79:=x||80,x80:=x||81;
x81:=x||82,x82:=x||83,x83:=x||84,x84:=x||85,x85:=x||86;
x86:=x||87,x87:=x||88,x88:=x||89,x89:=x||90,x90:=x||91;
x91:=x||92,x92:=x||93,x93:=x||94,x94:=x||95,x95:=x||96;
x96:=x||97,x97:=x||98,x98:=x||99,x99:=x||100,x100:=x||101;
x101:=x||102,x102:=x||103,x103:=x||104,x104:=x||105,x105:=x||106;
x106:=x||107,x107:=x||108,x108:=x||109,x109:=x||110,x110:=x||111;
x111:=x||112,x112:=x||113,x113:=x||114,x114:=x||115,x115:=x||116;
x116:=x||117,x117:=x||118,x118:=x||119,x119:=x||120,x120:=x||121;
x121:=x||122,x122:=x||123,x123:=x||124,x124:=x||125,x125:=x||126;
x126:=x||127,x127:=x||128,x128:=x||129,x129:=x||130,x130:=x||131;
x131:=x||132,x132:=x||133,x133:=x||134,x134:=x||135,x135:=x||136;
x136:=x||137,x137:=x||138,x138:=x||139,x139:=x||140,x140:=x||141;
x141:=x||142,x142:=x||143,x143:=x||144,x144:=x||145,x145:=x||146;
x146:=x||147,x147:=x||148,x148:=x||149,x149:=x||150,x150:=x||151;
x151:=x||152,x152:=x||153,x153:=x||154,x154:=x||155,x155:=x||156;
x156:=x||157,x157:=x||158,x158:=x||159,x159:=x||160,x160:=x||161;
x161:=x||162,x162:=x||163,x163:=x||164,x164:=x||165,x165:=x||166;
x166:=x||167,x167:=x||168,x168:=x||169,x169:=x||170,x170:=x||171;
x171:=x||172,x172:=x||173,x173:=x||174,x174:=x||175,x175:=x||176;
x176:=x||177,x177:=x||178,x178:=x||179,x179:=x||180,x180:=x||181;
x181:=x||182,x182:=x||183,x183:=x||184,x184:=x||185,x185:=x||186;
x186:=x||187,x187:=x||188,x188:=x||189,x189:=x||190,x190:=x||191;
x191:=x||192,x192:=x||193,x193:=x||194,x194:=x||195,x195:=x||196;
x196:=x||197,x197:=x||198,x198:=x||199,x199:=x||200,x200:=x||201;
x201:=x||202,x202:=x||203,x203:=x||204,x204:=x||205,x205:=x||206;
x206:=x||207,x207:=x||208,x208:=x||209,x209:=x||210,x210:=x||211;
x211:=x||212,x212:=x||213,x213:=x||214,x214:=x||215,x215:=x||216;
x216:=x||217,x217:=x||218,x218:=x||219,x219:=x||220,x220:=x||221;
x221:=x||222,x222:=x||223,x223:=x||224,x224:=x||225,x225:=x||226;
x226:=x||227,x227:=x||228,x228:=x||229,x229:=x||230,x230:=x||231;
x231:=x||232,x232:=x||233,x233:=x||234,x234:=x||235,x235:=x||236;
x236:=x||237,x237:=x||238,x238:=x||239,x239:=x||240,x240:=x||241;
x241:=x||242,x242:=x||243,x243:=x||244,x244:=x||245,x245:=x||246;
x246:=x||247,x247:=x||248,x248:=x||249,x249:=x||250,x250:=x||251;
x251:=x||252,x252:=x||253,x253:=x||254,x254:=x||255,x255:=x||256;
x256:=x||257,x257:=x||258,x258:=x||259,x259:=x||260,x260:=x||261;
x261:=x||262,x262:=x||263,x263:=x||264,x264:=x||265,x265:=x||266;
x266:=x||267,x267:=x||268,x268:=x||269,x269:=x||270,x270:=x||271;
x271:=x||272,x272:=x||273,x273:=x||274,x274:=x||275,x275:=x||276;
x276:=x||277,x277:=x||278,x278:=x||279,x279:=x||280,x280:=x||281;
x281:=x||282,x282:=x||283,x283:=x||284,x284:=x||285,x285:=x||286;
x286:=x||287,x287:=x||288,x288:=x||289,x289:=x||290,x290:=x||291;
x291:=x||292,x292:=x||293,x293:=x||294,x294:=x||295,x295:=x||296;
x296:=x||297,x297:=x||298,x298:=x||299,x299:=x||300,x300:=x||301;
x301:=x||302,x302:=x||303,x303:=x||304,x304:=x||305,x305:=x||306;
x306:=x||307,x307:=x||308,x308:=x||309,x309:=x||310,x310:=x||311;
x311:=x||312,x312:=x||313,x313:=x||314,x314:=x||315,x315:=x||316;
x316:=x||317,x317:=x||318,x318:=x||319,x319:=x||320,x320:=x||321;
x321:=x||322,x322:=x||323,x323:=x||324,x324:=x||325,x325:=x||326;
x326:=x||327,x327:=x||328,x328:=x||329,x329:=x||330,x330:=x||331;
x331:=x||332,x332:=x||333,x333:=x||334,x334:=x||335,x335:=x||336;
x336:=x||337,x337:=x||338,x338:=x||339,x339:=x||340,x340:=x||341;
x341:=x||342,x342:=x||343,x343:=x||344,x344:=x||345,x345:=x||346;
x346:=x||347,x347:=x||348,x348:=x||349,x349:=x||350,x350:=x||351;
x351:=x||352,x352:=x||353,x353:=x||354,x354:=x||355,x355:=x||356;
x356:=x||357,x357:=x||358,x358:=x||359,x359:=x||360,x360:=x||361;
x361:=x||362,x362:=x||363,x363:=x||364,x364:=x||365,x365:=x||366;
x366:=x||367,x367:=x||368,x368:=x||369,x369:=x||370,x370:=x||371;
x371:=x||372,x372:=x||373,x373:=x||374,x374:=x||375,x375:=x||376;
x376:=x||377,x377:=x||378,x378:=x||379,x379:=x||380,x380:=x||381;
x381:=x||382,x382:=x||383,x383:=x||384,x384:=x||385,x385:=x||386;
x386:=x||387,x387:=x||388,x388:=x||389,x389:=x||390,x390:=x||391;
x391:=x||392,x392:=x||393,x393:=x||394,x394:=x||395,x395:=x||396;
x396:=x||397,x397:=x||398,x398:=x||399,x399:=x||400,x400:=x||401;
x401:=x||402,x402:=x||403,x403:=x||404,x404:=x||405,x405:=x||406;
x406:=x||407,x407:=x||408,x408:=x||409,x409:=x||410,x410:=x||411;
x411:=x||412,x412:=x||413,x413:=x||414,x414:=x||415,x415:=x||416;
x416:=x||417,x417:=x||418,x418:=x||419,x419:=x||420,x420:=x||421;
x421:=x||422,x422:=x||423,x423:=x||424,x424:=x||425,x425:=x||426;
x426:=x||427,x427:=x||428,x428:=x||429,x429:=x||430,x430:=x||431;
x431:=x||432,x432:=x||433,x433:=x||434,x434:=x||435,x435:=x||436;
x436:=x||437,x437:=x||438,x438:=x||439,x439:=x||440,x440:=x||441;
x441:=x||442,x442:=x||443,x443:=x||444,x444:=x||445,x445:=x||446;
x446:=x||447,x447:=x||448,x448:=x||449,x449:=x||450,x450:=x||451;
x451:=x||452,x452:=x||453,x453:=x||454,x454:=x||455,x455:=x||456;
x456:=x||457,x457:=x||458,x458:=x||459,x459:=x||460,x460:=x||461;
x461:=x||462,x462:=x||463,x463:=x||464,x464:=x||465,x465:=x||466;
x466:=x||467,x467:=x||468,x468:=x||469,x469:=x||470,x470:=x||471;
x471:=x||472,x472:=x||473,x473:=x||474,x474:=x||475,x475:=x||476;
x476:=x||477,x477:=x||478,x478:=x||479,x479:=x||480,x480:=x||481;
x481:=x||482,x482:=x||483,x483:=x||484,x484:=x||485,x485:=x||486;
x486:=x||487,x487:=x||488,x488:=x||489,x489:=x||490,x490:=x||491;
x491:=x||492,x492:=x||493,x493:=x||494,x494:=x||495,x495:=x||496;
x496:=x||497,x497:=x||498,x498:=x||499,x499:=x||500,x500:=x||501;
x501:=x||502,x502:=x||503,x503:=x||504,x504:=x||505,x505:=x||506;
x506:=x||507,x507:=x||508,x508:=x||509,x509:=x||510,x510:=x||511;
x511:=x||512,x512:=x||513,x513:=x||514,x514:=x||515,x515:=x||516;
x516:=x||517,x517:=x||518,x518:=x||519,x519:=x||520,x520:=x||521;
x521:=x||522,x522:=x||523,x523:=x||524,x524:=x||525,x525:=x||526;
x526:=x||527,x527:=x||528,x528:=x||529,x529:=x||530,x530:=x||531;
x531:=x||532,x532:=x||533,x533:=x||534,x534:=x||535,x535:=x||536;
x536:=x||537,x537:=x||538,x538:=x||539,x539:=x||540,x540:=x||541;
x541:=x||542,x542:=x||543,x543:=x||544,x544:=x||545,x545:=x||546;
x546:=x||547,x547:=x||548,x548:=x||549,x549:=x||550,x550:=x||551;
x551:=x||552,x552:=x||553,x553:=x||554,x554:=x||555,x555:=x||556;
x556:=x||557,x557:=x||558,x558:=x||559,x559:=x||560,x560:=x||561;
x561:=x||562,x562:=x||563,x563:=x||564,x564:=x||565,x565:=x||566;
x566:=x||567,x567:=x||568,x568:=x||569,x569:=x||570,x570:=x||571;
x571:=x||572,x572:=x||573,x573:=x||574,x574:=x||575,x575:=x||576;
x576:=x||577,x577:=x||578,x578:=x||579,x579:=x||580,x580:=x||581;
x581:=x||582,x582:=x||583,x583:=x||584,x584:=x||585,x585:=x||586;
x586:=x||587,x587:=x||588,x588:=x||589,x589:=x||590,x590:=x||591;
x591:=x||592,x592:=x||593,x593:=x||594,x594:=x||595,x595:=x||596;
x596:=x||597,x597:=x||598,x598:=x||599,x599:=x||600,x600:=x||601;
x601:=x||602,x602:=x||603,x603:=x||604,x604:=x||605,x605:=x||606;
x606:=x||607,x607:=x||608,x608:=x||609,x609:=x||610,x610:=x||611;
x611:=x||612,x612:=x||613,x613:=x||614,x614:=x||615,x615:=x||616;
x616:=x||617,x617:=x||618,x618:=x||619,x619:=x||620,x620:=x||621;
x621:=x||622,x622:=x||623,x623:=x||624,x624:=x||625,x625:=x||626;
x626:=x||627,x627:=x||628,x628:=x||629,x629:=x||630,x630:=x||631;
