

EÖTVÖS LORÁND TUDOMÁNYEGYETEM

Természettudományi Kar

Számelméleti gondolkodás lehetőségei a matematikai szemlélet fejlesztésében

Szakedolgozat

Vas Vivien

Matematika–Kémia tanár
osztatlan tanári mesterszak

Témavezető:

Szabó Csaba

Algebra és Számelmélet tanszék



2020.

EREDETISÉGI NYILATKOZAT

Alulírott Vas Vivien (UEU2K8) ezennel kijelentem és aláírással megerősítem, hogy az ELTE – Matematika – Kémia osztatlan tanári mesterszakján írt jelen diplomamunkám saját szellemi termékem, melyet korábban más szakon még nem nyújtottam be szakdolgozatként és amelybe mások munkáját (könyv, tanulmány, kézirat, internetes forrás, személyes közlés stb.) idézőjel és pontos hivatkozások nélkül nem építettem be.

Budapest, 2020. május 12.

Vas Vivien s. k.

Aláírás

Tartalomjegyzék

1. A dolgozat felépítése	5
2. A kísérlet	7
2.1. Bevezetés	7
2.2. Számelmélet oktatás helyzete a közoktatásban	8
2.3. Problémamegoldás	9
2.4. A kísérlet leírása	9
2.4.1. A kísérlet szempontjai	9
2.4.2. Az iskolák leírása	11
2.4.3. A feladatok koncepciója	11
2.4.4. Pontozás, javítás	14
2.4.5. Ellenőrzés	15
2.4.6. A kísérlet előkészületei	15
2.5. Kísérlet a gyakorlatban	16
2.5.1. Első rész	16
2.5.2. Második rész	17
2.5.3. Harmadik rész	18
2.5.4. Negyedik rész	19
2.6. Eredmények	19
2.7. A kísérlet alkalmazása a digitális oktatás keretei között	24
3. Magasabb fokú diofantikus egyenletek	31
3.1. Bevezetés	31
3.1.1. Körosztási polinomok számelmélete	31
3.2. Feladatok	32
3.3. Feladatok készítése	36
3.3.1. Alapfeladat	36
3.3.2. A mi feladatunk	37
3.3.3. Második feladatunk	44
3.3.4. Harmadik feladatunk	47
3.3.5. Meddig érdemes az egyenleteinket vizsgálni?	50

1. fejezet

A dolgozat felépítése

Dolgozatunk két részből áll. A két rész összekötő eleme a számelmélet. Az első rész egy matematika tanítási kísérletet mutat be, amelyben általános iskolás diákok számelméleti feladatokkal foglalkoznak. A második részben egy IMO-SHORTLIST feladatból kiindulva számelméleti feladatokat készítünk, és körbejárjuk egy megoldás technikai korlátait. Mindkét fejezetnek külön bevezetése van. A hivatkozásokhoz ahol tudtuk, odaírtuk az internetes elérhetőséget is.

2. fejezet

A kísérlet

2.1. Bevezetés

„A matematika a tudományok királynője, és a matematika királynője a számelmélet.”
(G. F. Gauss)

A magyarországi matematikaoktatás köztudottan problémaközpontú. A problémamegoldásra úgy is tekinthetünk, mint egy eszközre, ami által fejlődhet az általános matematikai gondolkodásunk. A matematikatanítás egyik fő célja, hogy fejlesszük a diákok problémamegoldó képességét [17]. Magyarországon több olyan tudós is foglalkozott a problémamegoldó képesség fejlesztésével, akinek módszere világhírű lett[1],[20].

Általában az emberi gondolkodás fejlődésének mértéke, csakúgy, mint a problémamegoldó képesség fejlődése számos tényezőtől függ, például a kívülről jövő segítség minőségétől és fajtájától [14], vagy hogy milyen típusú, milyen témakörhöz kapcsolódó feladatot oldunk meg. A középiskolai matematika tananyag nagyon sok területet ölel fel, így a tanárok változatos feladatokat készíthetnek és szabadon választhatnak a feladatok közül. Mégis, amikor tanítunk, általában egyszerre csak egy témakörrel foglalkozunk, és a problémamegoldás során nincs lehetőség változatos feladatokkal fejleszteni a diákok képességeit. A középiskolai tananyagban a számelmélet témaköre kis súllyal szerepel. A számelmélet a matematikának az a területe, ahol a legkülönbözőbb ötletekkel, legváltozatosabb feladattípusokkal találkozunk az egyszerű órai feladatoktól az olimpiai versenyfeladatokig.

Ezért kezdtük el vizsgálni, hogyan hathatnak a számelmélettel kapcsolatos feladatok a közoktatásban tanuló diákok gondolkodásának fejlődésére, általános matematikai gondolkodására. Egy kísérletet terveztünk, amely a számelmélettel való ismerkedést, számelméleti feladatok megoldását összeköti az általános matematikai problémamegoldó képességgel. A kísérletben hetedik és nyolcadik osztályos tanulók vettek részt. A kísérletben szereplő diákokat két részre osztottuk, egy kísérleti és egy kontroll csoportra. A kísérleti csoport diákjai minden óra elején egy számelmélettel kapcsolatos feladatot oldottak meg, a másik csoport tagjai a reguláris tananyaggal kapcsolatosan kaptak feladatot. A kísérlet eredményességét a

reguláris tananyaggal kapcsolatos dolgozatokkal, és olyan szintfelmérőkkel vizsgáltuk, melyekben a számelmélet témaköre nem szerepelt.

A dolgozat elején bemutatjuk a számelmélet matematika oktatásban való helyzetét, a NAT által megfogalmazott kulcskompetenciákat, melyek munkánk szempontjából kiemelkedően fontosak. Utána ismertetjük a kísérletben szereplő iskolákat, a kísérlet koncepcióját, menetét és felhasználhatóságát a digitális oktatás keretei között is. A végén összefoglaljuk a kísérlet eredményeit és a következtetést.

2.2. Számelmélet oktatás helyzete a közoktatásban

A számelmélet témaköre az egész általános iskolát végigkíséri. A magyar diákok már alsó tagozatban találkoznak a páros és páratlan számok, többszörös, osztó és a maradék fogalmával. Felső tagozat 5. osztályában már törtek összeadásával, kivonásával, egyszerűsítésével és bővítésével foglalkoznak. Törtek összeadásánál és kivonásánál célszerű a legkisebb közös nevezőt megtalálni, melyhez szükséges a legkisebb közös többszörös meghatározásának ismerete. Törtek egyszerűsítéséhez pedig a legnagyobb közös osztó meghatározásának ismeretére van szükségük.

Hétéves kor fölött mindenki képes absztrakt fogalmak elsajátítására [15], és ha Bruner spirális elve szerint építjük föl az iskolai tananyagot [3], akkor a tizenhárom éves diákok már érettek lesznek a tapasztalatok általános megfogalmazására. Felső tagozat 7. és 8. évfolyamában kibővítik az eddig tanult oszthatósági szabályokat. Átismétlik a prímtényező felbontást, a legnagyobb közös osztó és legkisebb közös többszörös kiválasztásának módszerét a pozitív egész számok nemnegatív egész kitevőjű hatványok alkalmazásával. Ezekkel párhuzamosan, általános iskola végén segítenünk kell a bizonyítás igényének kialakulását, hogy a későbbiekben képesek legyenek sejtések alapján, tételeket és definíciókat alkalmazni problémamegoldás során, és a korosztálynak megfelelő feladatok megoldását magyarázattal együtt megadni.

Láthattuk, hogy általános iskolában szinte folyamatosan foglalkozunk a számelmélet témakörével, középiskolában azonban a 9. évfolyam néhány órájától eltekintve szinte semmit [13]. A szaktanár dönthet úgy, hogy 12-ben az érettségi előtt röviden átismétli ezt a témakört, de ez is csak néhány plusz tanórát jelent. Ennek az lehet az oka, hogy mind a középszintű érettségien és mind az emelt szintű érettségien kevés számelmélettel kapcsolatos feladat van, és ezek nagyrésze az általános iskolai ismeretekkel megoldható. Elmondhatjuk tehát, hogy a számelmélet témakörét elhanyagolják a középiskolai matematikaoktatás során [5]. Ennek ellenére kevés olyan matematikaversennyel találkozunk, ahol ne fordulna elő számelméleti feladat. Ennek az lehet az oka, hogy a számelmélet a matematikának az a területe, ahol a legkülönbözőbb ötletekkel, legváltozatosabb feladattípusokkal találkozunk az egyszerű órai feladatoktól az olimpiai versenyfeladatokig. Emiatt ez a témakör alkalmassá válhat a diákok problémamegoldó képességének fejlesztésére is.

2.3. Problémamegoldás

„A matematikai kompetencia a matematikai gondolkodás fejlesztésének és alkalmazásának, az elvonatkoztatásnak és a logikus következtetésnek a képessége. Az arra való készséget is jelenti, hogy a mindennapi problémák megoldása során matematikai ismereteket és módszereket alkalmazzunk. A matematikai kompetencia képessé tesz arra, hogy felismerjük az alapvető matematikai elveket és törvényszerűségeket a természetben. Elősegíti a problémák megoldását a mindennapokban, otthon és a munkahelyen. Alkalmassá tesz az érvek láncolatának követésére, a matematika nyelvén megfogalmazott törvények megértésére. [17]”

Kutatásunkban a NAT kulcskompetenciái közül a problémamegoldást emeljük ki. A magyarországi matematikaoktatás problémaközpontú, nagy hangsúlyt fektetünk a problémafelismerés és a problémamegoldás kompetenciáinak fejlesztésére. Kimutatták, milyen előnyöket jelent a hétköznapi életben, ha jól tudunk problémát megoldani.

Magyarországon számos tankönyv, feladatgyűjtemény és versenyfeladatgyűjtemény áll rendelkezésünkre, melyek segítségével rendszeresen adhatunk problémákkal kapcsolatos feladatokat diákjainknak. Ennek ellenére a diákok problémamegoldó képessége nem elég fejlett, így egyetemre érkezésükkor hátrányba kerülnek, hisz nem rendelkeznek a feladatmegoldáshoz szükséges kompetenciákkal. Ezen kompetenciák javítása érdekében hoztuk létre kísérletünket. Azt szeretnénk volna megmutatni, hogy a számelmélet feladatoknak köszönhetően a diákok eredményei a matematika több területén is javulnak.

2.4. A kísérlet leírása

2.4.1. A kísérlet szempontjai

Egy kísérlet eredményességéhez több szempontot figyelembe kell vennünk, hogy az eredmény értékelhető legyen. Elronthatja az értékelhetőséget például ha

- a diákok motiválatlanok,
- nincs kontroll csoport,
- más szaktanár tanít az egyes csoportokban,
- különböző iskolákat hasonlítunk össze egymással,
- különböző képességű diákokat hasonlítunk össze egymással.

A kísérlet minél hosszabb távon való hatását szeretnénk volna vizsgálni, ezért a feladatok összeállításánál fontos szempont volt, hogy legalább három hónapra elegendő feladatot gyűjtsünk össze. A koncepciónk az volt, hogy összegyűjtünk 15 – 20 versenyfeladatot, melyek között voltak könnyebben és nehezebben megoldhatóak is. Amikor ezeket kiválasztottuk nehézségtől függően rávezető feladatokat készítettünk, a könnyebben megoldható

feladatokhoz 1 – 2-t, a nehezebben megoldhatóakhoz 3 – 4 feladatot. Az azonos témakörbe tartozó feladatokat nehézség szerint sorrendben egymás után helyeztük el, így a feladatso-ron belül blokkok alakultak ki. Ezeket a blokkokat azonos típusú feladatokkal választottuk el egymástól. Így összesen 63 feladatunk lett. A feladatokat 7-10. osztályos tanulóknak egyaránt ajánljuk, de mi 7. és 8. évfolyamos diákokon teszteltük az eredményt.

Tapasztalataink alapján a szaktanárok többsége nem szívesen vesz részt a kísérletekben. Véleményünk szerint ennek egyik legfőbb oka, hogy úgy gondolják a kísérletben való rész-vétel sok plusz munkával jár, ezen kívül félnek attól, hogy összehasonlítyák őket a kísérlet-ben részt vevő többi pedagógussal. Így arra törekedtünk, hogy az osztályban tanító szakta-nároknak minél kevesebb feladata legyen a kísérlettel kapcsolatosan, munkájukat segítsük amennyire csak lehet. A kísérletben négy osztály vett részt, melyek közül az egyiket én tanítom, a másik három osztályt három különböző matematikatanár.

A módszer hatékonyságát, azaz a diákok fejlődésének mértékét úgy próbáltuk meg fel-mérni, hogy az ne függjön a képességbeli különbségektől, és a tárgyat tanító tanártól sem. Azaz úgy kellett kísérleti és kontroll csoportot választanunk, hogy ne legyen nagy tudás- és képességbeli különbség a két csoport között. Az iskolában adja magát az ülésrend szerinti kettéosztás: minden osztályban a padsor egyik fele a kísérleti, a padsor másik fele a kont-roll csoportba került. Így a tárgyat tanító tanártól sem függ az eredmény, hiszen minden osztályon belül van egy kísérleti és egy kontrollcsoportunk azonos tanárral.

Számos kísérletről lehet hallani, hogy az eredmény nem értékelhető megfelelően, mert a diákok motivátlanságukból adódóan nem vesznek benne részt. Ezért a kísérletünk előtt fontos szempont volt ennek a kiküszöbölése is. Magyarországon a közoktatásban tanuló diákoknak nem jelent elég motivációt a tudás elsajátítása, ezért motivációként jó osztályzatok megszerzése mellett döntöttünk. Azért, hogy aktivitásukat fentartsuk, négy részre osztottuk a feladatokat, és minden rész teljesítése után ötöst szerezhettek az a diák, aki elérte az általunk megállapított pontszámot. Ez általában az összpontszám 50%-át jelentette, hiszen az volt a célunk, hogy minél motiváltabbak legyenek.

Fontos, hogy a diákok ne tudják, miről szól a kísérlet, ezért a kontroll csoportban lé-vők is kaptak feladatokat. Olyan feladatot kellett kapniuk, ami a kísérlet szempontjából nem befolyásolja az ő leendő agyi tevékenységüket vagy kognitív képességeiket. Így azalatt az idő alatt, amíg a kísérleti csoport számelmélet feladatokat oldott meg, addig a kontroll csoportnak tananyaggal kapcsolatos feladatokat kellett megoldania. Azaz a kontroll csoport diákjait minden órán tesztelték az aktuális tananyagból. Az előhívási hatásról ismert, hogy nagy mértékben segíti a reguláris tananyag elsajátítását, tehát a kontroll csoportot biztosan fejlesztettük az alatt az idő alatt, amíg a kísérleti csoport diákjai számelmélettel foglalkoztak. Összességében a kontroll csoport diákjai heti 20 – 25 perccel többet foglalkoztak a reguláris tananyaggal, mint a kísérleti csoport diákjai. Az, hogy valamilyen tevékenységet végezzen a másik csoport is, pszichológiai szempontból reálisabbá teszi a kísérletet, mert így nem tudják melyik csoportnak kellene jobban fejlődnie, csak azt tudja mindenki, hogy szerepel

a kísérletben. A tanárok sem tudták melyik csoporttól várunk nagyobb mértékű fejlődést, ráadásul nem is tudták az osztályokat tovább tanítani, mert nem tudták a két csoportot megkülönböztetni óra közben. Így a kísérletben tényleg azt mértük fel, amit szerettünk volna.