x631:=x||632,x632:=x||633,x633:=x||634,x634:=x||635,x635:=x||636;
x636:=x||637,x637:=x||638,x638:=x||639,x639:=x||640,x640:=x||641;
x641:=x||642,x642:=x||643,x643:=x||644,x644:=x||645,x645:=x||646;
x646:=x||647,x647:=x||648,x648:=x||649,x649:=x||650,x650:=x||651;
x651:=x||652,x652:=x||653,x653:=x||654,x654:=x||655,x655:=x||656;
x656:=x||657,x657:=x||658,x658:=x||659,x659:=x||660,x660:=x||661;
x661:=x||662,x662:=x||663,x663:=x||664,x664:=x||665,x665:=x||666;
x666:=x||667,x667:=x||668,x668:=x||669,x669:=x||670,x670:=x||671;
x671:=x||672,x672:=x||673,x673:=x||674,x674:=x||675,x675:=x||676;
x676:=x||677,x677:=x||678,x678:=x||679,x679:=x||680,x680:=x||681;
x681:=x||682,x682:=x||683,x683:=x||684,x684:=x||685,x685:=x||686;
x686:=x||687,x687:=x||688,x688:=x||689,x689:=x||690,x690:=x||691;
x691:=x||692,x692:=x||693,x693:=x||694,x694:=x||695,x695:=x||696;
x696:=x||697,x697:=x||698,x698:=x||699,x699:=x||700,x700:=x||701;
x701:=x||702,x702:=x||703,x703:=x||704,x704:=x||705,x705:=x||706;
x706:=x||707,x707:=x||708,x708:=x||709,x709:=x||710,x710:=x||711;
x711:=x||712,x712:=x||713,x713:=x||714,x714:=x||715,x715:=x||716;
x716:=x||717,x717:=x||718,x718:=x||719,x719:=x||720,x720:=x||721;
x721:=x||722,x722:=x||723,x723:=x||724,x724:=x||725,x725:=x||726;
x726:=x||727,x727:=x||728,x728:=x||729,x729:=x||730,x730:=x||731;
x731:=x||732,x732:=x||733,x733:=x||734,x734:=x||735,x735:=x||736;
x736:=x||737,x737:=x||738,x738:=x||739,x739:=x||740,x740:=x||741;
x741:=x||742,x742:=x||743,x743:=x||744,x744:=x||745,x745:=x||746;
x746:=x||747,x747:=x||748,x748:=x||749,x749:=x||750,x750:=x||751;
x751:=x||752,x752:=x||753,x753:=x||754,x754:=x||755,x755:=x||756;
x756:=x||757,x757:=x||758,x758:=x||759,x759:=x||760,x760:=x||761;
x761:=x||762,x762:=x||763,x763:=x||764,x764:=x||765,x765:=x||766;
x766:=x||767,x767:=x||768,x768:=x||769,x769:=x||770,x770:=x||771;
x771:=x||772,x772:=x||773,x773:=x||774,x774:=x||775,x775:=x||776;
x776:=x||777,x777:=x||778,x778:=x||779,x779:=x||780,x780:=x||781;
x781:=x||782,x782:=x||783,x783:=x||784,x784:=x||785,x785:=x||786;
x786:=x||787,x787:=x||788,x788:=x||789,x789:=x||790,x790:=x||791;
x791:=x||792,x792:=x||793,x793:=x||794,x794:=x||795,x795:=x||796;
x796:=x||797,x797:=x||798,x798:=x||799,x799:=x||800,x800:=x||801;
x801:=x||802,x802:=x||803,x803:=x||804,x804:=x||805,x805:=x||806;
x806:=x||807,x807:=x||808,x808:=x||809,x809:=x||810,x810:=x||811;
x811:=x||812,x812:=x||813,x813:=x||814,x814:=x||815,x815:=x||816;
x816:=x||817,x817:=x||818,x818:=x||819,x819:=x||820,x820:=x||821;
x821:=x||822,x822:=x||823,x823:=x||824,x824:=x||825,x825:=x||826;
x826:=x||827,x827:=x||828,x828:=x||829,x829:=x||830,x830:=x||831;
x831:=x||832,x832:=x||833,x833:=x||834,x834:=x||835,x835:=x||836;
x836:=x||837,x837:=x||838,x838:=x||839,x839:=x||840,x840:=x||841;
x841:=x||842,x842:=x||843,x843:=x||844,x844:=x||845,x845:=x||846;
x846:=x||847,x847:=x||848,x848:=x||849,x849:=x||850,x850:=x||851;
x851:=x||852,x852:=x||853,x853:=x||854,x854:=x||855,x855:=x||856;
x856:=x||857,x857:=x||858,x858:=x||859,x859:=x||860,x860:=x||861;
x861:=x||862,x862:=x||863,x863:=x||864,x864:=x||865,x865:=x||866;
x866:=x||867,x867:=x||868,x868:=x||869,x869:=x||870,x870:=x||871;
x871:=x||872,x872:=x||873,x873:=x||874,x874:=x||875,x875:=x||876;
x876:=x||877,x877:=x||878,x878:=x||879,x879:=x||880,x880:=x||881;
x881:=x||882,x882:=x||883,x883:=x||884,x884:=x||885,x885:=x||886;
x886:=x||887,x887:=x||888,x888:=x||889,x889:=x||890,x890:=x||891;
x891:=x||892,x892:=x||893,x893:=x||894,x894:=x||895,x895:=x||896;
x896:=x||897,x897:=x||898,x898:=x||899,x899:=x||900,x900:=x||901;
x901:=x||902,x902:=x||903,x903:=x||904,x904:=x||905,x905:=x||906;
x906:=x||907,x907:=x||908,x908:=x||909,x909:=x||910,x910:=x||911;
x911:=x||912,x912:=x||913,x913:=x||914,x914:=x||915,x915:=x||916;
x916:=x||917,x917:=x||918,x918:=x||919,x919:=x||920,x920:=x||921;
x921:=x||922,x922:=x||923,x923:=x||924,x924:=x||925,x925:=x||926;
x926:=x||927,x927:=x||928,x928:=x||929,x929:=x||930,x930:=x||931;
x931:=x||932,x932:=x||933,x933:=x||934,x934:=x||935,x935:=x||936;
x936:=x||937,x937:=x||938,x938:=x||939,x939:=x||940,x940:=x||941;
x941:=x||942,x942:=x||943,x943:=x||944,x944:=x||945,x945:=x||946;
x946:=x||947,x947:=x||948,x948:=x||949,x949:=x||950,x950:=x||951;
x951:=x||952,x952:=x||953,x953:=x||954,x954:=x||955,x955:=x||956;
x956:=x||957,x957:=x||958,x958:=x||959,x959:=x||960,x960:=x||961;
x961:=x||962,x962:=x||963,x963:=x||964,x964:=x||965,x965:=x||966;
x966:=x||967,x967:=x||968,x968:=x||969,x969:=x||970,x970:=x||971;
x971:=x||972,x972:=x||973,x973:=x||974,x974:=x||975,x975:=x||976;
x976:=x||977,x977:=x||978,x978:=x||979,x979:=x||980,x980:=x||981;
x981:=x||982,x982:=x||983,x983:=x||984,x984:=x||985,x985:=x||986;
x986:=x||987,x987:=x||988,x988:=x||989,x989:=x||990,x990:=x||991;
x991:=x||992,x992:=x||993,x993:=x||994,x994:=x||995,x995:=x||996;
x996:=x||997,x997:=x||998,x998:=x||999,x999:=x||1000,x1000:=x||1001;
x1001:=x||1002,x1002:=x||1003,x1003:=x||1004,x1004:=x||1005,x1005:=x||1006;
x1006:=x||1007,x1007:=x||1008,x1008:=x||1009,x1009:=x||1010,x1010:=x||1011;
x1011:=x||1012,x1012:=x||1013,x1013:=x||1014,x1014:=x||1015,x1015:=x||1016;
x1016:=x||1017,x1017:=x||1018,x1018:=x||1019,x1019:=x||1020,x1020:=x||1021;
x1021:=x||1022,x1022:=x||1023,x1023:=x||1024,x1024:=x||1025,x1025:=x||1026;
x1026:=x||1027,x1027:=x||1028,x1028:=x||1029,x1029:=x||1030,x1030:=x||1031;
x1031:=x||1032,x1032:=x||1033,x1033:=x||1034,x1034:=x||1035,x1035:=x||1036;
x1036:=x||1037,x1037:=x||1038,x1038:=x||1039,x1039:=x||1040,x1040:=x||1041;
x1041:=x||1042,x1042:=x||1043,x1043:=x||1044,x1044:=x||1045,x1045:=x||1046;
x1046:=x||1047,x1047:=x||1048,x1048:=x||1049,x1049:=x||1050,x1050:=x||1051;
x1051:=x||1052,x1052:=x||1053,x1053:=x||1054,x1054:=x||1055,x1055:=x||1056;
x1056:=x||1057,x1057:=x||1058,x1058:=x||1059,x1059:=x||1060,x1060:=x||1061;
x1061:=x||1062,x1062:=x||1063,x1063:=x||1064,x1064:=x||1065,x1065:=x||1066;
x1066:=x||1067,x1067:=x||1068,x1068:=x||1069,x1069:=x||1070,x1070:=x||1071;
x1071:=x||1072,x1072:=x||1073,x1073:=x||1074,x1074:=x||1075,x1075:=x||1076;
x1076:=x||1077,x1077:=x||1078,x1078:=x||1079,x1079:=x||1080,x1080:=x||1081;
x1081:=x||1082,x1082:=x||1083,x1083:=x||1084,x1084:=x||1085,x1085:=x||1086;
x1086:=x||1087,x1087:=x||1088,x1088:=x||1089,x1089:=x||1090,x1090:=x||1091;
x1091:=x||1092,x1092:=x||1093,x1093:=x||1094,x1094:=x||1095,x1095:=x||1096;
x1096:=x||1097,x1097:=x||1098,x1098:=x||1099,x1099:=x||1100,x1100:=x||1101;
x1101:=x||1102,x1102:=x||1103,x1103:=x||1104,x1104:=x||1105,x1105:=x||1106;
x1106:=x||1107,x1107:=x||1108,x1108:=x||1109,x1109:=x||1110,x1110:=x||1111;
x1111:=x||1112,x1112:=x||1113,x1113:=x||1114,x1114:=x||1115,x1115:=x||1116;
x1116:=x||1117,x1117:=x||1118,x1118:=x||1119,x1119:=x||1120,x1120:=x||1121;
x1121:=x||1122,x1122:=x||1123,x1123:=x||1124,x1124:=x||1125,x1125:=x||1126;
x1126:=x||1127,x1127:=x||1128,x1128:=x||1129,x1129:=x||1130,x1130:=x||1131;
x1131:=x||1132,x1132:=x||1133,x1133:=x||1134,x1134:=x||1135,x1135:=x||1136;
x1136:=x||1137,x1137:=x||1138,x1138:=x||1139,x1139:=x||1140,x1140:=x||1141;
x1141:=x||1142,x1142:=x||1143,x1143:=x||1144,x1144:=x||1145,x1145:=x||1146;
x1146:=x||1147,x1147:=x||1148,x1148:=x||1149,x1149:=x||1150,x1150:=x||1
```

Gráfok színezése - algebrai út

```
x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 0, x_5 = 1, x_6 = 0, x_7 = 2, x_8 = 1, x_9 = 0, x_{10} = 2 \}, \{x_1 = 0, x_2 = 2, x_3 = 1, x_4 = 0, x_5 = 2, x_6 = 2, x_7 = 0, x_8 = 1, x_9 = 0, x_{10} = 1\} ] ]  
> al:= [seq(op(A[1][k])[2],k=1..10)];  
al := [0, 1, 0, 1, 2, 1, 2, 0, 2, 0]  
> for s from 1 to 10 do HighlightVertex(P,s,COLOR(RGB,1/(1.5+al[s])),1/(2.9  
+al[s]),1/(7.1+al[s]));  
> end do;  
> DrawGraph(P);
```



Mátrixok hatványai sajátvektorokkal

Diagonálisítás

A egy mátrix, P a sajátvektorokból álló mátrix:

$$P^{-1}AP$$

diagonális. Ezt felhasználva meghatározhatjuk az A^n mátrixot zárt alakban.

Rekurzív sorozatok

Fibonacci sorozat

$F_0 = 0, F_1 = 1$ és $F_n = F_{n-1} + F_{n-2}$, legyen

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

akkor $A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}$.

Inhomogén rekurzív egyenletrendszer

Inhomogén rekurzió zárt alakjának meghatározása

$$x_{n+1} = ax_n + by_n + c$$

$$y_{n+1} = dx_n + ey_n + f$$

adott x_0, y_0 kezdőértékek mellett.

a	-2
b	3
c	2
d	-1
e	2
f	-2
x0	3
y0	2

Az A mátrix: $\begin{pmatrix} -2 & 3 \\ -1 & 2 \end{pmatrix}$

Az B vektor: $(2, -2)$

Az X_0 vektor: $(3, 2)$

Az A mátrix sajátértékei: -1 és 1

sajátérték: -1 , hozzá tartozó sajátvektor: $\begin{pmatrix} 1, \frac{1}{2} \end{pmatrix}$

sajátérték: 1 , hozzá tartozó sajátvektor: $(1, 1)$

A sajátvektorokból álló P mátrix: $\begin{pmatrix} 1 & 1 \\ \frac{1}{2} & 1 \end{pmatrix}$

P inverze: $\begin{pmatrix} \frac{3}{2} & -\frac{3}{2} \\ -\frac{1}{2} & \frac{3}{2} \end{pmatrix}$

Ekkor a $P^{-1}AP$ mátrix diagonális: $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

Innen A^n zárt alakja könnyen meghatározható: $A^n = P D^n P^{-1}$

Az A mátrix n -edik hatványa: $\begin{pmatrix} \frac{3}{2} (-1)^n - \frac{1}{2} & -\frac{3}{2} (-1)^n + \frac{3}{2} \\ \frac{1}{2} (-1)^n - \frac{1}{2} & -\frac{1}{2} (-1)^n + \frac{3}{2} \end{pmatrix}$

Az $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + (A^{n-1} + A^{n-2} + \dots + A + E)B$ összefüggés alapján adódik a formula x_n -re és y_n -re:

$$x_n = -\frac{3}{2} (-1)^n - 4n + \frac{9}{2}$$

$$y_n = -\frac{1}{2} (-1)^n - 4n + \frac{5}{2}$$

Mátrixok hatványai sajátvektorokkal