2.4.2. Az iskolák leírása

Egy átlagos (Szigetszentmiklós Bíró Lajos Általános Iskola) és egy elit általános iskola (Budapesti Fazekas Mihály Gyakorló Általános Iskola és Gimnázium) 7-es és 8-os diákjai vettek részt a kísérletben, mindkét iskolából 2-2 osztály.

A Bíró Lajos Általános iskolában a diákok a 7. és 8. évfolyamon a matematikát csoportbontásban tanulják. Az iskolában a matematika tudásszint alapján sorolják csoportba a gyerekeket az ötödik évfolyam kezdetén. Az évfolyam négy osztályából négy csoportot alakítanak. Az évek folyamán a csoportokba való átjárás a tudásszint változásával megengedett. A kísérleti csoport az iskola hetedik és nyolcadik osztály legjobb csoportjának egyik fele volt. Minden osztályban véletlenszerűen osztották szét a gyerekeket, az osztály egyik fele számelmélet feladatokat kapott, a másik fele tananyaggal kapcsolatosakat. A kontroll csoport tehát mindkét évfolyamon az osztály másik fele volt.

A Budapesti Fazekas Mihály Általános iskola és Gimnáziumban a diákok a 7. és 8. évfolyamon a matematikát egész osztályban tanulják. A kísérleti csoport az iskola egy olyan hetedik osztályának fele volt, akiket a mentorom tanít, és egy olyan nyolcadikos osztály fele, akiket én. A kontroll csoport mindkét évfolyamon a csoport másik fele volt.

A két iskola diákjainak szociális háttere nagyon eltérő. A Budapesti Fazekas Mihály Gyakorló Általános Iskola és Gimnázium egy rangos iskola, Budapest VIII. kerületében található, az elmúlt években a középiskolák rangsorában általában az 1. helyen szerepelt. Az általunk kiválasztott osztályok az intézmény általános iskolai tagozatához tartoznak. Ezzel szemben a Bíró Lajos Általános Iskola átlagosnak mondható. Vannak kiemelkedő, ugyanakkor hátrányos helyzetű diákok is. Mindkét iskolában az évfolyam a kerettantervnek megfelelő tananyagot tanulja. A szigetszentmiklói iskolában az osztályoknak heti öt matematika órája van, a budapesti iskolában heti négy.

2.4.3. A feladatok koncepciója

Azt szeretnénk volna, hogy a diákok eljussanak arra a szintre, hogy korosztályuknak megfelelő (számelméleti) versenyfeladatokat meg tudjanak oldani. A diákok általában erre nem képesek. Ennek az az oka, hogy a kerettantervben feltüntetett teljes alapóraszám négyötöd része az új ismeretek elsajátítására fordítódik. A fennmaradó órák felhasználhatók ismétlésre, gyakorlásra, felzárkóztatásra, tehetséggondozásra és számonkérésre. A szaktanár által szabadon rendelkeztetett óraszámok általában az ismétlésre, gyakorlásra, felzárkózásra, számonkérésre fordítódik, és a legtöbb esetben ezekre is kevés. Emiatt a diákok többsége nem, vagy csak alig találkozik versenyfeladatokkal általános-, és középiskolai tanulmányai során.

A feladatok megoldása során használt gondolatok nagyon hasznosak és később is tudják alkalmazni őket. Éppen ezért rávezető feladatokat készítettünk egy-egy blokkban, ezeket kellett megoldaniuk. Persze még mindig fennáll a veszélye, hogy a rávezető feladatokat sem tudják megoldani, ezért a diákok folyamatosan hozzáfértek a megoldásokhoz. Most felmerül a kérdés: "Miért érdekelné egy diákot a megoldás?" A diákok tudják, hogy a következő feladat erre a megoldásra lesz alapozva, jól akarnak teljesíteni, így beindítottunk egy tanulási folyamatot. Másrészt elértük, hogy az a diák, aki elakadt a folyamatban, behozza lemaradását, és a következő feladatokon már jól szerepelhessen. Tehát ahhoz, hogy a versenyfeladatot meg tudják oldani kellett az előző feladat megoldásai.

A számelmélettel kapcsolatos feladatokat különböző versenyekből válogattuk össze 7-8. évfolyamos diákok számára. Az összes feladatunk olyan volt, hogy már alaptudással és minimális logikai készséggel megértették volna a feladat jó megoldását, de még nem volt olyan problémamegoldási rutinjuk, vagy gondolati képességük, hogy ezeket maguktól meg tudják oldani, ezért kellett a rávezető feladatok. Figyeltünk arra, hogy ezek önmagukban is gondolkodtatóak legyenek.

Lentebb látunk egy mintafeladatsort. Észrevehetjük a feladatokon, hogy némelyik ugyanarra a sablonra épül. Ez azért volt fontos, hogy ha valaki egyszer elrontott egy feladattípust, utána tudja tovább gyakorolni, hiszen be is akartuk gyakoroltatni ezeket a feladatokat. Tehát nem az volt a célunk, hogy a diák kapott egy ötletet, amit egyszer látott és utána tudnia kell, hanem azt akartuk, hogy többször lássa, és megragadjon az ötlet a fejében. A 35 - 43. blokk egy jó mintafeladatsor arra, hogy bemutassuk egy blokkon belül, milyen rávezető feladatokon keresztül jut el a diák a versenyfeladathoz, és közben milyen ötletek jelennek meg. Különböző nagyságú kettő hatványról, három hatványokról, öt hatványokról kérdeztük végződéseiket. Megkapták a megoldásokat, majd megint kaptak ilyen feladatokat, de már magasabb kitevőre. Az utolsó feladat már egy versenyfeladat, melynek megoldásához az előző ötletek mindegyikét kellett használni.

35. Milyen számjegyre végződik 5^{2019} ? Segítség: Írd fel 5 hatványait, és nézd meg milyen számjegyre végződnek. Észreveszel valamit?

A feladat megoldása:

Az 5 bármely hatványa 5-re végződik, tehát 5^{2019} is 5-re végződik.

36. Milyen számjegyre végződik 2^{22} ? Segítség: Írd fel 2 hatványait, és nézd meg milyen számjegyre végződnek. Észreveszel valamit?

A feladat megoldása:

Észrevesszük, hogy 2, 4, 8, 6 végződéseket kapunk, melyek újra és újra ismétlődnek. $22 = 4 \cdot 5 + 2 \rightarrow$ Tehát ötször ismétlődik a leírt négy szám, majd leírunk még kettőt. Tehát 2^{22} végződése ugyanaz, mint 2^2 végződése, vagyis 4.

37. Milyen számjegyre végződik 3^{19} ? Segítség: Írd fel 3 hatványait, és nézd meg milyen számjegyre végződnek. Észreveszel valamit?

A feladat megoldása:

Azt vesszük észre, hogy 3, 9, 7, 1 végződéseket kapunk, melyek újra és újra ismétlődnek. $19 = 4 \cdot 4 + 3 \rightarrow$ Tehát négyszer ismétlődik a leírt négy szám, majd leírunk még hármat. Tehát 3^{19} végződése ugyanaz, mint 3^3 végződése, vagyis 7.

40. Milyen számjegyre végződik 2^{999} ? Segítség: Írd fel 2 hatványait, és nézd meg milyen számjegyre végződnek. Észreveszel valamit?

A feladat megoldása:

Azt vesszük észre, hogy 2, 4, 8, 6 végződéseket kapunk, melyek újra és újra ismétlődnek. $9999 = 4 \cdot 2499 + 3 \rightarrow$ Tehát 2499-szer ismétlődik a leírt négy szám, majd leírunk még hármat. Tehát 2^{9999} végződése ugyanaz, mint 2^3 végződése, vagyis 8.

41. Milyen számjegyre végződik 3^{1993} ? Segítség: Írd fel 3 hatványait, és nézd meg milyen számjegyre végződnek. Észreveszel valamit?

A feladat megoldása:

Azt vesszük észre, hogy 3, 9, 7, 1 végződéseket kapunk, melyek újra és újra ismétlődnek. $1993 = 4 \cdot 498 + 1 \rightarrow$ Tehát 498-szor ismétlődik a leírt négy szám, majd leírunk még egyet. Tehát 3^{1993} végződése ugyanaz, mint 3^1 végződése, vagyis 3.

42. Igazold, hogy $3^{202} + 5 \cdot 3^{210} + 1$ összetett szám! (Segítség: Nézd az öttel való maradékot.)

A feladat megoldása

$5 \cdot 3^{210}$ biztosan osztható 5-tel, tehát elég belátnunk, hogy $3^{202} + 1$ osztható. 3^{202} végződése ugyanaz, mint 3^2 végződése, vagyis 9, amihez 1-et adva 0-t kapunk. Az összeg osztható 5-tel is, tehát összetett szám.

43. Milyen számjegyre végződik $2^{101} + 3^{101} + 5^{101}$? (Segítség: Vizsgáld a tagokat külön-külön!)

A feladat megoldása:

Ehhez meg kell néznünk a tagokat külön-külön milyen számjegyekre végződnek.

A 2 hatványait felírva látjuk, hogy a 2, 4, 8, 6 végzések ismétlődnek négyesével. Nézzük $2^{101} \rightarrow 101 = 4 \cdot 25 + 1 \rightarrow$ Ez azt jelenti, hogy a négy leírt szám 25-ször ismétlődik, majd leírunk még egyet. Tehát 2^{101} utolsó számjegye ugyanaz, mint $2^1 = 2$.

A 3 hatványait felírva látjuk, hogy a 3, 9, 7, 1 végzések ismétlődnek négyesével. Nézzük $3^{101} \rightarrow 101 = 4 \cdot 25 + 1 \rightarrow$ Ez azt jelenti, hogy a négy leírt szám 25-ször ismétlődik, majd leírunk még egyet. Tehát 3^{101} utolsó számjegye ugyanaz, mint $3^1 = 3$.

Az 5 hatványait felírva látjuk, hogy minden 5 hatvány 5-re végződik, tehát 5^{101} utolsó számjegye 5. A $2^{101} + 3^{101} + 5^{101}$ utolsó számjegye $2 + 3 + 5 = 10$, tehát 0-ra végződik.

A fenti levezetésnél vigyáztunk, hogy ne legyen direkt a rávezetés, de mindegyik "kisebb feladathoz" kelljen egy új gondolat, és végül a "nagy feladathoz" minden ötletet fel kelljen használniuk.

A feladatok megoldásánál látszik az is, nem elég csupán a végeredmény. Ez javítja a kommunikációs készségüket, és látják, hogy is néz ki a részletes, precíz megoldás.

A feladatokat 4 részre osztottuk, és a fentebb említett koncepció alapján blokkokra osztottuk. Az azonos blokkba tartozó feladatok azonos típusúak. Azt szeretnénk volna, ha a diákok tudják mikor érkeznek egy blokk végére, emiatt a különböző blokkok között azonos típusú, szintén számelméleti feladatokat helyeztünk el. Ilyen például a következő feladat:

$$\mathbf{51. \text{ Melyik a nagyobb? }} \quad (-0,99)^{100} \quad \text{vagy} \quad \frac{3^4 \cdot 4^4 \cdot 5^4}{60^4}$$

A feladat megoldása:

A $(-0,99)$ kitevője páros, tehát pozitív lesz a szám. A $0,99$ kisebb, mint 1 , ezért a 100 . hatványa is kisebb, mint 1 . A jobb oldalon szereplő tört nevezőjét felbontva: $60^4 = (3 \cdot 4 \cdot 5)^4 = 3^4 \cdot 4^4 \cdot 5^4$.

A tört számlálója és nevezője egyenlő, tehát a tört értéke 1 . Tehát a jobb oldali szám nagyobb.

Azért, hogy a diákok valóban részt vegyenek a kísérletben, motiválni kellett őket. A magyar diákoknál általában az a legjobb motiváció, ha ezért szerezhettek valami plusz pontot, vagy plusz lehetőséget.

2.4.4. Pontozás, javítás

A diákok munkáját osztályoztuk, hogy komolyan vegyék a feladatok megoldását. Figyeltünk arra, hogy minden diák motivált maradjon, ezért olyan osztályzási rendszert dolgoztunk ki, hogy a diákok végig motiváltak maradjanak. Azok is akiknek az elején nem sikerül olyan jól teljesíteni, és azok is, akiknek jól megy. Ezt úgy oldottuk meg, hogy a diákok az egyes feladatok megoldására nem érdemjegyet, hanem pontokat kaptak. A feladatokat négy részre osztottuk, és az összegyűlt pontokat minden rész végén összeadtuk. Azok a diákok, akik az adott rész végén elérték a megfelelő pontszámot, jelest kaptak. Ez általában a pontok 50%-át jelentette. Így azoknak a diákoknak is volt esélyük a jó osztályzat elérésére, akik az elején rosszul teljesítettek, akik pedig jól szerepeltek, több ötöst szerezhettek.

A kísérletünk egyik célja az volt, hogy a diákoknak minél gazdagabb ötlettára legyen, ezért a számelméleti feladatok javításánál a pontok nagy része a jó ötletek megjelenéséért járt, nem a megoldásért. Ezzel azt közvetítettük a diákok felé, hogy áldozzanak energiát a részletes leírásra, és legyen világos számukra, hogy a matematikában sokszor fontosabb az ötlet, mint a végeredmény. Ezt a diákokkal az első feladat előtt közöltük, és közben is elhangzott, hogy nem elég a végeredményt leírni. Azért, hogy egységes legyen a pontozás, mind a négy osztály feladatait én javítottam. Az első résznél a vezető tanárom ellenőrizte a javításom, utána erre nem volt szükség. A javítási útmutató a kísérlet kezdete előtt elkészült, ezért a feladatok javítása nem igényelt sok időt. A diákok számára elérhető volt egy táblázat, melyben az addig elért pontjaikat tudták ellenőrizni.

A kontrollcsoport az aktuális tananyaghoz kapcsolódó tankönyvi feladatot kapta. Ezekre ugyanannyi pontot szerezhettek, mint a kísérleti csoport tagjai az ugyanebben az időben írt feladataikra. Tehát az adott órán írt számelmélet feladatra adható maximális pontszám megegyezett a tankönyvi feladatra adható maximális pontszámmal. A reguláris tananyaghoz kapcsolódó feladatok magyarázatát meg lehetett beszélni közvetlen a feladat megoldása után (amennyiben erre szükség volt), hiszen ez az aktuális tananyaghoz kapcsolódott. Ahhoz, hogy a fejlődés mértékét fel tudjuk mérni, a számelmélet feladatok megbeszélése nem történhetett meg a tanórán. Ez nehézséget okozott, de megtaláltuk a megoldást. A kísérleti csoport minden feladatához tartozott egy kód, amit a feladat megoldása után kaptak meg az órát tartó pedagógustól. A kód ismeretében a www.vasvivien.com honlapon a diákok ellenőrizhették a helyes végeredményt, és megnézhatték az ehhez vezető gondolatmenetet is.

2.4.5. Ellenőrzés

A feladatok megoldásait feltöltöttük a www.vasvivien.com honlapra → Diákjainnak → Versenyfeladatok.

Ezen az oldalon megjelenik az összes feladat, mindegyik külön linkkel. Amikor megnyitunk egy feladatot, a készülék automatikusan letölti azt, de megtekinteni csak a feladathoz kapott kóddal lehet. Minden feladathoz külön kód tartozik, melyet a tanárok megkaptak a feladatokkal együtt. Így a diákok akár óra végén le tudták ellenőrizni jól gondolkodtak-e. Azt is látták mi a helyes megoldás, és a tesztek kijavítása után az addig elért pontjaikat is meg tudták nézni. Ezzel azonnali visszajelzést kaptak a diákok a munkájukról, és az is látható volt, hogy mennyi pontra van még szükségük az ötös megszerzéséhez. Azt tapasztaltuk, hogy a diákok lelkesek voltak, és érdeklődők, hiszen minden óra után rögtön elővették a telefonjukat, hogy megnézzék az adott feladat helyes megoldását.

2.4.6. A kísérlet előkészületei

Törekedtünk arra, hogy a szaktanároknak minél kevesebb feladata legyen a kísérlettel kapcsolatosan. Éppen ezért minden lehetséges segítséget és dokumentumot biztosítottunk. A kísérlet kezdete előtt felkerestük a kísérletben szereplő szaktanárokat, odaadtuk a szükséges segédanyagokat, és pontosítottuk a kísérlet menetét. A szaktanárok megkapták:

- a feladatokat megoldással együtt,
- a kódokat tartalmazó táblázatot,
- a feladatokat egyesével, a szükséges darabszámban.

A kísérlet elején részt vettem minden osztály első óráján, és elmondtam a kísérlettel kapcsolatos információkat. Készítettünk egy tájékoztatót is a diákok számára, melyet a füze-

tükbe ragasztva kellett tárolni. A tájékoztatóban részleteztük milyen megoldásokat várunk, hol találják a megoldásokat, és hogy a sikeres teljesítés érdekében segítséget jelent, ha folyamatosan ellenőrzik a megoldást.

Ez a tájékoztató azért volt fontos, hogy a leglényegesebb információk, amik szóban elhangzottak, elérhetőek legyenek számukra az egész kísérlet alatt. Tapasztalataink alapján ez segítséget jelentett azokban az osztályokban, ahol nem én tanítottam. Sok üzenetet kaptunk a tájékoztatóban leírt e-mail címre a kódokkal és az aktuális pontszámokkal kapcsolatban, főleg a kísérlet elején.

2.5. Kísérlet a gyakorlatban

Most röviden összefoglaljuk a kísérlet alakulását és az egyes blokkok utáni tapasztalatokat. Úgy alakítottuk ki a kísérletet, hogy ne vegyen el sok időt az órából. A szaktanárok az aktuális feladattal, kóddal, és a kontroll csoport számára kiválasztott feladattal érkeztek a terembe. A jelentés után a hetesek kiosztották a számelmélet feladatokat a megfelelő diákoknak, a tanár pedig felírta a kontroll csoport tagjai által elvégzendő feladat számát a táblára. Pár perc gondolkodás után, mikor a tanulók kész voltak a feladatokkal, a tanár mindkét csoport munkáját beszedte, majd felírta a táblára az aznapi kódot. Így a kísérlettel kapcsolatos feladatok 5 – 10 percet vettek el az adott tanórából.

2.5.1. Első rész

Az első 15 feladatban a prímtényező felbontás, legnagyobb közös osztó, legkisebb közös többszörös, oszthatóság fogalma, osztási maradékokkal való számolás, skatulyaelv alkalmazása és kombinatorikával kapcsolatos feladatok szerepeltek.

Motiválásként a diákok bizonyos szint elérésekor jelest szerezhettek. Úgy döntöttünk ezt a szintet az adott rész végén határozzuk meg, hogy minél több diák kaphasson ötöst. A határt ennél a résznél úgy határoztuk meg, hogy a diákok fele kapjon ötöst. Ez azért volt jó, mert azok a diákok, akik ötöst kaptak még motiváltabbak lettek, akik nem kaptak, látták, hogy a szükséges szint elérése teljesíthető. Ez a szint a pontok 50%-át jelentette.

Volt néhány olyan diák, aki kiemelkedően jól teljesített mindkét típusú feladatnál. Úgy döntöttünk, ők két jelest érdemelnek. Döntésünket az indokolta, hogy azokat a diákokat, akik már az adott rész elején jól teljesítettek, tovább ösztönözzük.

Tapasztalataink

- Az első résznél a szaktanárokkal személyesen konzultáltunk minden héten, hogy halad a kísérlet, van-e bármilyen észrevételük vagy problémájuk a feladatokkal kapcsolatban. A válasz megnyugtató volt.

- A feladatok javításakor az első néhány feladatra általában minimális pontot kaptak a diákok. Ennek oka egyrészt az, hogy csak a végeredményt írták le, másrészt azoknál a feladatoknál, ahol több megoldás is volt, eggyel is megelégedtek.
- A diákokat érdekelte a megoldás, amit közvetlen az óra után meg is néztek.
- A megoldások érthetőek és kellően részletesek voltak, így utólagos magyarázatot és korigálást nem igényeltek.
- A legtöbb tapasztalat és visszaigazolás a saját osztályomtól érkezett. Többször említették azok a diákok, akik számelmélettel kapcsolatos feladatot kaptak, hogy jobban szeretnék a másik csoport feladatát írni, hiszen az sokkal könnyebb. Válaszomban kifejtettem, hogy ez egy kísérlet, mellyel segítenek nekünk, és már nem tudjuk megváltoztatni a csoportok felosztását.

2.5.2. Második rész

A második rész témakörei között az oszthatóság fogalma, oszthatósági szabályok, indirekt bizonyítás, hatványozás azonosságai, számok tizes számrendszerbeli alakjának értelmezése szerepeltek.

A jeleshez szükséges határokat az előző részben leírtak szerint határoztuk meg. Tehát a második rész feladatainak befejezésével alakítottuk ki a ponthatárt úgy, hogy a diákok fele kapjon ötöst. A diákoknak itt már volt viszonyítási alapja, mivel ez a határ 50% volt az előző résznél, tehát viszonylag könnyen elérhető. Ez azért volt meglepő a diákok számára, mert általában a dolgozatokhoz alakított százalékokhoz vannak hozzászokva, emiatt úgy gondolták ezeknél a feladatoknál sem lesz másképp. Miután megkapták az első rész eredményeit megnyugodtak, és még motiváltabbak lettek. Innentől kezdve a megoldással együtt a pontjaikat tartalmazó táblázatokat is folyamatosan nézték, hogy tudják az aktuális összpontszámukat.

Tapasztalataink

- Ettől a résztől kezdve minden héten telefonon és e-mailen keresztül konzultáltunk a szaktanárokkal, szükség esetén személyesen is.
- A diákok fejlődése már ennél a résznél érzékelhető volt, akár matematikai gondolkodásukat, akár érvelési és kommunikációs készségeiket tekintjük. A feladatok megoldásánál legtöbbször nem a megoldás szerepelt, hanem a megoldáshoz tartozó ötletek.
- Az egyik szaktanár jobbnak látta megváltoztatni a kísérlet kivitelezési módját. Innentől kezdve ez az osztály nem egy feladatot, hanem öt-hat feladatot írt egy órán. Ez jó tapasztalat arra, hogy a kísérlet kivitelezési módja nem csak rajtunk múlik, hiába

kommunikálunk pontosan. Viszont ha már így történt, próbáltuk a kialakult helyzetet a kísérlet javára fordítani, és úgy gondoltuk a végén levonhatjuk a következtetést, érdemes-e egyesével íratni a feladatokat.

- A második rész utolsó feladatánál az osztályom egy külön feladatot is kapott. A feladat megoldása mellé kellett írniuk mennyire találják nehéznek a feladatokat, és melyik típusú feladatot választanák, ha az ő döntésük lenne? A feladatok nehézségére 10-es skálát használtunk, ahol 1 volt a nagyon könnyű és 10 a nagyon nehéz. Azok a diákok, akik a reguláris tananyaggal kapcsolatos feladatokat oldották meg, általánosságban 4 – 5 nehézségűre, akik számelmélet feladatokat írtak 8 – 9 nehézségűre értékelték. A kísérleti csoport 10 diákja közül 9 magától is a számelmélet feladattal folytatta volna, és a kontroll csoport 9 diákja közül 6 inkább a számelmélet feladatot írta volna. A kísérleti csoport diákjainak válaszai megnyugtatóak voltak, hiszen az első résznél még a legtöbben cseréltek volna a másik csoport tagjaival. A kontroll csoportban levő diákoknak megígértük a kísérlet után ők is kapnak számelmélettel kapcsolatos feladatokat.

2.5.3. Harmadik rész

A 31 – 45. feladatok témakörei: adott szám többszöröseinek fogalma, oszthatósági szabályok alkalmazása, oszthatósági maradékokkal való számolás, hatványozás azonosságai, számok tízes számrendszerbeli alakja, összetett szám fogalma, prímhatványok végződése, periodikusság fogalma.

Ettől a résztől kezdve a ponthatárokat előre ismertettük:

- az a diák, aki eléri legalább az összpontszám 50%-át ötöst kap,
- az a diák, aki eléri legalább az összpontszám 90%-át két ötöst kap.

Ezt a ponthatárt az előző részek tapasztalatai alapján határoztuk meg. A tanulók az előző részek folyamata során többször kérdezték, hány ponttól kaphatnak majd ötöst, emiatt úgy gondoltuk segítséget jelent, ha előre tudják.

Tapasztalataink

- Ennél a résznél azt éreztük, elértük a diákoknál azt, hogy gondolkodjanak és precízen megadják egy adott feladat megoldását. Válaszaikban majdnem mindig leírták a feladathoz kapcsolódó elméletet (akár kérte a feladat, akár nem), a gondolatmenetüket érvekkel alátámasztva, és végül a megoldást. Azt vettük észre a diákoknak tetszenek ezek a feladatok, főleg most, hogy már sikerélményük is van.
- Abban az osztályban, ahol egy órán több feladatot oldottak meg, tapasztaltunk fejlődést, és szerepelt magyarázat is, de nem volt olyan precízen és logikusan megfogalmazva, mint a többi osztályban.

2.5.4. Negyedik rész

Az utolsó részt próbáltuk úgy összeállítani, hogy minden eddigi téma megjelenjen ezekben a feladatokban. Ez azért volt, hogy lássuk a feladatok megoldása mennyire mélyült el. Ezen kívül új téma is szerepelt: prímszámok fogalma, tíz feletti prímszámok végződése, prímszámok paritásából adódó tulajdonságok.

Tapasztalataink

- Ebben a részben az eddig gyengébben teljesítő diákoknál is tapasztalható volt a fejlődés.
- Annál a csoportnál, ahol a feladatokat nem egyesével írták nem tapasztaltunk olyan fejlődést, mint a többi osztálynál.
- Az osztályomban tanuló diákok elmondták mennyire tetszettek nekik ezek a feladatok. Tudják, hogy a kísérletnek vége, de szeretnék, ha ehhez hasonló feladatok írását továbbra is folytatnánk.
- A többi szaktanárnak is hasonló visszajelzést adtak diákjai.

2.6. Eredmények

A diákok húsz héten keresztül oldották meg a kísérlettel kapcsolatos feladatokat. A kísérlet alatt összesen négy dolgozatot írtak.

Az elején felmértük a kísérleti és a kontrollcsoportok diákjainak előzetes tudását és megvizsgáltuk, hogy eltérő matematikai képességekkel rendelkeznek-e a két csoport. Így a kísérleti és a kontrollcsoportoknak nem csak az eredményeit, hanem fejlődésük mértékét is fel tudtuk mérni. Ehhez összegyűjtöttük az azonos osztályba járó diákok tanév elején írt első témazáró dolgozatainak eredményeit (**Bemeneti mérés**). Ezt minden osztály akkor írta, amikor az osztályok felosztása már megtörtént (kísérleti, és kontroll csoport), de a kísérlet feladatait még nem kezdték el megoldani. A dolgozat témaköre a hetedik és a nyolcadik évfolyamon is algebra volt.

A második dolgozatot (**Függvények 1.**) a kísérlet 15. hetében írták a függvények témaköréből. A harmadik dolgozatot (**Szintfelmérő**) az utolsó számelmélet feladat beadása után egy héttel írták meg. Ebben olyan témájú feladatokat válogattunk össze, melyeket ebben a tanévben tanultak, de nem kapcsolódik a számelmélet témaköréhez. A negyedik dolgozatot (**Függvények 2.**) az utolsó számelmélet feladat beadása után 3 – 4 héttel írták a függvények témaköréből. Azért választottuk a függvényeket, mert olyan témából szerettük volna felmérni a diákok tudását, amit 2 – 3 hónappal ezelőtt tanultak, tehát még emlékeznek, de azóta már új téma is feldolgozásra került. Így a tudásuk hosszú távú hatását is vizsgáltuk.

A járvány miatt bevezetett digitális oktatás teljesen megváltoztatta a kísérlet kivitelezését, ezért a legtöbb eredmény még nem érkezett be. A Budapesti Fazekas Mihály Gyakorló Általános Iskola és Gimnázium 8 - os osztályának eredményei már mind beérkeztek, ezért ezek alapján vonjuk le a következtetéseinket.

Az év elején írt első dolgozatra (Bemeneti mérés) maximálisan 40 pontot szerezhettek a diákok. A dolgozat eredményeit a 2.1 táblázatban láthatjuk.

2.1. táblázat. Bemeneti mérés

Kísérleti csoport	Kontroll csoport
40	40
40	40
40	40
39	39
39	37
39	36
38	34
37	34
36	30
33	
Átlag: 38,1	Átlag: 36,67

Látható a táblázatból, hogy a két csoport teljesítménye között minimális az eltérés, tehát a két csoport egyformának tekinthető.

A kísérlet 15. hetében a függvények témából írtak témazáró dolgozatot (Függvények 1.), ahol maximálisan 31 pontot szerezhettek. Ezeket az eredményeket a 2.2 táblázatban láthatjuk.

2.2. táblázat. Függvények 1.

Kísérleti csoport	Kontroll csoport
31	31
31	31
30	30
29	29
29	28
29	27
28	25
28	21
28	21
27	
Átlag: 29,0	Átlag: 27,0
Szórás: 1,333	Szórás: 3,905

Az utolsó számelmélet feladat megoldása után egy héttel megírták a harmadik dolgozatot (Szintfelmérő). Ez a dolgozat reguláris tananyaggal kapcsolatos feladatokat tartalmazott, melyen legfeljebb 24 pontot lehetett szerezni. Az eredményeket a 2.3 táblázatban láthatjuk.

2.3. táblázat. Szintfelmérő

Kísérleti csoport	Kontroll csoport
24	24
24	24
24	24
24	21
23	20
21	19
21	16
20	14
17	9
14	
Átlag: 21,2	Átlag: 19,0
Szórás: 3,425	Szórás: 5,172

Az utolsó számelmélet feladat megoldása után négy héttel megírták a negyedik dolgozatot is (Függvények 2.). Ezen a dolgozaton legfeljebb 35 pontot lehetett szerezni. Az eredményeket a 2.4 táblázatban láthatjuk.

2.4. táblázat. Függvények 2.