```

> with(LinearAlgebra):
> matrixN:=proc(A)
> local u,v,Diag; u,v:=Eigenvectors(A);
> Diag:=Matrix([[u[1]^n,0],[0,u[2]^n]]):
> v.Diag.v=(-1);
> end proc;
matrixN:= proc()
local u, v, Diag;
u, v := LinearAlgebra:-Eigenvectors(A); Diag := Matrix([[u[1]^n,0],[0,u[2]^n]]); `)(v,Diag,1/v)
end proc;

> matrixN(Matrix([[4,-3],[1,0]]));

$$\begin{bmatrix} -\frac{1}{2} + \frac{3\sqrt{3}}{2} & \frac{1}{2} - \frac{3\sqrt{3}}{2} \\ -\frac{1}{2} + \frac{\sqrt{3}}{2} & \frac{3}{2} - \frac{\sqrt{3}}{2} \end{bmatrix}$$


> Fib:=(matrixN(Matrix([[1,1],[1,0]])).Vector([1,0]))(2);
Fib:= 
$$\frac{\left(\frac{\sqrt{5}}{2} + \frac{1}{2}\right)^n \sqrt{5} (\sqrt{5}-1) (\sqrt{5}+1)}{20} - \frac{\left(\frac{1}{2} - \frac{\sqrt{5}}{2}\right)^n \sqrt{5} (\sqrt{5}-1) (\sqrt{5}+1)}{20}$$


> simplify(Fib);

$$\sqrt{5} \left( \left( \frac{\sqrt{5}}{2} + \frac{1}{2} \right)^n - \left( \frac{1}{2} - \frac{\sqrt{5}}{2} \right)^n \right) / 5$$


> seq(evala(subs(n=k,Fib)),k=0..10);
0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55

> A:=Matrix([[2,1],[1,2]]);
A:= 
$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$


> U1:=subs(t=n,sum(matrixN(A),n=0..t-1)).Vector([1,1]);
U1:= 
$$\begin{bmatrix} -\frac{1}{2} + \frac{3\sqrt{3}}{2} \\ -\frac{1}{2} + \frac{\sqrt{3}}{2} \end{bmatrix}$$


> U2:=matrixN(A).Vector([2,3]);
U2:= 
$$\begin{bmatrix} -\frac{1}{2} + \frac{5\sqrt{3}}{2} \\ \frac{1}{2} + \frac{5\sqrt{3}}{2} \end{bmatrix}$$


> U1+U2;

$$\begin{bmatrix} -1 + 3\sqrt{3} \\ 3\sqrt{3} \end{bmatrix}$$


```

Berlekamp algoritmus

Polinomok $\mathbb{F}_q[X]$ felett

$f(X) = \sum_{k=0}^n a_i X^i$ ekkor a kis Fermat-tétel miatt

$$f(X)^q = \sum_{k=0}^n a_i X^{qi}.$$

Az $X^q - X$ polinom faktorizációja egyszerű. Egy F polinom faktorizációjához keresunk olyan $f(X)$ -et, amelyre

$$f(X) \equiv f(X)^q \pmod{F}.$$

Berlekamp algoritmus

```

> P:=x^5+10*x^4+25*x^2+28;
P:= $x^5 + 10x^4 + 25x^2 + 28$ 

> h:=add(s,s=[seq(a[i]*x^i,i=0..4)]);
h:= $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ 

> h31:=add(s,s=[seq(a[i]*x^(31*i),i=0..4)]);
h31:= $a_0 + a_1x^{31} + a_2x^{62} + a_3x^{93} + a_4x^{124}$ 

> for k from 31 to 124 do h31:=subs(x^k=modpol(x^k,P,x,31),h31); end do:
h31;
a_0 + a_1(8x^4 + 9x^3 + 9x^2 + 28x + 19) + a_2(26x^4 + x^3 + 7x^2 + 3x + 3) + a_3(7x^4 + 3x^3 + 4x^2 + 6x
+ 28) + a_4(24x^4 + 26x^3 + 22x^2 + 16x + 28)