Kísérleti csoport	Kontroll csoport
35	35
35	35
33	35
32	28
30	27
30	25
30	23
29	22
28	11
24	
Átlag: 30,6	Átlag: 26,8
Szórás: 3,34	Szórás: 7,85

Az osztályból öt diák legtöbbször maximális pontot ért el az év közben írt dolgozatokon. Az öt diák közül három a kontroll csoportba, kettő a kísérleti csoportba tartozik. Őket az eredmények értékelése során kihagyjuk, ugyanis a legszorgalmasabb és legtehetségesebb tanulóknál nem számít mit és hogyan tanítunk, tudni fogják a tananyagot. Újrászámoltuk az átlagokat, az így kapott eredményeket a következő táblázatokban láthatjuk.

2.5. táblázat. Függvények 1. (öt diák nélkül)

Kísérleti csoport	Kontroll csoport
31	29
30	28
29	27
29	25
28	21
28	21
28	
27	
Átlag: 28,75	Átlag: 25,167
Szórás: 1,282	Szórás: 3,488

2.6. táblázat. Szintfelmérő (öt diák nélkül)

Kísérleti csoport	Kontroll csoport
24	24
24	20
24	19
24	16
23	14
21	9
20	
17	
Átlag: 22,13	Átlag: 17,0
Szórás: 2,588	Szórás: 5,215

A negyedik dolgozat (Függvények 2.) összesen négy feladatot tartalmazott, melyből kettő átlagos nehézségű volt (1. és 3.), kettő nehezebb, több gondolkodást igényelt (2. és 4.). Az itt elért eredményeket feladatonként részletezzük. A könnyebb áttekinthetőség érdekében a kísérleti csoport eredményeit lilával, a kontroll csoport eredményeit zölddel emeltük ki.

2.7. táblázat. Függvények 2. (öt diák nélkül)

	1.	1.	2.	2.	3.	3.	4.	4.	Összesen	Összesen
Max. pont	10	10	11	8	8	8	6	6	35	35
	10	10	11	6	8	8	6	6	33	28
	10	10	10	6	8	8	6	4	32	27
	10	10	9	5	8	8	6	3	30	25
	10	10	8	3	8	8	6	2	30	23
	10	9	6	3	7	7	6	0	30	22
	10	9	5	1	7	0	5	0	29	11
	9		5		7		5		28	
	8		3		5		4		24	
Átlag:	9,625	9,67	7,125	4,0	7,25	6,5	5,5	2,5	29,5	22,67
Szórás:	0,744	0,516	2,8	2,0	1,035	3,209	0,756	2,345	2,726	6,154

A második dolgozaton (Függvények 1.) elérhető maximális pontszám 31 volt. Az átlagpontszám a kísérleti csoportnál 28,75, a szórás 1,282, a kontroll csoportnál az átlagpontszám 25,167, a szórás 3,488 volt. A harmadik dolgozaton (Szintfelmérő) elérhető maximális pontszám 24 volt. Az átlagpontszám a kísérleti csoportnál 22,13, a szórás 2,588, a kontroll csoportnál az átlagpontszám 17,0, a szórás 5,215 volt. A negyedik dolgozaton (Függvények 2.) elérhető maximális pontszám 35 volt. Az összpontszámra vonatkozó átlag pontszám a kísérleti csoportnál 29,5, a szórás 2,726, a kontroll csoportnál az átlagpontszám 22,67, a szórás 6,154 volt.

A kísérleti csoportokban tanuló diákok szignifikánsan több pontot szereztek, mint a kontrollcsoportokban lévők, annak ellenére, hogy az év eleji dolgozaton hasonlóan teljesített a két csoport.

A 2.7 táblázatban az is látható, hogy azokon a feladatokon, melyek több gondolkodást igényeltek (2. és 4.) még nagyobb a differencia a kísérleti csoport és a kontroll csoport diákjai között. Azt is elmondhatjuk, hogy egy diák kivételével a kísérleti csoport minden tagja legalább annyi pontot ért el, mint a kontroll csoport legjobban teljesítő diákja.

Azt gondolhatnánk, hogy azoknak a diákoknak, akik a reguláris tananyagot többet gyakorolták, jobban kellene teljesíteniük az ebben a témában írt dolgozatokon. A 2.5, 2.6 és 2.7 táblázatokban rögzített eredmények igazolják, hogy azok a diákok, akik több hónapon keresztül számelmélet feladatokkal foglalkoztak, jobban teljesítenek a reguláris tananyagból is. Megállapíthatjuk, hogy módszerünk közép-, és hosszútávon hatékony volt. A kiváló diákokon, akik a hagyományos módon rendszeresen és jól tanulnak, nem tudtuk "rendesen" felmérni a kísérlet hatását. Ők a kísérlet nélkül is majdnem mindig maximálisan teljesítenek. Ez nem jelenti sem azt, hogy ők nem fejlődtek, sem azt, hogy a kísérletünk hatása pótolható a hagyományos tanulással. Az ő fejlődésüket egy külön kísérletben lehetne vizsgálni.

2.7. A kísérlet alkalmazása a digitális oktatás keretei között

Magyarországon a koronavírus terjedésének megelőzése érdekében 2020. Március 18-ától visszavonásig hivatalossá tették az oktatás digitális keretek melletti folytatását.

A bejelentés után egy teljesen új és addig ismeretlen helyzetben találta magát a legtöbb pedagógus. Bár a tanári kompetenciák között szerepel az IKT eszközök használata, a digitális oktatás egészen más helyzet.

Megfogalmazott tanári kompetenciák az IKT eszközök használatával kapcsolatban:

- „Tisztában van IKT pedagógiai alkalmazásának sajátosságaival.”
- „Ismeri a hatékony (írásos, szóbeli és IKT) kommunikáció összetevőiről összegyűlt tudást, az erről szóló alapvető szakirodalomban tájékozott.”
- „Elismeri a hatékony kommunikáció, s a hozzátartozó technikák jelentőségét mind a nevelő-oktatómunkában, mind az iskolai szervezet fenntartásában, működtetésében.”
- „Tud tájékozódni a szakirodalomban, könyvtárban és interneten, ismeri az alapvető hazai pedagógiai műhelyekhez tartozó alpművek és periodikák elérhetőségét. Képes az IKT hatékony alkalmazására.”

Úgy gondoltuk kísérletünk számos szaktanárnak jelenthet segítséget. Az Eötvös Loránd Tudományegyetem Matematika Tanuláselméleti és -Pszichológiai Kutatócsoport tagjaival összeállítottunk egy tájékoztatót, melyben ismertetjük a kísérlethez szükséges információkat és teendőket. A tájékoztató megírásánál ügyeltünk arra, hogy a kísérlet leírása érthető és részletes legyen, hogy a szaktanár feladata egyértelmű és világos legyen, és hogy a szaktanár minden lehetséges segítséget megkapjon. A tájékoztató számos közoktatási intézménybe el lett küldve az országban. Nagy örömünkre az Oktatási Hivatal honlapjára is kikerült "A tanulást támogató hasznos anyagok" közé.



Matematika Tanulásméleti és -Pszichológiai Kutatócsoport

Eötvös Loránd Tudományegyetem Természettudományi Kar, Matematikai Intézet

Kutatócsoport vezető: Dr. Szabó Csaba egyetemi tanár, email: csaba@cs.elte.hu

TÁJÉKOZTATÓ

Az Eötvös Loránd Tudományegyetem Matematika Tanulásméleti és -Pszichológiai Kutatócsoport egyik kutatási területe annak vizsgálata, hogy különböző matematikai tevékenységek hogyan hatnak az általános gondolkodásra és a későbbi matematikai képességekre. A magyar matematikaoktatás problémaközpontú. A feladatmegoldásban az eltérő megoldási módszerek használata a matematika különböző ágazatain belül, vagy például a rendszeres társasjátékozás más és más hatással vannak a gondolkodásunkra. Ezek közben különböző funkciójú agyi tevékenységeket végez az ember. A számelmélet egy olyan része a matematikának, ahol a legkülönbözőbb fajta ötletekkel, megoldási módszerekkel találkozhatnak a diákok. A kutatócsoport egy korábbi projektjében kimutatta, hogy számelmélet feladatok megoldása pozitívan hat a diákok általános matematikai gondolkodására. Azok a diákok, akik a matematika óra öt percében nem a tananyaghoz kapcsolódóan oldottak meg feladatokat, hanem számelmélet problémákkal foglalkoztak, jobban szerepeltek a tananyaghoz kapcsolódó dolgozatokon is, mint társaik. A módszert teszteltük elit és hagyományos általános iskolában is. A diákok fejlődése már a projekt felénél mérhető volt. Mindenkinek ajánljuk a módszert, amelyhez rengeteg kész segédanyagot elküldünk, ezzel segítve a szaktanárok munkáját. A módszer könnyen kipróbálható az online oktatás során, de jól működik a „hagyományos” iskolai környezet keretei között is.

Amennyiben szívesen részt venne a módszer továbbfejlesztésében, kérjük, válasszon a **Továbbfejlesztési lehetőségek** fejezetben lévő lehetőségek közül.

Ezeket a feladatokat 7-10. osztályos diákoknak javasoljuk.

A projekt menete

A projekt során a szaktanár fő feladata a feladatokat és a megoldásokat tartalmazó kódok kiküldése, és bizonyos időközönként a feladatok kijavítása megadott szempontok szerint. Ezen kívül lehetőség van egy bemeneti és egy kimeneti dolgozat megíratására, amellyel a diákok fejlődését lehet mérni. (A két tesztben hasonló feladatok vannak. A teszteknel ügyelünk arra, hogy olyan témájú feladatokat adjunk, melyeket már tanultak a diákok, de azok között ne szerepeljenek számelmélettel kapcsolatos feladatok.)

Az alábbiakban részletesen kifejtjük a főbb lépéseket:

1. A projekthez minden feladatot elküldünk a szaktanárnak e-mailben, aki naponta egyet továbbít a diákoknak. (A szaktanár megkapja a feladatokat egyesével is, így ezeket ki tudja küldeni külön-külön.)
2. Ezután a diákok a megoldást leírják egy lapra (erre 5-10 percük van), majd lefényképezve visszaküldik szaktanárunknak (fotó helyett természetesen bármilyen más megoldás is megfelel).



Matematika Tanuláselméleti és -Pszichológiai Kutatócsoport

Eötvös Loránd Tudományegyetem Természettudományi Kar, Matematikai Intézet

Kutatócsoport vezető: Dr. Szabó Csaba egyetemi tanár, email: csaba@cs.elte.hu

3. Miután minden diák beküldte a feladatot, kapnak egy kódot a szaktanártól, mellyel otthon megnézhetik a megoldást.
4. A megoldás tudatában a következő napi feladat sokkal könnyebben megoldható.
5. Értékelés: Mivel a diákok a megoldást ismerik, ezért a kijavított dolgozatokat nem kell visszakapniuk, elég, ha a dolgozatra kapott pontszámot ismerik. Így a feladatok pontozása egy nagyon gyors feladat a szaktanárnak, mondhatni ránézésre elvégezhető munka, ezen kívül nem kell minden nap javítania. (Esetleg furcsának tűnhet, hogy nem fektetünk nagyobb energiát a visszajelzésre. Ezt azért így terveztük, mert a módszer lényege a problémamegoldás, ennek várjuk fejlesztő hatását.)
6. A feladatokra kapott pontok rögzítése egy előre megírt táblázatban.
7. Összesen 63 feladat van négy részre osztva: 1. rész: 1-15. feladat; 2. rész: 16-30. feladat; 3. rész: 31-45. feladat; 4. rész: 46-63. feladat.

Az a tapasztalatunk, hogy a diákok a projekt elején még rosszul teljesítenek, de minél több feladatot oldanak meg, és látják a megoldásokat, annál jobban fejlődnek. Az utolsó részre már szinte minden diák elérte az ötös határát, tehát megéri a módszert folytatni.

A feladatsort úgy állítottuk össze, hogy egy átlagos képességű diák a feladatsor megoldását követően eljusson egy olyan szintre, ahol korosztályának megfelelő versenyfeladatokat tud megoldani. A 63 feladtból álló feladatsor több blokkból áll. Minden egyes blokk egy-egy nehezebb versenyfeladat megoldását készíti elő, a blokkban szereplő feladatok rávezető feladatsorként funkcionálnak.

Ellenőrzés

A 63 számelmélet feladat megtalálható megoldással együtt a www.vasvivien.com honlapon → Diákjaimnak → Versenyfeladatok. Ezen az oldalon megjelenik az összes feladat, mindegyik külön linkkel. Amikor megnyitunk egy feladatot, a készülék automatikusan letölti azt. A feladat megtekintése azonban csak a feladathoz tartozó kód ismeretében lehetséges. Minden feladathoz külön kód tartozik, melyet a szaktanárnak e-mailben elküldünk. Így az aznapi feladat kódját továbbítani tudja a diákoknak, és a diákok egyrészt le tudják ellenőrizni jól gondolkodtak-e, másrészt látják a helyes megoldást. Amikor a diák beüti a letöltött feladathoz tartozó kódot, látja a feladat szövegét és megoldását is.

A megoldókulcsot használva a szaktanár viszonylag könnyen le tudja ellenőrizni a diákok megoldását. A helyes megoldásokért, megoldásrészletekért a diákok pontokat szerezhetnek, ezeket a pontokat kérjük rögzítse a szaktanár egy táblázatba.

Pontozási útmutató

Minden feladat megoldásáért pontokat lehet szerezni. (Az adott feladatra adható maximális pontszámot a kiküldött táblázatok tartalmazzák.)

Példa (Megtekintése csak a feladathoz tartozó kód ismeretében lehetséges.):

Határozd meg azokat az $\overline{aaa}$ alakú háromjegyű természetes számokat, melyek oszthatóak 6-tal. (4 pont)



Matematika Tanulásméleti és -Pszichológiai Kutatócsoport

Eötvös Loránd Tudományegyetem Természettudományi Kar, Matematikai Intézet

Kutatócsoport vezető: Dr. Szabó Csaba egyetemi tanár, email: csaba@cs.elte.hu

A feladat megoldása:

Egy szám pontosan akkor osztható 6-tal, ha osztható 2-vel és 3-mal is. **(1 pont)**

Hárommal pontosan akkor osztható, ha számjegyeinek összege osztható 3-mal.

Számjegyeinek összege: $a + a + a = 3a \rightarrow$ Biztosan osztható 3-mal. **(1 pont)**

Kettővel pontosan akkor osztható, ha 0, 2, 4, 6, 8-ra végződik. A 0-t kizárjuk, hiszen akkor nem lenne 3-jegyű a szám. **(1 pont)**

Tehát azok a számok, amik nekünk jók: 222, 444, 666, 888. **(1 pont)**

A példán is látható, hogy a pontok nagy része nem a helyes végeredményre jár, hanem az ötletre, magyarázatra. Ezt a diákokkal már az első feladat előtt érdemes közölni, és közben is lehet többször emlékeztetni rá őket, hogy a pontok nagy része a jó ötletekért és a magyarázatért jár, nem elegendő a végeredmény megadása.

Annak érdekében, hogy a diákok motiváltak maradjanak, jó módszer lehet, ha egy bizonyos feladatszám végeztével adott pontszám elérését követően a diákok ötös érdemjegyet szerezhettek. Mi a projektünkben négy részre osztottuk a 63 feladatból álló feladatsort és az egyes részek befejeztével értékeltük a diákok teljesítményét. Diákjaink akkor kaptak ötöst, ha elérték legalább a pontok 50%-át (ettől persze el lehet térni). Így az a tanuló is motivált maradhat, aki az elején nem teljesít jól, és nagyon le van maradva – és ehhez hasonlóan azok a tanulók sem lankadhatnak el, akik az elején nagyon jól teljesítenek.

A kiküldött dokumentumok

- Két szintfelmérő (egy bemeneti, és egy kimeneti teszt)
- A feladatok megoldásokkal együtt
- A feladatok egyesével (diákoknak küldhető)
- A feladatok kódjait tartalmazó táblázatok
- Táblázatok, melyekbe a pontokat lehet rögzíteni
- Tájékoztató a diákoknak részletes leírással

A szaktanár teendői a projekt során

1. Írni egy e-mailt a szamelm.kiserlet@gmail.com email címre, hogy szívesen kipróbálná ezt a módszert. Az emailben meg kell adni a tanított csoportok
 - évfolyamát, és
 - a projekt kivitelezését (itt kell a lentebb írt 3 opció közül választani).
2. Az emailre egy napon belül válaszolunk, melyben elküldjük a szükséges dokumentumokat. Illetve megbeszéljük az első szintfelmérő időpontját is.
3. Mikor a diákok megírták a szintfelmérőt, az eredmények rögzítéséhez elküldünk egy táblázatot.



Matematika Tanuláselméleti és -Pszichológiai Kutatócsoport

Eötvös Loránd Tudományegyetem Természettudományi Kar, Matematikai Intézet

Kutatócsoport vezető: Dr. Szabó Csaba egyetemi tanár, email: csaba@cs.elte.hu

4. Segítséget jelentene a projektünk szempontjából, ha a kitöltött táblázatokat visszaküldenék a fent említett email címre. (Ez természetesen nem kötelező, bárki kipróbálhatja a módszert.)
5. A diákoknak tájékoztatót küldeni a projektről, illetve arról, hogy hol találják a megoldásokat.
6. Minden órán küldeni egy feladatot, a megoldást a diákok lefotózva beküldik.
7. Mikor mindenki elküldte, eljuttatni hozzájuk az adott feladat kódját, hogy meg tudják nézni a megoldást.
8. A szaktanár megnézi a feladatokat, és pontozza, majd a táblázatban rögzíti.
9. A pontokról időnként tájékoztatja a diákokat (akár elküldve nekik a táblázatot, akár elküldve a fent említett email címre, ami kikerülne a weboldalra).
10. Részenként összesíteni a pontokat, kiosztani az ötösöket.
(1. rész: 1-15. feladat; 2. rész: 16-30. feladat; 3. rész: 31-45. feladat; 4. rész: 46-63. feladat)
11. Örülünk, ha a tapasztalataikat és részeredményeiket időnként elküldik nekünk.
12. Amikor minden feladatnak vége, íratnak egy hasonló felmérőt, mint az elején, amit szintén táblázatban rögzítenek.

Úgy gondoljuk ez egy jó lehetőség. Bár sok munkának tűnik, "csak" a feladatokat kell javítani és rögzíteni egy táblázatban, a többi anyagot küldjük. Azoknál az osztályoknál, ahol elvégeztük ezt a projektet jelentős fejlődést tapasztaltunk.

A módszert minden kolléga kipróbálhatja, a projektben nem kötelező részt venni.

Nekik a kezükbe adjuk a feladatokat, a javaslatainkat, amiket szabadon használhatnak.

Amennyiben szívesen részt venne a módszer kipróbálásában, kérjük válasszon az alábbi három opció közül:

1. Az osztály minden tagja számelmélet feladatot old meg az óra végén (ezen kívül egy bemeneti és egy kimeneti szintfelmérőt, ami vegyes feladatokat tartalmaz).
2. Nem oldanak meg a diákok számelmélet feladatokat, csak a két szintfelmérőt írják meg.
3. Az osztály egyik fele számelmélet, a másik fele az adott tananyaggal kapcsolatos feladatot old meg az óra végén, (és az osztály egésze ír mind egy bemeneti mind egy kimeneti szintfelmérőt).

Továbbfejlesztési lehetőségek

Ha valakinek van rá lehetősége és van hozzá kedve akkor külön segíthet, ha az alábbi két pont közül az egyik szerint tudnak haladni, vagy valami ezekhez hasonló megoldást tudnak találni a saját iskolájukban.

- **Két párhuzamos osztályban végzik a projektet.** Az évfolyam egyik osztálya minden órán számelmélet feladatot kap, az évfolyam másik osztálya „csak” tananyaggal kapcsolatos feladatokat.



Matematika Tanulásméleti és -Pszichológiai Kutatócsoport

Eötvös Loránd Tudományegyetem Természettudományi Kar, Matematikai Intézet

Kutatócsoport vezető: Dr. Szabó Csaba egyetemi tanár, email: csaba@cs.elte.hu

VAGY

- **Egy osztályban végzik a projektet.** Az osztályt két csoportra osztja a szaktanár, az egyik csoport a számelmélet feladatokat kapja, a másik csoport tananyaggal kapcsolatos feladatokat.

Sok lehetőséget el tudunk még képzelni a módszer kivitelezéséhez. Így, ha valaki szívesen elküldené az eredményeket, de másképp szeretné csinálni, akkor egy rövid egyeztetés után nem látjuk ennek akadályát.

Kapcsolattartó: Vas Vivien

Email cím: szamelm.kiserlet@gmail.com

Matematika Tanulásméleti és -Pszichológiai Kutatócsoport, ELTE TTK, Matematikai Intézet
Kutatócsoport vezető: Dr. Szabó Csaba egyetemi tanár

email: csaba@cs.elte.hu

Köszönettel: Matematika Tanulásméleti és -Pszichológiai Kutatócsoport

3. fejezet

Magasabb fokú diofantikus egyenletek

3.1. Bevezetés

Szinte nincs olyan matematika verseny, ahol ne fordulna elő számelmélettel kapcsolatos feladat. Akár első forduló, akár döntő, a számélet jelen van. Ebben a fejezetben egy Matematika Diákolimpiára született feladatjavaslatból (IMO Shortlist) indulunk ki, és hasonló alakú feladatokat próbálunk készíteni. Megmutatjuk, hogy ez nem is olyan könnyű. A kiindulási feladatunk megoldása a körosztási polinomok tulajdonságain alapszik. A körosztási polinomok általános számelmélete nehéz. Ezért megpróbáltunk olyan feladatokat is készíteni, amelyek kisebb tárgyi tudást igényelnek.

Először röviden összefoglaljuk a körosztási polinomok elméleti hátterét, majd ehhez kapcsolódva megoldunk egy feladatot, elkészítünk két hasonló feladatot, végül megmutatjuk, hogy tudnánk és hogyan nem lehet hasonló szellemű feladatot készíteni.

3.1.1. Körosztási polinomok számelmélete

Ebben a fejezetben először átismétljük a körosztási polinomok legfontosabb tulajdonságait, majd összefoglaljuk az egész helyeken fölvev értékeikről ismert számelméleti tételeket.

Legyen n pozitív egész szám. Az n -edik komplex egységgyökök azok a z komplex számok, amelyekre teljesül, hogy $z^n = 1$. Például a negyedik egységgyökök az $1, i, -1, -i$. Egy n -edik egységgyököt primitív n -edik egységgyöknek nevezzük, ha semelyik $k < n$; $k = 1, 2, \dots, n-1$ pozitív egész szám esetén nem k -edik egységgyök. Egy $z \in \mathbb{C}$ komplex szám rendje, $o(z)$, az a legkisebb pozitív n , melyre $z^n = 1$. (Ha ilyen nincs, akkor $o(z) = \infty$.) Ez azt is jelenti, hogy $z \in \mathbb{C}$ pontosan akkor primitív n -edik egységgyök, ha $o(z) = n$. Ha $n \geq 1$, akkor legyen

$$\Phi_n(x) = (x - \xi_1) \cdot \dots \cdot (x - \xi_{\varphi(n)}),$$

ahol $\xi_1, \dots, \xi_{\varphi(n)}$ az összes primitív n -edik egységgyök. Φ_n foka $\varphi(n)$, ahol φ az Euler-féle φ függvény, $\Phi_n(x)$ neve az n -edik körosztási polinom. Ezek alapján, ha $n \geq 1$, akkor

$\prod_{d|n} \Phi_{d(x)} = x^n - 1$, azaz

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{k|n, \\ k \neq n}} \Phi_k(x)}$$

Speciálisan, ha p prím és n pozitív egész szám, akkor

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + 1$$

és

$$\Phi_{p^n}(x) = \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1} = x^{(p-1)p} + x^{(p-2)p} + \dots + x^p + 1$$

Például $\Phi_{11}(x) = \frac{x^{11}-1}{x-1} = x^{10} + x^9 + \dots + 1$ és $\Phi_9(x) = \frac{x^9-1}{x^3-1} = x^6 + x^3 + 1$.

A rend számelméleti fogalma megegyezik a redukált maradékosztályok multiplikatív csoportjában vett renddel. Legyen $(a, m) = 1$. A k pozitív egész számot az a rendjének nevezzük modulo m , ha $a^k \equiv 1(m)$, de bármely $0 < i < k$ esetén $a^i \not\equiv 1(m)$. Az " a " szám, vagy a maradékosztály modulo m vett rendjét $o_m(a)$ jelöli.

Legyen c egy egész szám és q prím. Ekkor $o_q(c) = m$ pontosan akkor teljesül, ha $q \mid \Phi_m(c)$ és $q \nmid m$. Ebből rögtön következik az alábbi állítás:

1. Tétel. Ha a egész szám, akkor $\Phi_n(a)$ minden prímosztója vagy osztója n -nek, vagy $n \cdot k + 1$ alakú.

Másképpen fogalmazva, ha a pozitív egész szám, akkor $\Phi_n(a)$ minden p prímosztójára teljesül, hogy $p \equiv 1(n)$ vagy $p \mid n$. Ebből rögtön következik az is, hogy $\Phi_n(a)$ minden d osztója vagy osztható n valamely prímosztójával, vagy $d \equiv 1 \pmod{n}$. Prímszámok esetén $d \mid \Phi_p(a)$ -ból következik, hogy vagy $p \mid d$, vagy $p \mid d - 1$,

Ezzel a tudással felvértezve nézzünk meg néhány feladatot.

3.2. Feladatok

A következő feladat a 2006-os Olimpiához készült válogatott feladatok között szerepelt, az úgynevezett IMO Shortlist-en [25].

1. Feladat. Bizonyítsuk be, hogy az $\frac{x^7 - 1}{x - 1} = y^5 - 1$ egyenletnek nincs egész megoldása.

Bizonyítás. Ha felbontjuk mind a két oldalt, akkor az

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (y - 1) \cdot (y^4 + y^3 + y^2 + y + 1)$$

egyenlőséget kapjuk. Látjuk, hogy a bal oldal a hetedik körosztási polinom, $\Phi_7(x)$, melyről

tudjuk, hogy minden p prímosztójára teljesül, hogy

$$p = 7 \quad \text{vagy} \quad p \equiv 1 \pmod{7}$$

Ennek a feltételnek a jobb oldal minden osztójára is teljesülnie kell. Tehát a jobb oldalon minden tényező $7k$, vagy $7k + 1$ alakú szám, ami azt jelenti, hogy

$$y - 1 \equiv 0 \pmod{7} \quad \text{vagy} \quad y - 1 \equiv 1 \pmod{7}$$

1. eset Ha $y - 1 \equiv 0 \pmod{7}$, akkor $y \equiv 1 \pmod{7}$.

A baloldal másik tényezője: $y^4 + y^3 + y^2 + y + 1$, melynek szintén minden prímosztója 7 vagy $(7k + 1)$ alakú, azaz 7-tel osztva 0 vagy 1 maradékot kell, hogy adjon, azaz:

$$y^4 + y^3 + y^2 + y + 1 \equiv 0 \pmod{7} \quad \text{vagy} \quad y^4 + y^3 + y^2 + y + 1 \equiv 1 \pmod{7}$$

kell, hogy teljesüljön. Ha $y \equiv 1 \pmod{7}$, akkor $y^4 + y^3 + y^2 + y + 1 \equiv 1^4 + 1^3 + 1^2 + 1 + 1 \equiv 5 \pmod{7}$. Ezzel ellentmondásra jutunk.

2. eset Ha $y - 1 \equiv 1 \pmod{7}$, akkor $y \equiv 2 \pmod{7}$.

Ahogy az előbb is, a baloldal másik tényezője $y^4 + y^3 + y^2 + y + 1$, melynek szintén minden prímosztója 7 vagy $7k + 1$ alakú, azaz 7-tel osztva 0 vagy 1 maradékot kell, hogy adjon, azaz

$$y^4 + y^3 + y^2 + y + 1 \equiv 0, \pmod{7} \quad \text{vagy} \quad y^4 + y^3 + y^2 + y + 1 \equiv 1 \pmod{7}$$

kell, hogy teljesüljön. Ha $y \equiv 2 \pmod{7}$, akkor $y^4 + y^3 + y^2 + y + 1 \equiv 2^4 + 2^3 + 2^2 + 2 + 1 \equiv 16 + 8 + 4 + 2 + 1 \equiv 2 + 1 + 4 + 2 + 1 \equiv 10 \equiv 3 \pmod{7}$. Ekkor is ellentmondásra jutunk, tehát ennek az egyenletnek nincs megoldása az egész számok körében. $\square$

Ebből a feladatból ötletet merítve hasonló feladatot próbáltunk készíteni.

2. Feladat. (Saját feladat) Bizonyítsuk be, hogy az $x^6 + x^3 + 1 = y^{11} - 1$ egyenletnek nincs egész megoldása.

Bizonyítás. Látjuk, hogy a bal oldal a kilencedik körosztási polinom, $\Phi_9(x)$, a jobb oldalt felbontva a

$$(y - 1) \cdot (y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)$$

szorzatot kapjuk, ahol $y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1$ a tizenegyedik körosztási polinom, $\Phi_{11}(y)$.