> with(LinearAlgebra):
> sys:=[seq(coeff(h31,x,k)=coeff(h,x,k),k=0..4)];
sys:=[a_0 + 19a_1 + 3a_2 + 28a_3 + 28a_4 = a_0, 28a_1 + 3a_2 + 6a_3 + 16a_4 = a_1, 9a_1 + 7a_2 + 4a_3 + 22a_4
- a_2, 9a_1 + a_2 + 3a_3 + 26a_4 = a_2, 8a_1 + 26a_2 + 7a_3 + 24a_4 = a_3]

> var:=[seq(a[k],k=0..4)];
var:=[a_0, a_1, a_2, a_3, a_4]

> (A,b):=GenerateMatrix(sys,var);
A,b:=

$$\begin{pmatrix} 0 & 19 & 3 & 28 & 28 \\ 0 & 27 & 3 & 6 & 16 \\ 0 & 9 & 6 & 4 & 22 \\ 0 & 9 & 1 & 2 & 26 \\ 0 & 8 & 26 & 7 & 23 \end{pmatrix} \left| \begin{array}{l} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{array} \right.$$


> with(LinearAlgebra[Modular]):
> A31:=Mod(31,A,integer[]);
A31:=

$$\begin{pmatrix} 0 & 19 & 3 & 28 & 28 \\ 0 & 27 & 3 & 6 & 16 \\ 0 & 9 & 6 & 4 & 22 \\ 0 & 9 & 1 & 2 & 26 \\ 0 & 8 & 26 & 7 & 23 \end{pmatrix}$$


> N:=Basis(31,A31,row,false,column);
N:=

$$\begin{pmatrix} 1 & | & 0 & | & 0 \\ 0 & | & 26 & | & 17 \\ 0 & | & 12 & | & 7 \\ 0 & | & 1 & | & 0 \\ 0 & | & 0 & | & 1 \end{pmatrix}$$


> T1:=x^3+12*x^2+26*x;
T1:= $x^3 + 12x^2 + 26x$ 

> for k from 0 to 30 do PT:=Gcd(P,T1+k) mod 31; if PT>1 then print(PT);
and if; end do:
```

Berlekamp algoritmus

```
x2 + 15 x + 9
x + 1
x2 + 25 x + 10
> T2:=x^4+7*x^2+17*x;
T2 := x4 + 7 x2 + 17 x
> for k from 0 to 30 do PT:=Gcd(P,T2+k) mod 31; if PT<>1 then print(PT);
end if; end do:
x + 1
x2 + 25 x + 10
x2 + 15 x + 9
```

Rácsok

Adott b_1, b_2, \dots, b_k vektorok \mathbb{R}^n -ben,

$$\Lambda = \{z_1 b_1 + z_2 b_2 + \dots + z_k b_k : z_i \in \mathbb{Z}\}$$

egy rács.

Adott rácsot több vektorrendszer is meg tud határozni. Rövid vektorokból álló rendszerek a gyakorlatban hasznosak (titkosítások). Az LLL-algoritmus segítségével találunk rövid vektorokat. Bemutatunk néhány érdekes alkalmazást.

Polinomok gyökei

```

> f:=expand(cos(16*x));
f:= 32768 cos(x)^16 - 131072 cos(x)^14 + 212992 cos(x)^12 - 180224 cos(x)^10 + 84480 cos(x)^8
      - 21504 cos(x)^6 + 2688 cos(x)^4 - 128 cos(x)^2 + 1
> cos(Pi);
                                         -1
> F:=subs(cos(x)=x,f)+1;
F:= 32768 x^16 - 131072 x^14 + 212992 x^12 - 180224 x^10 + 84480 x^8 - 21504 x^6 + 2688 x^4 - 128 x^2
      + 2
> Fsol:=solve(F,x);
Fsol :=  $\frac{\sqrt{2-\sqrt{2-\sqrt{2}}}}{2}, \frac{\sqrt{2-\sqrt{2-\sqrt{2}}}}{2}, \frac{\sqrt{2-\sqrt{2-\sqrt{2}}}}{2}, \frac{\sqrt{2-\sqrt{2-\sqrt{2}}}}{2},$ 
 $\frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2}, \frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2}, \frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2}, \frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2},$ 
 $\frac{\sqrt{2+\sqrt{2-\sqrt{2}}}}{2}, \frac{\sqrt{2+\sqrt{2-\sqrt{2}}}}{2}, \frac{\sqrt{2+\sqrt{2-\sqrt{2}}}}{2}, \frac{\sqrt{2+\sqrt{2-\sqrt{2}}}}{2},$ 
 $\frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2}, \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2}, \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2}, \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2}$ 
> evalf(Fsol[13]);
0.9807852805
> a:=evalf(25)(cos(Pi/16));
a := 0.9807852804032304491261822
> with(LinearAlgebra):
> M:=Matrix(9,shape=identity);
M := 
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

> M1:=<M|<seq(round(evalf[100](10^50*cos(Pi/16)^k)),k=0..8)>>;

```

Polinomok gyökei



Polinomok faktorizációja

```

> f:=expand((x^5+x^2+2014)*(x^6+x^3+x+2014));
f:=x11+2*x8+2015*x6+2015*x5+2015*x3+2014*x2+2014*x+4056196
> factor(f);
(x5+x2+2014) (x6+x3+x+2014)
> a:=evalf[50](fsolve(f,x));
a := -4.588971774900065964618262061854619597229082925560
> with(LinearAlgebra):
> M:=Matrix(6,shape=identity);
M:=
<math display="block">\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}
> M1:=<math>\langle M | \langle \text{seq}(\text{round}(\text{evalf}[50](10^20*a^k)), k=0..5) \rangle \rangle\gt;;
M1:=
<math display="block">\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 100000000000000000000000000000 \\ 0 & 1 & 0 & 0 & 0 & 0 & -458897177490006596462 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2105866195082946168955 \\ 0 & 0 & 0 & 1 & 0 & 0 & -9663760530951836046332 \\ 0 & 0 & 0 & 0 & 1 & 0 & 44346724315931250914222 \\ 0 & 0 & 0 & 0 & 0 & 1 & -203505866195082946168955 \end{bmatrix}
> \text{with(IntegerRelations)}:
> \text{LLL}(M1);

```

2014	0	1	0	0	1	0
-273	4668	-2012	854	-4263	-1001	5965
-605	-2848	-1717	4011	6370	1186	3899
563	-5226	-797	6052	-2480	-824	373
-574	-4342	4219	-5509	1107	556	6911
746	-3523	-15296	-3408	97	33	3421

Hátizsák probléma - Merkle-Hellman titkosítás

```
> S:=[7,11,19,39,79,159,329,649,1297,2663];add(k,k=S);
S := [7, 11, 19, 39, 79, 159, 329, 649, 1297, 2663]
5252

> p:=nextprime(5252);
p := 5261

> m:=3000;
m := 3000

> minv:=l/m mod p;
minv := 4663

> publikus:=[seq((S[k])^m) mod p,k=1..nops(S))];
publikus := [5217, 1434, 4390, 1258, 255, 3510, 3193, 430, 3121, 2802]

> uzenet:=[1,0,1,0,1,0,1,0,1,0];
uzenet := [1, 0, 1, 0, 1, 0, 1, 0, 1, 0]