A bal oldalon a kilencedik körosztási polinom szerepel, $\Phi_9(x)$, melynek minden prímosztója 3 vagy $9k + 1$ alakú. Ezért minden osztója ilyen prímek szorzata, így $3k$ vagy $9k + 1$ alakú. Ennek a feltételnek a jobb oldal minden osztójára is teljesülnie kell. Tehát a jobb oldalon minden tényező $3k$ vagy $9k + 1$ alakú szám. Először tekintsük a jobboldal második

tényezőinek lehetséges értékeit modulo 9:

$$\begin{aligned}
\Phi_{11}(0) &\equiv 0^{10} + 0^9 + 0^8 + 0^7 + 0^6 + 0^5 + 0^4 + 0^3 + 0^2 + 0 + 1 && \equiv 1 \\
\Phi_{11}(1) &\equiv 1^{10} + 1^9 + 1^8 + 1^7 + 1^6 + 1^5 + 1^4 + 1^3 + 1^2 + 1 + 1 && \equiv 2 \\
\Phi_{11}(2) &\equiv 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2 + 1 \equiv \\
&\equiv (-2) + (-1) + (4) + 2 + 1 + (-4) + (-2) + (-1) + (4) + (2) + (1) && \equiv 4 \\
\Phi_{11}(3) &\equiv (3^{10} + 3^9 + 3^8 + 3^7 + 3^6 + 3^5 + 3^4 + 3^3 + 3^2 + 3 + 1) \equiv \\
&\equiv (0) + (0) + (0) + (0) + (0) + (0) + (0) + (0) + (0) + (3) + (1) && \equiv 4 \\
\Phi_{11}(4) &\equiv (4^{10} + 4^9 + 4^8 + 4^7 + 4^6 + 4^5 + 4^4 + 4^3 + 4^2 + 4 + 1) \equiv \\
&\equiv (4) + (1) + (-2) + (4) + (1) + (-2) + (4) + (1) + (-2) + (4) + (1) && \equiv 5 \\
\Phi_{11}(5) &\equiv 5^{10} + 5^9 + 5^8 + 5^7 + 5^6 + 5^5 + 5^4 + 5^3 + 5^2 + 5 + 1 \equiv \\
&\equiv (4) + (-1) + (-2) + (5) + (1) + (2) + (4) + (-1) + (-2) + (5) + (1) && \equiv 7 \\
\Phi_{11}(6) &\equiv 6^{10} + 6^9 + 6^8 + 6^7 + 6^6 + 6^5 + 6^4 + 6^3 + 6^2 + 6 + 1 \equiv \\
&\equiv (0) + (0) + (0) + (0) + (0) + (0) + (0) + (0) + (0) + (6) + (1) && \equiv 7 \\
\Phi_{11}(7) &\equiv 7^{10} + 7^9 + 7^8 + 7^7 + 7^6 + 7^5 + 7^4 + 7^3 + 7^2 + 7 + 1 \equiv \\
&\equiv (-2) + (1) + (4) + (-2) + (1) + (4) + (-2) + (1) + (4) + (7) + (1) && \equiv 8 \\
\Phi_{11}(8) &\equiv 8^{10} + 8^9 + 8^8 + 8^7 + 8^6 + 8^5 + 8^4 + 8^3 + 8^2 + 8 + 1 \equiv \\
&\equiv (1) + (-1) + (1) + (-1) + (1) + (-1) + (1) + (-1) + (1) + (-1) + (1) && \equiv 1
\end{aligned}$$

A kifejezés lehetséges értékei modulo 9: 1, 2, 4, 5, 7, 8. A kapott értékek közül csak az 1-re teljesül, hogy $3k$, vagy $9k + 1$ alakú. Ekkor $y \equiv 0 \pmod{9}$ vagy $y \equiv 8 \pmod{9}$.

1. eset: $y \equiv 0 \pmod{9}$.

Ha $y \equiv 0 \pmod{9}$, akkor $y - 1 \equiv 8 \pmod{9}$. Az $(y - 1)$ kifejezésre is teljesülnie kell, hogy $3k$, vagy $9k + 1$ alakú, ezzel ellentmondásra jutunk.

2. eset $y \equiv 8 \pmod{9}$.

Ha $y \equiv 8 \pmod{9}$, akkor $y - 1 \equiv 7 \pmod{9}$, ezzel is ellentmondásra jutunk.

Tehát ennek az egyenletnek nincs megoldása az egész számok körében. $\square$

A rutinosabb versenyzők kezdhettek máshogy a feladatot, mellyel lényegesen megrövidíthetik az előző számolást.

2. feladat - Rövidebb megoldás

Bizonyítsuk be, hogy az $x^6 + x^3 + 1 = y^{11} - 1$ egyenletnek nincs egész megoldása.

Bizonyítás. A jobb oldalt felbontva az

$$(y - 1) \cdot (y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)$$

szorzatot kapjuk. A bal oldal a kilencedik körosztási polinom, $\Phi_9(x)$, melynek az összes lehetséges prímosztója $9k+1$ alakú vagy 3. Ennek a feltételnek a jobb oldal minden osztójára is teljesülnie kell. Tehát a jobb oldalon minden tényező $3k$, vagy $9k+1$ alakú szám kell hogy legyen.

Először nézzük $(y-1)$ lehetséges értékeit, (hiszen lényegesen kevesebb számolást igényel, mintha $(y^{10}+y^9+y^8+y^7+y^6+y^5+y^4+y^3+y^2+y+1)$ lehetséges értékeit néznénk). Ekkor:

$$y-1 \equiv 0 \pmod{3} \quad \text{vagy} \quad y-1 \equiv 1 \pmod{9}.$$

1. eset Ha $y-1 \equiv 0 \pmod{3}$, akkor $y \equiv 1 \pmod{3}$, és $(y^{10}+y^9+y^8+y^7+y^6+y^5+y^4+y^3+y^2+y+1) \equiv (1^{10}+1^9+1^8+1^7+1^6+1^5+1^4+1^3+1^2+1+1) \equiv 2 \pmod{3}$, azaz nem $3k$, és nem $9k+1$ alakú ez a tényező.

2. eset Ha $y-1 \equiv 1 \pmod{9}$, akkor $y \equiv 2 \pmod{9}$. Ekkor $(y^{10}+y^9+y^8+y^7+y^6+y^5+y^4+y^3+y^2+y+1) \equiv (2^{10}+2^9+2^8+2^7+2^6+2^5+2^4+2^3+2^2+2+1) \equiv 2 \cdot (2^3)^3 + (2^3)^3 + 2^2 \cdot (2^3)^2 + 2 \cdot (2^3)^2 + (2^3)2 + 2^2 \cdot 2^3 + 2 \cdot 2^3 + 2^3 + 2^2 + 2 + 1 \equiv (-2) + (-1) + (4) + 2 + 1 + (-4) + (-2) + (-1) + (4) + (2) + (1) \equiv 4 \pmod{9}$

Ezzel is ellentmondásra jutunk, tehát ennek az egyenletnek nincs megoldása az egész számok körében. $\square$

Az eddigi feladatok mintájára hasonló feladatok kitalálására törekedtünk, még egyet ismertettünk.

3. Feladat. (Saját feladat) Bizonyítsuk be, hogy az $\frac{x^{19}-1}{x-1} = y^9-1$ egyenletnek nincs egész megoldása.

Bizonyítás. A bal oldal a tizenkilencedik körosztási polinom $\Phi_{19}(x)$, melynek minden prímosztója 19 vagy $19k+1$ -alakú. Ennek a feltételnek a jobb oldal minden osztójára is teljesülnie kell. Tehát a jobb oldalon minden tényező $19k$, vagy $19k+1$ alakú szám.

A jobb oldalt átalakítva az

$$(y-1) \cdot (y^8+y^7+y^6+y^5+y^4+y^3+y^2+y+1).$$

szorzatot kapjuk. Az egyenletnek van megoldása, ha:

$$y-1 \equiv 0 \pmod{19} \quad \text{vagy} \quad y-1 \equiv 1 \pmod{19}$$

1. eset Ha $y-1 \equiv 0 \pmod{19}$, akkor $y \equiv 1 \pmod{19}$.

Ekkor $y^8+y^7+y^6+y^5+y^4+y^3+y^2+y+1 \equiv 1^8+1^7+1^6+1^5+1^4+1^3+1^2+1+1 \equiv 9 \pmod{19}$. Így ez a tényező nem $19k$, vagy $19k+1$ alakú szám.

2. eset Ha $y-1 \equiv 1 \pmod{19}$, akkor $y \equiv 2 \pmod{19}$

$$\begin{aligned} \text{Ekkor } (y^8+y^7+y^6+y^5+y^4+y^3+y^2+y+1) &\equiv (2^8+2^7+2^6+2^5+2^4+2^3+2^2+2+1) \\ &\equiv (2^4 \cdot 2^4 + 2^4 \cdot 2^3 + 2^4 \cdot 2^2 + 2^4 \cdot 2 + 2^4 + 2^3 + 2^2 + 2 + 1) \end{aligned}$$

$\equiv (-3) \cdot (-3) + (-3) \cdot 8 + (-3) \cdot 4 + (-3) \cdot 2 + (-3) + (8) + (4) + (2) + (1) \equiv$
 $(9) + (-5) + (-12) + (-6) + (-3) + (8) + (4) + (2) + (1) \equiv -2 \pmod{19}$, így ez a
 tényező sem $19k$, vagy $19k + 1$ alakú szám, ezzel is ellentmondásra jutunk.

Tehát az egyenletnek nincs megoldása az egész számok körében. $\square$

3.3. Feladatok készítése

Ennek a fejezetnek a célja olyan diofantikus egyenletek készítése, és a készítés menetének bemutatása, amelyeknek nincs megoldása az egész számok körében. Az egyszerűség és a szépség kedvéért olyan egyenleteket vizsgálunk, amelyben kevés tag szerepel. Adódik az $x^n = y^m + c$ típusú egyenletek vizsgálata. Bár a stratégiák néha hasonlóak, esetleg egymásra alapulnak, az áttekinthetőség kedvéért a készítés menetének vázlatát minden feladatnál leírjuk.

Az egyenletek melyeket a fejezet során vizsgálunk:

$$x^3 - y^4 = 6$$

$$y^5 - x^4 = 4$$

$$y^5 - x^4 = 6$$

$$y^5 - x^4 = 12$$

$$y^5 - x^4 = 29$$

$$y^5 - x^4 = 35$$

$$y^7 - x^4 = 2$$

$$y^7 - x^4 = 3$$

$$y^7 - x^4 = 15$$

$$y^7 - x^4 = 19$$

$$y^7 - x^4 = 20$$

$$y^7 - x^4 = 24$$

3.3.1. Alapfeladat

Az Algebra és Számelmélet 1 kurzus végefele tipikusnak számít az alábbi kérdés:

4. Feladat. Határozzuk meg az $x^{12} - y^6 = 11111111111111$ egyenlet összes egész megoldását.

Bizonyítás. A tipikus megoldás azt kívánja meg, hogy vegyük észre, hogy a feladatban minden kitevő a $\varphi(7) = 6$ többszöröse. Az Euler-Fermat tétel alapján

$$a^6 \equiv \begin{cases} 1 & \text{ha } (a, 7) = 1 \\ 0 & \text{ha } 7|a \end{cases}$$

Ugyanez a kongruencia teljesül, ha a kitevő 6 tetszőleges többszöröse. Így az egyenlet bal oldalán x^{12} és y^6 lehetséges értékei 0 és 1 modulo 7. A bal oldal így a 6, 0, 1 értékeket veheti fel modulo 7, míg a jobb oldal 7-tel vett maradéka 4. Így az egyenletnek nincs megoldása modulo 7, így nincs megoldása az egészek közt sem. $\square$

3.3.2. A mi feladatunk

5. Feladat. Határozzuk meg az $y^3 - x^4 = 6$ egyenlet összes egész megoldását.

A startégiánk egy q prím vagy prímhatvány választása, majd az egyenlet két oldalának vizsgálata modulo q . Amennyiben az egyenletben lévő kitevő relatív prím $\varphi(q)$ -hoz, akkor a megfelelő tag (szinte) minden értéket fölvehet modulo q . Szerencsére $\varphi(q)$ mindig páros, így a 4-gyel nem kell törődnünk, mert $(\varphi(q), 4) = 2$ vagy 4. Tehát olyan prímszámokat keresünk, amelyre $3|p-1$, azaz $p = 6k + 1$ valamilyen k -ra.

1. Próbálkozás

Az első prím ahol $p-1$ osztható 3-mal, a 7. Tekintsük y^3 és x^4 lehetséges értékeit modulo 7. Az y^3 lehetséges értékei: 0, 1, 6, az x^4 lehetséges értékei: 0, 1, 2, 4 modulo 7. Bár ezeket a hatványokat könnyű „kézzel” kiszámolni, a későbbiek miatt bemutatunk egy másik módszert is. Tudjuk, hogy a 3 primitív gyök mod(7):

$$\begin{aligned} 3^1 &= 3 &= 3^0 \cdot 3 &\equiv 1 \cdot 3 &\equiv 3 &\pmod{7} \\ 3^2 &= 9 &= 3^1 \cdot 3 &\equiv 3 \cdot 3 &\equiv 2 &\pmod{7} \\ 3^3 &= 27 &= 3^2 \cdot 3 &\equiv 2 \cdot 3 &\equiv 6 &\pmod{7} \\ 3^4 &= 81 &= 3^3 \cdot 3 &\equiv 6 \cdot 3 &\equiv 18 &\equiv 4 &\pmod{7} \\ 3^5 &= 243 &= 3^4 \cdot 3 &\equiv 4 \cdot 3 &\equiv 12 &\equiv 5 &\pmod{7} \\ 3^6 &= 729 &= 3^5 \cdot 3 &\equiv 5 \cdot 3 &\equiv 15 &\equiv 1 &\pmod{7} \end{aligned}$$

Mivel minden maradékosztály előáll egy primitív gyök hatványaként, a köbszámok előállnak a primitív gyök köbének hatványaiként. Így a köbök lehetséges maradékai modulo 7 nem mások, mint a 3^3 hatványai és a 0.

$$\begin{aligned} 3^3 &= 27 \equiv 6 &\pmod{7} \\ 6^2 &= 36 \equiv 1 &\pmod{7} \end{aligned}$$

Hasonlóan, a negyedik hatványok lehetséges maradékai modulo 7 pedig nem mások, mint a 3^4 hatványai és a 0.

$$3^4 = 81 \equiv 4 \pmod{7}$$

$$4^2 = 16 \equiv 2 \pmod{7}$$

$$4^3 = 4 \cdot 2 \equiv 1 \pmod{7}$$

Ennél a módszernél az elvégzett szorzások száma lényegesen kevesebb, mintha kiszámolnánk az összes köböt vagy negyedik hatványt. Minden újabb szorzással megkapjuk a megfelelő hatvány egy újabb lehetséges értékét. Ha már megvan a primitív gyök köbe, akkor az elvégzendő szorzások száma $\frac{p-1}{(3, p-1)} - 1$. Általánosan, ha modulo p ismerem egy primitív gyök k -adik hatványát, akkor az összes k -adik hatvány maradéka kiszámolható $\frac{p-1}{(k, p-1)} - 1$ szorzással.

A 3.1 táblázat első sorában y^3 lehetséges értékei: 0, 1, 6 szerepelnek, az első oszlopban x^4 lehetséges értékei: 0, 1, 2, 4. A táblázat többi eleme a megfelelő sor és oszlop különbsége modulo 7.

3.1. táblázat. $y^3 - x^4 \pmod{7}$

	0	1	6
0	0	1	6
1	6	0	5
2	5	6	4
4	3	4	2

Látható a táblázatból, hogy minden lehetséges maradékosztály előáll $y^3 - x^4$ különbségként modulo 7. Egy-egy értéket kiemeltünk zölddel. Így szerepel a 6 is, azaz a feladatunk nem oldható meg az általunk tervezett módszerrel modulo 7. Mivel minden maradék szerepel a táblázatban, ha lenne egy feladatunk, amiben x^4 , y^3 és egy konstans szerepel, az biztosan megoldható lenne modulo 7.

2. Próbálkozás

A következő $3k + 1$ alakú prím a 13. A 6 primitív gyök mod(13). A fenti stratégia alapján kiszámoljuk a harmadik hatványát mod(13), majd hatványozzuk. Kiszámoljuk a negyedik hatványát mod(13), és azt is hatványozzuk.

A köbszámok lehetséges maradékai modulo 13 nem mások, mint a 6^3 hatványai és a 0.

$$\begin{aligned} 6^3 &= 36 \cdot 6 \equiv 10 \cdot 6 = 60 \equiv 8 \pmod{13} \\ 8^2 &= 8 \cdot 8 \equiv (-5) \cdot (-5) \equiv 25 \equiv 12 \pmod{13} \\ 8^3 &= 8^2 \cdot 8 \equiv 12 \cdot 8 \equiv 96 \equiv 5 \pmod{13} \\ 8^4 &= 8^2 \cdot 8^2 \equiv 12 \cdot 12 \equiv 144 \equiv 1 \pmod{13} \end{aligned}$$

A negyedik hatványok lehetséges maradékai modulo 13 pedig nem mások, mint 6^4 hatványai és a 0.

$$\begin{aligned} 6^4 &= 36 \cdot 36 \equiv (-3) \cdot (-3) \equiv 9 \pmod{13} \\ 9^2 &= 9 \cdot 9 \equiv 81 \equiv 3 \pmod{13} \\ 9^3 &= 9 \cdot 9^2 \equiv 9 \cdot 3 \equiv 1 \pmod{13} \end{aligned}$$

A 3.2 táblázat első sorában y^3 lehetséges értékei: 0, 1, 5, 8, 12 szerepelnek, az első oszlopban x^4 lehetséges értékei: 0, 1, 3, 9. A táblázat többi eleme a megfelelő sor és oszlop különbsége modulo 13.

3.2. táblázat. $y^3 - x^4 \pmod{13}$

	0	1	5	8	12
0	0	1	5	8	12
1	12	0	4	7	11
3	10	11	2	5	9
9	4	5	9	12	3

Látható a táblázatból, hogy a 6-ot kivéve minden lehetséges maradékosztály előáll különbséggént modulo 13. Egy-egy értéket kiemeltünk zölddel. Mivel a 6 nem szerepel a táblázatban, így az a feladatunk, hogy $y^3 = x^4 + 6$ nem oldható meg mod(13), tehát az egyenletnek nincs megoldása az egész számok körében. Az is látható, hogy a 6 az egyetlen olyan maradékosztály, amely nem szerepel a táblázatban.

3-7. Próbálkozás

A következő néhány $3k + 1$ alakú prím a 19, 31, 37, 43, 61. Most kipróbáljuk a módszerünket ezekre a prímekekre:

A 10 primitív gyök mod(19). Kiszámoljuk a harmadik hatványát mod(19), majd hatványozzuk. Kiszámoljuk a negyedik hatványát mod(19), majd hatványozzuk. A köbszámok

lehetséges maradékai modulo 19 nem mások, mint a 10^3 hatványai és a 0.

$$\begin{aligned}
 10^3 &= 100 \cdot 10 \equiv 5 \cdot 10 \equiv 12 \pmod{19} \\
 12^2 &= 12 \cdot 12 \equiv 144 \equiv 11 \pmod{19} \\
 12^3 &= 144 \cdot 12 \equiv 11 \cdot 12 \equiv 18 \pmod{19} \\
 12^4 &= 12^2 \cdot 12^2 \equiv 11 \cdot 11 \equiv 7 \pmod{19} \\
 12^5 &= 12^4 \cdot 12 \equiv 7 \cdot 12 \equiv 8 \pmod{19} \\
 12^6 &= 12^3 \cdot 12^3 \equiv (-1) \cdot (-1) \equiv 1 \pmod{19}
 \end{aligned}$$

A negyedik hatványok lehetséges maradékai modulo 19 pedig nem mások, mint a 10^4 hatványai és a 0.

$$\begin{aligned}
 10^4 &= 100 \cdot 100 \equiv 5 \cdot 5 \equiv 6 \pmod{19} \\
 6^2 &= 6 \cdot 6 \equiv 36 \equiv 17 \pmod{19} \\
 6^3 &= 6^2 \cdot 6 \equiv 17 \cdot 6 \equiv 7 \pmod{19} \\
 6^4 &= 6^2 \cdot 6^2 \equiv (-2) \cdot (-2) \equiv 4 \pmod{19} \\
 6^5 &= 6^4 \cdot 6 \equiv 4 \cdot 6 \equiv 5 \pmod{19} \\
 6^6 &= 6^5 \cdot 6 \equiv 5 \cdot 6 \equiv 11 \pmod{19} \\
 6^7 &= 6^6 \cdot 6 \equiv 11 \cdot 6 \equiv 9 \pmod{19} \\
 6^8 &= 6^7 \cdot 6 \equiv 9 \cdot 6 \equiv 16 \pmod{19} \\
 6^9 &= 6^4 \cdot 6^5 \equiv 4 \cdot 5 \equiv 1 \pmod{19}
 \end{aligned}$$

A 3.3 táblázat első sorában y^3 lehetséges értékei: 0, 1, 7, 8, 11, 12, 18 szerepelnek, az első oszlopban x^4 lehetséges értékei: 0, 1, 4, 5, 6, 7, 9, 11, 16, 17. A táblázat többi eleme a megfelelő sor és oszlop különbsége modulo 19.

3.3. táblázat. $y^3 - x^4 \pmod{19}$

	0	1	7	8	11	12	18
0	0	1	7	8	11	12	18
1	18	0	6	7	10	11	17
4	15	16	3	4	7	8	14
5	14	15	2	3	6	7	13
6	13	14	1	2	5	6	12
7	12	13	0	1	4	5	11
9	10	11	17	18	2	3	9
11	8	9	15	16	0	1	7
16	3	4	10	11	14	15	2
17	2	3	9	10	13	14	1

Látható a táblázatból, hogy minden lehetséges különbség előáll modulo 19. Egy-egy értéket kiemeltünk zölddel. Mivel minden maradék szerepel a táblázatban, ha lenne egy feladatunk, amiben x^4 , y^3 és egy konstans szerepel, az biztosan megoldható lenne modulo 19.

A következő $3k + 1$ alakú prím a **31**. A 17 primitív gyök mod(31). A fenti módszer alapján kiszámoljuk a harmadik hatványát mod(31), majd hatványozzuk. Kiszámoljuk a negyedik hatványát mod(31), majd hatványozzuk. A számolás menetét már nem, csak a végeredményt rögzítjük. A könnyebb áttekinthetőség érdekében az eredményeket táblázatban rögzítjük. A harmadik hatványok:

	17^3	15^2	15^3	15^4	15^5	15^6	15^7	15^8	15^9	15^{10}
mod (31)	15	8	27	2	30	16	23	4	29	1

A negyedik hatványok:

	17^4	7^2	7^3	7^4	7^5	7^6	7^7	7^8	7^9	7^{10}	7^{11}	7^{12}	7^{13}	7^{14}	7^{15}
mod (31)	7	18	2	14	5	4	28	10	8	25	20	16	19	9	1

Ez alapján x^4 lehetséges értékei mod(31): 0, 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28. Az y^3 lehetséges értékei mod(31): 0, 1, 2, 4, 8, 15, 16, 23, 27, 29, 30.

A 3.4 táblázat első sorában y^3 lehetséges értékei: 0, 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 szerepelnek, az első oszlopban x^4 lehetséges értékei: 0, 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28. A táblázat többi eleme a megfelelő sor és oszlop különbsége modulo 31.

3.4. táblázat. $y^3 - x^4 \pmod{31}$

	0	1	2	4	8	15	16	23	27	29	30
0	0	1	2	4	8	15	16	23	27	29	30
1	30	0	1	3	7	14	15	22	26	28	29
2	29	30	0	2	6	13	14	21	25	27	28
4	27	28	29	0	4	11	12	19	23	25	26
5	26	27	28	30	3	10	11	18	22	24	25
7	24	25	26	28	1	8	9	16	20	22	23
8	23	24	25	27	0	7	8	15	19	21	22
9	22	23	24	26	30	6	7	14	18	20	21
10	21	22	23	25	29	5	6	13	17	19	20
14	17	18	19	21	25	1	2	9	13	15	16
16	15	16	17	19	23	30	0	7	11	13	14
18	13	14	15	17	21	28	29	5	9	11	12
19	12	13	14	16	20	27	28	4	8	10	11
20	11	12	13	15	19	26	27	3	7	9	10
25	6	7	8	10	14	21	22	29	2	4	5
28	3	4	5	7	11	18	19	26	30	1	2

Látható a táblázatból, hogy minden lehetséges különbség előáll modulo 31. Egy-egy értéket kiemeltünk zölddel. Mivel minden maradék szerepel a táblázatban, ha lenne egy

feladatunk, amiben x^4 , y^3 és egy konstans szerepel, az biztosan megoldható lenne modulo 31.

A következő $3k + 1$ alakú prím a **37**. Az 5 primitív gyök mod(37). A fenti módszer alapján kiszámoljuk a harmadik hatványát mod(37), majd hatványozzuk. Kiszámoljuk a negyedik hatványát mod(37), majd hatványozzuk. A számolás menetét már nem, csak a végeredményt rögzítjük. A könnyebb áttekinthetőség érdekében az eredményeket táblázatban rögzítjük. A harmadik hatványok:

	5^3	14^2	14^3	14^4	14^5	14^6	14^7	14^8	14^9	14^{10}	14^{11}	14^{12}
mod (37)	14	11	6	10	29	36	23	26	31	27	8	1

A negyedik hatványok:

	5^4	33^2	33^3	33^4	33^5	33^6	33^7	33^8	33^9
mod (37)	33	16	10	34	12	26	7	9	1

A táblázat elemei a megfelelő sor és oszlop különbsége modulo 37.

3.5. táblázat. $y^3 - x^4 \pmod{37}$

	0	1	6	8	10	11	14	23	26	27	29	31	36
0	0	1	6	8	10	11	14	23	26	27	29	31	36
1	36	0	5	7	9	10	13	22	25	26	28	30	35
7	30	31	36	1	3	4	7	16	19	20	22	24	29
9	28	29	34	36	1	2	5	14	17	18	20	22	27
10	27	28	33	35	0	1	4	13	16	17	19	21	26
12	25	26	31	33	35	36	2	11	14	15	17	19	24
16	21	22	27	29	31	32	35	7	10	11	13	15	20
26	11	12	17	19	21	22	25	34	0	1	3	5	10
33	4	5	10	12	14	15	18	27	30	31	33	35	3
34	3	4	9	11	13	14	17	26	29	30	32	34	2

Látható a táblázatból, hogy minden lehetséges különbség előáll modulo 37. Egy-egy értéket kiemeltünk zölddel. Mivel minden maradék szerepel a táblázatban, ha lenne egy feladatunk, amiben x^4 , y^3 és egy konstans szerepel, az biztosan megoldható lenne modulo 37.

A következő $3k + 1$ alakú prím a **43**. A 28 primitív gyök mod(43). A fenti módszer alapján kiszámoljuk a harmadik hatványát mod(43), majd hatványozzuk. Kiszámoljuk a negyedik hatványát mod(43), majd hatványozzuk. A harmadik hatványok:

	28^3	22^2	22^3	22^4	22^5	22^6	22^7	22^8	22^9	22^{10}	22^{11}	22^{12}	22^{13}	22^{14}
mod (43)	22	11	27	35	39	41	42	21	32	16	8	4	2	1

A negyedik hatványok:

	28^4	14^2	14^3	14^4	14^5	14^6	14^7	14^8	14^9	14^{10}	14^{11}
mod (43)	14	24	35	17	23	21	36	31	4	13	10
	14^{12}	14^{13}	14^{14}	14^{15}	14^{16}	14^{17}	14^{18}	14^{19}	14^{20}	14^{21}	
mod (43)	11	25	6	41	15	38	16	9	40	1	

3.6. táblázat. $y^3 - x^4 \pmod{43}$

	0	1	2	4	8	11	16	21	22	27	32	35	39	41	42
0	0	1	2	4	8	11	16	21	22	27	32	35	39	41	42
1	42	0	1	3	7	10	15	20	21	26	31	34	38	40	41
4	39	40	41	0	4	7	12	17	18	23	28	31	35	37	38
6	37	38	39	41	2	5	10	15	16	21	26	29	33	35	36
9	34	35	36	38	42	2	7	12	13	18	23	26	30	32	33
10	33	34	35	37	41	1	6	11	12	17	22	25	29	31	32
11	32	33	34	36	40	0	5	10	11	16	21	24	28	30	31
13	30	31	32	34	38	41	3	8	9	14	19	22	26	28	29
14	29	30	31	33	37	40	2	7	8	13	18	21	25	27	28
15	28	29	30	32	36	39	1	6	7	12	17	20	24	26	27
16	27	28	29	31	35	38	0	5	6	11	16	19	23	25	26
17	26	27	28	30	34	37	42	4	5	10	15	18	22	24	25
21	22	23	24	26	30	33	38	0	1	6	11	14	18	20	21
23	20	21	22	24	28	31	36	41	42	4	9	12	16	18	19
24	19	20	21	23	27	30	35	40	41	3	8	11	15	17	18
25	18	19	20	22	26	29	34	39	40	2	7	10	14	16	17
31	12	13	14	16	20	23	28	33	34	39	1	4	8	10	11
35	8	9	10	12	16	19	24	29	30	35	40	0	4	6	7
36	7	8	9	11	15	18	23	28	29	34	39	42	3	5	6
38	5	6	7	9	13	16	21	26	27	32	37	40	1	3	4
40	3	4	5	7	11	14	19	24	25	30	35	38	42	1	2
41	2	3	4	6	10	13	18	23	24	29	34	37	41	0	1

Látható a táblázatból, hogy minden lehetséges különbség előáll modulo 43. Egy-egy értéket kiemeltünk zölddel. Mivel minden maradék szerepel a táblázatban, ha lenne egy feladatunk, amiben x^4 , y^3 és egy konstans szerepel, az biztosan megoldható lenne modulo 43.