> kodolt:=add(t,t=[seq(uzenet[k]*publikus[k],k=1..nops(S))]);
kodolt := 16176

> ul:=kodolt*minv mod p;
ul := 1731

> hatizzak:=proc(H,s)
> local V,k,s1; V:=[seq(0,k=1..nops(H))];s1:=s;
> for k from nops(H) to 1 by -1 do
> if s1=>H[k] then V[k]:=1; s1:=s1-H[k]; end if;
> end do;
> V;
> end proc;
hatizzak := proc(H, s)
local V, k, s1;
V := [seq(0, k = 1 .. nops(H))];
s1 := s;
for k from nops(H) by -1 to 1 do if H[k] <= s1 then V[k] := 1; s1 := s1 - H[k] end if end do;
V
end proc;

> hatizzak(S,ul);
[1, 0, 1, 0, 1, 0, 1, 0, 1, 0]

> with(LinearAlgebra):
> M:=Matrix(10,shape=identity);
```

Hátizsák probléma - Merkle-Hellman titkosítás

```


$$M := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$


> M1:=convert(<M,Vector[row](10,fill=0)>,matrix);

$$M1 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$


> M1:=<M1|Vector[column](11,[seq(publikus[k],k=1..10)],fill=-kodolt)>;
convert(M1,matrix);


$$M2 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5217 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1434 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4390 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1258 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 255 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 3510 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3193 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 430 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3121 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2802 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -16176 \end{bmatrix}$$


> with(IntegerRelations):
> convert(LLL(M2),matrix);

```

Hátizsák probléma - Merkle-Hellman titkosítás

$$\begin{bmatrix} 0 & -1 & 0 & 1 & -1 & 0 & 0 & 1 & 0 & 0 & -1 \\ 1 & 0 & -1 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & -1 & 0 & -1 & 0 & 0 & 0 & -1 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 & -2 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & -1 & 1 & -2 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & -1 & 0 & 1 & -1 & 0 & 1 & 0 & 1 \\ -1 & -1 & -1 & 1 & 0 & 2 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 1 & 2 & -1 \\ -1 & -1 & 1 & -1 & 1 & 0 & 2 & 0 & -1 & 0 & 1 \\ 2 & -1 & -1 & 0 & 0 & -2 & -1 & 0 & 0 & 2 & 1 \end{bmatrix}$$

Index kalkulus

Additív és multiplikatív csoportok

$$(G, +) \Rightarrow ng_1 = g_2 \quad \text{additív}$$

$$(H, \times) \Rightarrow h_1^n = h_2 \quad \text{multiplikatív}$$

\mathbb{F}_q multiplikatív csoportban:

$$a^k \equiv p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m} \pmod{q}$$

$$k \equiv t_1 \log_a p_1 + t_2 \log_a p_2 + \dots + t_m \log_a p_m \pmod{q-1}$$

Index kalkulus

```

> q:=101;
q := 101
> nops({seq(7^k mod 101,k=1..101)});
100
> seq([k,ifactor(7^k mod 101)],k=1..20);
[[1, (7)], [2, (7)], [3, (2)^3 (5)], [4, (2) (3) (13)], [5, (41)], [6, (5) (17)], [7, (2) (3)^2 (5)], [8,
(2)^3 (3)], [9, (67)], [10, (5) (13)], [11, (3) (17)], [12, (2) (3)^3], [13, (3) (5)^2], [14, (2)^2 (5)],
[15, (3) (13)], [16, (71)], [17, (3) (31)], [18, (3)^2 (5)], [19, (2)^2 (3)], [20, (2)^2 (3) (7)]]
> with(LinearAlgebra[Modular]):
> M:=Mod(100,Matrix([[0,0,0,1],[3,0,1,0],[0,1,2,0],[3,1,0,0]]),integer[]):
M := 
$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 3 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 3 & 1 & 0 & 0 \end{pmatrix}$$

> MI:=Inverse(100,M);
MI := 
$$\begin{pmatrix} 0 & 78 & 11 & 89 \\ 0 & 66 & 67 & 34 \\ 0 & 67 & 67 & 33 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

> b:=Mod(100,Matrix(4,1,[1,3,13,8]),integer[]):
b := 
$$\begin{pmatrix} 1 \\ 3 \\ 13 \\ 8 \end{pmatrix}$$

> Multiply(100,MI,b);
Multiply(100,MI,b) := 
$$\begin{pmatrix} 89 \\ 41 \\ 36 \\ 1 \end{pmatrix}$$

> seq([k,ifactor(7^k+25 mod 101)],k=1..20);
[[1, (2) (37)], [2, (13)], [3, (7) (13)], [4, (31)], [5, (3) (5)], [6, (2)^2], [7, (2)^2 (7)], [8, (5) (19)],
[9, (59)], [10, (3)^2], [11, (3)^2 (7)], [12, (37)], [13, (3) (19)], [14, (2)^3 (3)], [15, (2) (3) (11)],
[16, (2) (29)], [17, (2)], [18, (2) (7)], [19, (2) (7)^2], [20, (2)^4 (5)]]
> x:=(41+36-5) mod 100;
x := 72
> 7^x mod 101;
25
> IndexCalc:=proc(a,b,q,F) local B,M,MI,k,l,f,LOGS,logseq;
with(numtheory); with(padic):
```

Index kalkulus

```

> with(LinearAlgebra[Modular]):
> B:=Mod(q-1,Matrix(nops(FB),1),integer[]):
> M:=Mod(q-1,Matrix(nops(FB),nops(FB)),integer[]):
> M1:=M;
> k:=1; l:=1; r:=(seq(Rank(p,M1),p=factorset(q-1)));
> while add(s,s=(seq(Rank(p,M),p=factorset(q-1)))<nops(factorset(q-1))*nop(
FB) do
> if evalb(factorset(a*k mod q) subset FB) then M1[1]:=Mod(q-1,Matrix[1..1,nop(
FB),[seq(OrdP(a*k mod q,f),f=FB)]],integer[]); print(M1,r,[seq(Rank(p,
M1),p=factorset(q-1))],l,k); end if;
> if add(s,s=[seq(Rank(p,M1),p=factorset(q-1))])-add(s,s=r)=nops(factorset(
q-1)) then M:=M1; B[1]:=k; l:=l+1; r:=(seq(Rank(p,M1),p=factorset(q-1)))
end if; k:=k+1;
> end do;
> M; print(FB); LOGS:=Multiply(q-1,Inverse(q-1,M),B); print(LOGS);
> k:=1; while not evalb(factorset((a*k*b) mod q) subset FB) do
> k:=k+1; print(k); print(factorset((a*k*b) mod q));
> end do;
> logseq:=[seq(OrdP((a*k*b) mod q,f),f=FB)]; print(logseq);
> (add(k,k=[seq(LOGS[t..1]*logseq[t],t=l..nops(LOGS))-k]) mod (q-1));
> end proc;
indexCalc:=proc(a,b,q,FB)
local B, M, M1, s, l, r, LOGS, logseq;
with(modntheory);
with(padic);
with(LinearAlgebra[Modular]);
B:= LinearAlgebra:-Modular`>Mod(q-1,Matrix(nops(FB),1),integer[] );
M:= LinearAlgebra:-Modular`>Mod(q-1,Matrix(nops(FB),nops(FB)),integer[] );
M1:=M;
k:=1;
l:=1;
r:=(seq('LinearAlgebra:-Modular`>Rank(p,M1),p=modntheory:-factorset(q-1)) );
while add(s,s=[seq('LinearAlgebra:-Modular`>Rank(p,M1),p=modntheory:-factorset(q-1)) ]
< nops(modntheory:-factorset(q-1))*nop(FB) do
if evalb(subset(modntheory:-factorset(mod(a*k,q)),FB)) then
M1[1]:=LinearAlgebra:-Modular`>Mod(q-1,Matrix[1..1,nops(FB),[seq(padic:-ordP(mod(a
*q),q,f),f=FB)]],integer[] );
print(M1,r,[seq('LinearAlgebra:-Modular`>Rank(p,M1),p=modntheory:-factorset(q-1)) ],
l,k);
end if;
if add(s,s=[seq('LinearAlgebra:-Modular`>Rank(p,M1),p=modntheory-
factorset(q-1))])-add(s,s=r)=nops(modntheory:-factorset(q-1)) then
M:=M1;
B[1]:=k;
l:=l+1;
r:=(seq('LinearAlgebra:-Modular`>Rank(p,M1),p=modntheory:-factorset(q-1)) );
end if;
if add(s,s=[seq('LinearAlgebra:-Modular`>Rank(p,M1),p=modntheory-
factorset(q-1))])-add(s,s=r)=nops(modntheory:-factorset(q-1)) then
M:=M1;
B[1]:=k;
l:=l+1;
r:=(seq('LinearAlgebra:-Modular`>Rank(p,M1),p=modntheory:-factorset(q-1)) );
end if;
end while;
end proc;

```

Index kalkulus

```
end if;
k:=k+1
end do;
M;
print(FB);
LOGS:= `LinearAlgebra:-Modular`-Multiply(q-1, `LinearAlgebra:-Modular`-Inverse(q-1, M), B);
print(LOGS);
k:=1;
while not evalb(subset(numtheory:-factorset(mod(a^k*b, q)), FB)) do
  k:=k+1; print(k); print(numtheory:-factorset(mod(a^k*b, q)))
end do;
logseq:=[seq(padic:-ordp(mod(a^k*b, q), f)=FB)];
print(logseq);
modi add(k, k=[seq(LOGS[t, 1]*logseq[t], t=1..nops(LOGS))]) ->k, q-1)
end proc
> IndexCalc(7,24,101,{2,3,5,7,11}):
[ 0 0 0 1 0 ]
[ 0 0 0 0 0 ]
[ 0 0 0 0 0 ] -> [0,0],[1,1],1,1
[ 0 0 0 0 0 ]
[ 0 0 0 0 0 ]
[ 0 0 0 1 0 ]
[ 0 0 0 2 0 ]
[ 0 0 0 0 0 ] -> [1,1],[1,1],2,2
[ 0 0 0 0 0 ]
[ 0 0 0 0 0 ]
[ 0 0 0 1 0 ]
[ 3 0 1 0 0 ]
[ 0 0 0 0 0 ] -> [1,1],[2,2],2,3
[ 0 0 0 0 0 ]
[ 0 0 0 0 0 ]
[ 0 0 0 1 0 ]
[ 3 0 1 0 0 ]
[ 1 2 1 0 0 ] -> [2,2],[2,3],3,7
[ 0 0 0 0 0 ]
[ 0 0 0 0 0 ]
```

Index kalkulus

$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$, [2,2], [3,3], 3, 8

$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$, [3,3], [3,4], 4, 12

$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$, [3,3], [4,4], 4, 13

$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 \end{bmatrix}$, [4,4], [4,4], 5, 14

$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \end{bmatrix}$, [4,4], [4,4], 5, 18

$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \end{bmatrix}$, [4,4], [4,4], 5, 19

$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \end{bmatrix}$, [4,4], [4,4], 5, 20

Index kalkulus

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \end{bmatrix}, [4, 4], [4, 4], 5, 23$$

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 \end{bmatrix}, [4, 4], [5, 5], 5, 24$$

(2, 3, 5, 7, 11)

$$\begin{bmatrix} 89 \\ 41 \\ 36 \\ 1 \\ 57 \end{bmatrix}$$

2

{5, 13}

3

{3, 17}

4

(2, 3)

[1, 3, 0, 0, 0]

8

Elliptikus görbék - összeadás

Elliptikus görbe

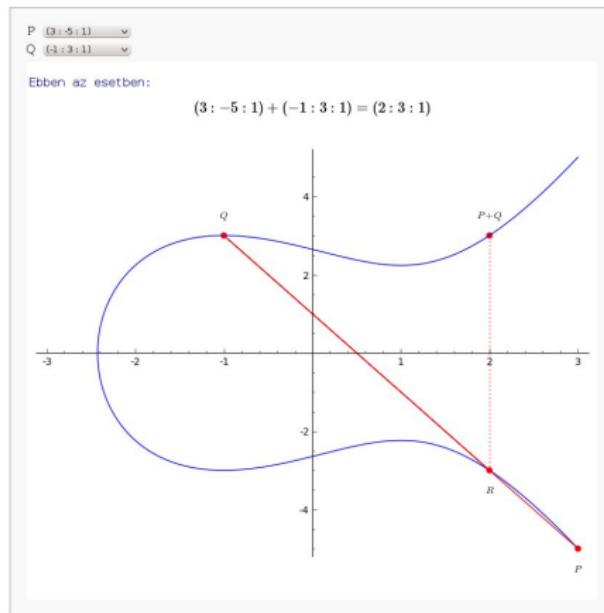
$$E : \quad y^2 = x^3 + ax + b$$

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

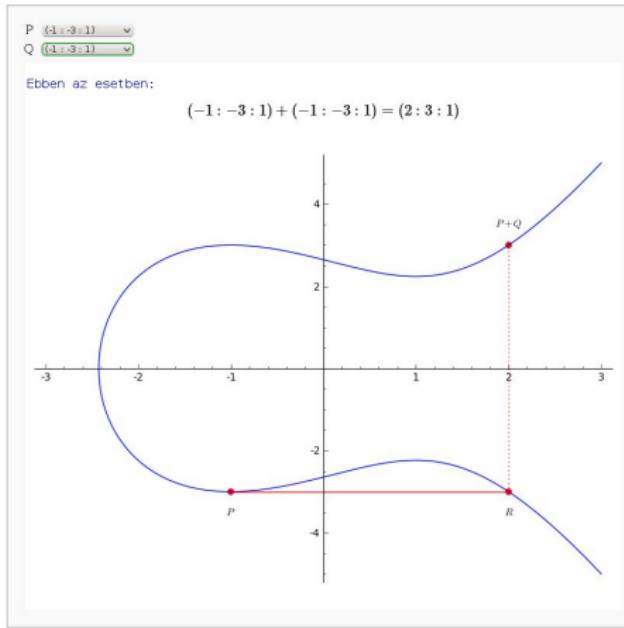
A görbe pontjain bevezetünk egy összeadás műveletet.

Elliptikus görbék - összeadás

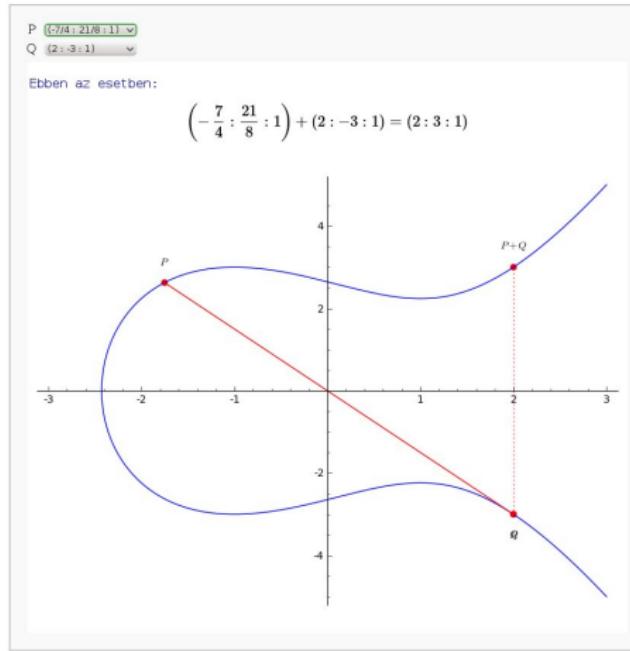
$$y^2 = x^3 - 3x + 7$$



Elliptikus görbék - összeadás



Elliptikus görbék - összeadás



Elliptikus görbék - összeadás

P $(2 : 3 : 1)$ ▾
Q $(2 : -3 : 1)$ ▾

Ebben az esetben:
 $(2 : 3 : 1) + (2 : -3 : 1) = (0 : 1 : 0)$

azaz a két pont összege a végtelen távoli pont.

Most bemutatjuk hogyan lehet a Maple segítségével az összeadást elvégezni adott elliptikus görbék esetében. A módszer működik \mathbb{Z}_N felett is, de összetett N esetében előfordulhat, hogy nem tudunk kiszámítani bizonyos nevezőket. Ezt fel tudjuk használni faktorizációra.

Elliptikus görbék - összeadás

```
> elliptic_add := proc(p1,p2,E) local g,inv,x1,x2,x3,y1,y2,y3,a,b,n;
  x1 := p1[1]; x2 := p2[1]; y1 := p1[2]; y2 := p2[2];
  a := E[1]; b := E[2]; n := E[3];

  if (x1=-infinity and y1=-infinity) then [x2,y2];
  elif (x2=infinity and y2=infinity) then [x1,y1];
  elif (x1=x2 and y1 <> y2) then [infinity,infinity];
  elif (x1=x2 and y1+y2 and y1<>0) then
    g := igcdex(2*y1,n,inv);
    if g = 1 then
      x3 := ((3*x1^2+a)*inv)^2-2*x1 mod n;
      y3 := ((3*x1^2+a)*inv)*(x1-x3)-y1 mod n;
      [x3,y3];
    else g; end if;
  elif (x1=x2 and y1=y2 and y1=0) then
    [infinity,infinity];
  else
    g := igcdex(x2-x1,n,inv);
    if g = 1 then
      x3 := ((y2-y1)*inv)^2-x1-x2 mod n;
      y3 := (y2-y1)*inv*(x1-x3)-y1 mod n;
      [x3,y3];
    else g; end if;
  end if;
end proc;
elliptic_add:=proc(p1,p2,E)
local g,inv,x1,x2,x3,y1,y2,y3,i,a,b,n;
x1:=p1[1];
x2:=p1[2];
y1:=p1[3];
y2:=p2[2];
y3:=p2[3];
i:=p2[1];
a:=E[1];
b:=E[2];
n:=E[3];
if x1=-infinity and y1=-infinity then
  [x2,y2];
elif x2=-infinity and y2=-infinity then
  [x1,y1];
elif x1=x2 and y1<>y2 then
  [infinity,infinity];
elif x1=x2 and y1=y2 and y1<>0 then
  g:=igcdex(2*y1,n,inv);
  if g = 1 then
    x3:=mod((3*x1^2+a)^2*inv^2-2*x1,i);
    y3:=mod((3*x1^2+a)*inv
              *(x1-x3)-y1,i);
    [x3,y3];
  else
    g;
  end if;
  if x1=x2 and y1=y2 and y1=0 then
    [infinity,infinity];
  else
    g:=igcdex(x2-x1,n,inv);
  end if;
end if;
end proc;
```

Elliptikus görbék - pont többszöröse

```
if g = 1 then
    x3 := mod((y2-y1)^2 * inv^2 - x1 - x2, n); y3 := mod((y2-y1) * inv
    *(x1-x3)-y1, n);
    [x3,y3]
else
    g
end if
end if
end proc;
> elliptic_mul := proc(p1,k,E) local pn,ps,d,r;
pn := p1; r := irem(k,2);
if r = 1 then ps := p1; else ps := [infinity,infinity]; end if;
d := (k-r)/2;

while (d > 0 and (not (type(ps,integer) or type(ps,integer)) and (pn <>
[infinity,infinity])))) do
r := irem(d,2);
pn := elliptic_add(pn,pn,E);
if r = 1 then ps := elliptic_add(ps,pn,E); end if;

d := (d-r)/2;
end do;

if type(pn,integer) then pn;
else ps; end if;
end proc;
elliptic := proc(p1,k,E)
local pn,ps,d,r;
pn := p1;
r := irem(k,2);
if r = 1 then ps := [infinity,infinity]; end if;
d := 1/2^(k-1)*1/2^r;
while 0 < d and (not (type(ps,integer) or type(ps,integer)) and pn <>[infinity,infinity]) do
r := irem(d,2);
pn := elliptic_add(pn,pn,E);
if r = 1 then ps := elliptic_add(ps,pn,E); end if;
d := 1/2^(k-1)*d-1/2^r;
end do;
if type(ps,integer) then pn else ps end if
end proc;
> N:=
10628080253478339771393136453028132434200582652706852594290946888153648140075413497;
38517055811826139684918212890689
> elliptic_mul([0,1],2^3*5^7*11^13*17^19,[21,1,N]);
12653
> N mod 12653;
0
> N/12653;
839965245671251068631402549041976798719717272797506725226503571391398467873827654518704;
699132084201128974805413
> k:=1; while nops(elliptic_mul([0,1],2^3*5^7*11^13*17^19*[21,1,N]))<>1 do k:=k+1; end do;
[k,1,N/12653]]<>1 do k:=k+1; end do;
k:=1
```



Elliptikus görbék - faktorizáció

```
          31
          > elliptic_mul([0,1],2+3+5+7+11+13+17+19+23+29+31+37+41+43,[31,1,N/(12653)]);
          136573
          > k:=1; while nops(elliptic_mul([0,1],2+3+5+7+11+13+17+19+23+29+31+37+41+43
          [k,1,N/(12653+136573)]))<>1 do k:=k+1; end do;
          k := 1
          > k;
          131
          > elliptic_mul([0,1],2+3+5+7+11+13+17+19+23+29+31+37+41+43,[131,1,N/(12653+
          136573)]);
          8909
          > N/(12653+136573+89009);
          69975336279659420330852565411677475191672511680407054887907340368896259443260421405
          056566099610009
          > k:=1; while nops(elliptic_mul([0,1],2+3+5+7+11+13+17+19+23+29+31+37+41+43
          [k,1,N/(12653+136573+89009)]))<>1 do k:=k+1; end do;
          k := 1
          > k;
          161
          > elliptic_mul([0,1],2+3+5+7+11+13+17+19+23+29+31+37+41+43,[161,1,N/(12653+
          136573+89009)]);
          929501
          > N/(12653+136573+89009+929501);
          7433831015551994245625672834837312466314631963942808098699064415642036923676728976538384
          63494509
          > k:=1; while nops(elliptic_mul([0,1],2+3+5+7+11+13+17+19+23+29+31+37+41+43
          [k,1,N/(12653+136573+89009+929501)]))<>1 do k:=k+1; end do;
          k := 1
          > k;
          376
          > elliptic_mul([0,1],2+3+5+7+11+13+17+19+23+29+31+37+41+43,[376,1,N/(12653+
          136573+89009+929501)]);
          2500297
          > N/(12653+136573+89009+929501+2500297);
          297317919253272481054277665206865929809351434626689588756481496255059668382087798854881
          . 97
```