A következő $3k + 1$ alakú prím a **61**. A 10 primitív gyök mod(61). A fenti módszer alapján a harmadik hatványok:

	10^3	24^2	24^3	24^4	24^5	24^6	24^7	24^8	24^9	24^{10}
mod (61)	24	27	38	58	50	41	8	9	33	60
	24^{11}	24^{12}	24^{13}	24^{14}	24^{15}	24^{16}	24^{17}	24^{18}	24^{19}	24^{20}
mod (61)	37	34	23	3	11	20	53	52	28	1

A negyedik hatványok:

	10^4	57^2	57^3	57^4	57^5	57^6	57^7	57^8	57^9	57^{10}
mod (61)	57	16	58	12	13	9	25	22	34	47
	57^{11}	57^{12}	57^{13}	57^{14}	57^{15}					
mod (61)	56	20	42	15	1					

3.7. táblázat. $y^3 - x^4 \pmod{61}$

	0	1	9	12	13	15	16	20	22	25	34	42	47	56	57	58
0	0	1	9	12	13	15	16	20	22	25	34	42	47	56	57	58
1	60	0	8	11	12	14	15	19	21	24	33	41	46	55	56	57
3	58	59	6	9	10	12	13	17	19	22	31	39	44	53	54	55
8	53	54	1	4	5	7	8	12	14	17	26	34	39	48	49	50
9	52	53	0	3	4	6	7	11	13	16	25	33	38	47	48	49
11	50	51	59	1	2	4	5	9	11	14	23	31	36	45	46	47
20	41	42	50	53	54	56	57	0	2	5	14	22	27	36	37	38
23	38	39	47	50	51	53	54	58	60	2	11	19	24	33	34	35
24	37	38	46	49	50	52	53	57	59	1	10	18	23	32	33	34
27	34	35	43	46	47	49	50	54	56	59	7	15	20	29	30	31
28	33	34	42	45	46	48	49	53	55	58	6	14	19	28	29	30
33	28	29	37	40	41	43	44	48	50	53	1	9	14	23	24	25
34	27	28	36	39	40	42	43	47	49	52	0	8	13	22	23	24
37	24	25	33	36	37	39	40	44	46	49	58	5	10	19	20	21
38	23	24	32	35	36	38	39	43	45	48	57	4	9	18	19	20
41	20	21	29	32	33	35	36	40	42	45	54	1	6	15	16	17
50	11	12	20	23	24	26	27	31	33	36	45	53	58	6	7	8
52	9	10	18	21	22	24	25	29	31	34	43	51	56	4	5	6
53	8	9	17	20	21	23	24	28	30	33	42	50	55	3	4	5
58	3	4	12	15	16	18	19	23	25	28	37	45	50	59	60	61
60	1	2	10	13	14	16	17	21	23	26	35	43	48	57	58	59

Látható a táblázatból, hogy minden lehetséges különbség előáll modulo 61. Egy-egy értéket kiemeltünk zölddel.

Senkitől nem várható el, hogy egy ilyen feladatot modulo 61-ig vizsgáljon. Mi a teljesség kedvéért kipróbáltuk, de ennél nagyobb prímekre nem vizsgáljuk. Fölmerül a kérdés, hogy vajon találunk-e ellentmondást modulo valamilyen nagyobb prímszám. Mind az igen mind a nem irányába tudnánk heurisztikus érveket mondani...

3.3.3. Második feladatunk

6. Feladat. Határozzuk meg az $y^5 - x^4 = 12$ egyenlet összes egész megoldását.

A startégiánk az előző feladathoz hasonlóan egy q prím vagy prímszám választása, majd az egyenlet két oldalának vizsgálata modulo q . Amennyiben az egyenletben lévő kitevő relatív prím $\varphi(q)$ -hoz, akkor a megfelelő tag „szinte minden” értéket fölvehet modulo q .

Szerencsére ilyen szempontból a 4-gyel nem kell törődnünk, az $5k + 1$ alakú prímek mind $10k + 1$ alakúak is egyben.

1-3. Próbálkozás

Az első prím ahol $p - 1$ osztható 5-tel, a 11. A következő prímszám, melyre teljesül, hogy $\varphi(q)$ osztható öttel, a 25, $\varphi(25) = 20$, és megnézzük még az egyenletünket modulo 41 is.

Először Tekintsük y^5 és x^4 lehetséges értékeit modulo 11. A 2 primitív gyök mod(11). Kiszámoljuk az ötödik hatványát mod(11), majd hatványozzuk. Kiszámoljuk a negyedik hatványát mod(11), majd hatványozzuk. A számolás menetét már nem, csak a végeredményt rögzítjük. Az ötödik hatványok:

	2^5	10^2
mod (11)	10	1

A negyedik hatványok:

	2^4	5^2	5^3	5^4	5^5
mod (11)	5	3	4	9	1

3.8. táblázat. $y^5 - x^4 \pmod{11}$

	0	1	10
0	0	1	10
1	10	0	9
3	8	9	7
4	7	8	6
5	6	7	5
9	2	3	1

Látható a táblázatból, hogy a 4-et kivéve minden lehetséges különbség előáll modulo 11. Egy-egy értéket kiemeltünk zölddel. Mivel a 4 nem szerepel, az az egyenlet, hogy $y^5 = x^4 + 4$ nem oldható meg mod(11), ezért az egyenletnek nincs megoldása az egész számok körében. Az 1 viszont szerepel, és $12 \equiv 1 \pmod{11}$, tehát a feladatunk nem oldható meg az általunk tervezett módszerrel modulo 11.

Térjünk át a mod(25) esetre. A 2 primitív gyök mod(25). Kiszámoljuk a 2 ötödik hatványát mod(25), majd hatványozzuk. Kiszámoljuk a negyedik hatványát is mod(25), majd hatványozzuk. A számolás menetét már nem, csak a végeredményt rögzítjük. Az ötödik hatványok:

	2^5	7^2	7^3	7^4
mod (25)	7	24	18	1

A negyedik hatványok:

	2^4	16^2	16^3	16^4	16^5
mod (25)	16	6	21	11	1

3.9. táblázat. $y^5 - x^4 \pmod{25}$

	0	1	7	18	24
0	0	1	7	18	24
1	24	0	6	17	23
6	19	20	1	12	18
11	14	15	21	7	13
16	9	10	16	2	8
21	4	5	11	22	3

Látható a táblázatból, hogy minden lehetséges különbség előáll modulo 25. Egy-egy értéket kiemeltünk zölddel. Így szerepel a 12 is, azaz a feladatunk nem oldható meg az általunk tervezett módszerrel modulo 25. Mivel minden maradék szerepel a táblázatban, ha lenne egy feladatunk, amiben x^4 , y^5 és egy konstans szerepel, az biztosan megoldható lenne modulo 25.

Az utolsó $5k+1$ alakú prím, amit tekintünk a 41. A 6 primitív gyök mod(41). A számolás menetét már nem, csak a végeredményt rögzítjük. Az ötödik hatványok:

	6^5	27^2	27^3	27^4	27^5	27^6	27^7	27^8
mod (41)	27	32	3	40	14	9	38	1

A negyedik hatványok:

	6^4	25^2	25^3	25^4	25^5	25^6	25^7	25^8	25^9	25^{10}
mod (41)	25	10	4	18	40	16	31	37	23	1

3.10. táblázat. $y^5 - x^4 \pmod{41}$

	0	1	3	9	14	27	32	38	40
0	0	1	3	9	14	27	32	38	40
1	40	0	2	8	13	26	31	37	39
4	37	38	40	5	10	23	28	34	36
10	31	32	34	40	4	17	22	28	30
16	25	26	28	34	39	11	16	22	24
18	23	24	26	32	37	9	14	20	22
23	18	19	21	27	32	4	9	15	17
25	16	17	19	25	30	2	7	13	15
31	10	11	13	19	24	37	1	7	9
37	4	5	7	13	18	31	36	1	3
40	1	2	4	10	15	28	33	39	0

Látható a táblázatból, hogy a 6, 12, 29 és a 35 nem áll elő különbséggként $\text{mod}(41)$. Egy-egy értéket kiemeltünk zölddel. Mivel a 6, 12, 29 és 35 nem szerepelnek, az $y^5 = x^4 + 6$, $y^5 = x^4 + 12$, $y^5 = x^4 + 29$ és $y^5 = x^4 + 35$ egyenleteknek nincs megoldásuk modulo 41, tehát az egyenleteknek nincs megoldása az egész számok körében. Ezek között szerepel az általunk kitűzött feladat is, tehát az egyenletnek nincs megoldása az egész számok körében.

3.3.4. Harmadik feladatunk

7. Feladat. Határozzuk meg az $y^7 - x^4 = 3$ egyenlet összes egész megoldását.

A stratégiánk az előző feladathoz hasonlóan egy q prím vagy prímhatalvány választása, majd az egyenlet két oldalának vizsgálata modulo q . Most a $14k + 1$ alakú prímeket érdemes vizsgálni.

1. Próbálkozás

Az első prím ahol $p - 1$ osztható 7-tel, a 29. Tekintsük y^7 és x^4 lehetséges értékeit modulo 29. A 10 primitív gyök $\text{mod}(29)$. Kiszámoljuk a hetedik hatványát $\text{mod}(29)$, majd hatványozzuk. Kiszámoljuk a negyedik hatványát $\text{mod}(29)$, majd hatványozzuk. A számolás menetét már nem, csak a végeredményt rögzítjük. A hetedik hatványok:

	10^7	17^2	17^3	17^4
$\text{mod}(29)$	17	28	12	1

A negyedik hatványok:

	10^4	24^2	24^3	24^4	24^5	24^6	24^7
$\text{mod}(29)$	24	25	20	16	7	23	1

3.11. táblázat. $y^7 - x^4 \text{ mod}(29)$

	0	1	12	17	28
0	0	1	12	17	28
1	28	0	11	16	27
7	22	23	5	10	21
16	13	14	25	1	12
20	9	10	21	26	8
23	6	7	18	23	5
24	5	6	17	22	4
25	4	5	16	21	3

Látható a táblázatból, hogy a 2, 15, 19, 20 és 24 nem áll elő különbséggként $\text{mod}(29)$. Egy-egy értéket kiemeltünk zölddel. A 3 szerepel, így a feladatunk nem oldható meg az általunk tervezett módszerrel modulo 29. Azok az egyenletek, hogy $y^7 = x^4 + 2$, $y^7 = x^4 + 15$, $y^7 = x^4 + 19$, $y^7 = x^4 + 20$ és $y^7 = x^4 + 24$ viszont nem oldhatóak meg $\text{mod}(29)$, tehát az egyenleteknek nincs megoldása az egész számok körében.

2. Próbálkozás

A következő prím ahol $p - 1$ osztható 7-tel, a 43. Tekintsük y^7 és x^4 lehetséges értékeit modulo 43. A 28 primitív gyök mod(43). A hetedik hatványok:

	28^7	7^2	7^3	7^4	7^5	7^6
mod (43)	7	6	42	36	37	1

A negyedik hatványok:

	28^4	14^2	14^3	14^4	14^5	14^6	14^7	14^8	14^9	14^{10}	14^{11}
mod (43)	14	24	35	17	23	21	36	31	4	13	10
	14^{12}	14^{13}	14^{14}	14^{15}	14^{16}	14^{17}	14^{18}	14^{19}	14^{20}	14^{21}	
mod (43)	11	25	6	41	15	38	16	9	40	1	

3.12. táblázat. $y^7 - x^4 \pmod{43}$

	0	1	6	7	36	37	42
0	0	1	6	7	36	37	42
1	42	0	5	6	35	36	41
4	39	40	2	3	32	33	38
6	37	38	0	1	30	31	36
9	34	35	40	41	27	28	33
10	33	34	39	40	26	27	32
11	32	33	38	39	25	26	31
13	30	31	36	37	23	24	29
14	29	30	35	36	22	23	28
15	28	29	34	35	21	22	27
16	27	28	33	34	20	21	26
17	26	27	32	33	19	20	25
21	22	23	28	29	15	16	21
23	20	21	26	27	13	14	19
24	19	20	25	26	12	13	18
25	18	19	24	25	11	12	17
31	12	13	18	19	5	6	11
35	8	9	14	15	1	2	7
36	7	8	13	14	0	1	6
38	5	6	11	12	41	42	4
40	3	4	9	10	39	40	2
41	2	3	8	9	38	39	1

Látható a táblázatból, hogy minden lehetséges különbség előáll modulo 43. Egy-egy értéket kiemeltünk zölddel. Így szerepel a 3 is, azaz a feladatunk nem oldható meg az általunk tervezett módszerrel modulo 43. Mivel minden maradék szerepel a táblázatban, ha lenne egy feladatunk, amiben x^4 , y^7 és egy konstans szerepel, az biztosan megoldható lenne modulo 43.

Harmadik próbálkozás

A következő prím ahol $p - 1$ osztható 7-tel, a 71. Tekintsük y^7 és x^4 lehetséges értékeit modulo 71.

A 62 primitív gyök mod(71). Kiszámoljuk a hetedik hatványát mod(71), majd hatványozzuk. Kiszámoljuk a negyedik hatványát mod(71), majd hatványozzuk.

A számolás menetét már nem, csak a végeredményt rögzítjük.

A hetedik hatványok:

	62^7	17^2	17^3	17^4	17^5	17^6	17^7	17^8	17^9	17^{10}
mod (71)	17	5	14	25	70	54	66	57	46	1

A negyedik hatványok:

	62^4	29^2	29^3	29^4	29^5	29^6	29^7	29^8	29^9	29^{10}	29^{11}	29^{12}
mod (71)	29	60	36	50	30	18	25	15	9	48	43	40
	29^{13}	29^{14}	29^{15}	29^{16}	29^{17}	29^{18}	29^{19}	29^{20}	29^{21}	29^{22}	29^{23}	29^{24}
mod (71)	24	57	20	12	64	10	6	32	5	3	16	38
	29^{25}	29^{26}	29^{27}	29^{28}	29^{29}	29^{30}	29^{31}	29^{32}	29^{33}	29^{34}	29^{35}	
mod (71)	37	8	19	54	4	45	27	2	58	49	1	

A 3.13 táblázat első sorában y^7 lehetséges értékei: 0, 1, 5, 14, 17, 25, 46, 54, 57, 66, 70 szerepelnek, az első oszlopában x^4 lehetséges értékei: 0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 19, 20, 24, 25, 27, 29, 30, 32, 36, 37, 38, 40, 43, 45, 48, 49, 50, 54, 57, 58, 60, 64. A táblázat többi eleme a megfelelő sor és oszlop különbsége modulo 71.

Látható a táblázatból, hogy minden lehetséges különbség előáll modulo 71. Egy-egy értéket kiemeltünk zölddel. Így szerepel a 3 is, azaz a feladatunk nem oldható meg az általunk tervezett módszerrel modulo 71. Mivel minden maradék szerepel a táblázatban, ha lenne egy feladatunk, amiben x^4 , y^7 és egy konstans szerepel, az biztosan megoldható lenne modulo 71.

3.13. táblázat. $y^7 - x^4 \pmod{71}$

	0	1	5	14	17	25	46	54	57	66	70
0	0	1	5	14	17	25	46	54	57	66	70
1	70	0	4	13	16	24	45	53	56	65	69
2	69	70	3	12	15	23	44	52	55	64	68
3	68	69	2	11	14	22	43	51	54	63	67
4	67	68	1	10	13	21	42	50	53	62	66
5	66	67	0	9	12	20	41	49	52	61	65
6	65	66	70	8	11	19	40	48	51	60	64
8	63	64	68	6	9	17	38	46	49	58	62
9	62	63	67	5	8	16	37	45	48	57	61
10	61	62	66	4	7	15	36	44	47	56	60
12	59	60	64	2	5	13	34	42	45	54	58
15	56	57	61	70	2	10	31	39	42	51	55
16	55	56	60	69	1	9	30	38	41	50	54
18	53	54	58	67	70	7	28	36	39	48	52
19	52	53	57	66	69	6	27	35	38	47	51
20	51	52	56	65	68	5	26	34	37	46	50
24	47	48	52	61	64	1	22	30	33	42	46
25	46	47	51	60	63	0	21	29	32	41	45
27	44	45	49	58	61	69	19	27	30	39	43
29	42	43	47	56	59	67	17	25	28	37	41
30	41	42	46	55	58	66	16	24	27	36	40
32	39	40	44	53	56	64	14	22	25	34	38
36	35	36	40	49	52	60	10	18	21	30	34
37	34	35	39	48	51	59	9	17	20	29	33
38	33	34	38	47	50	58	8	16	19	28	32
40	31	32	36	45	48	56	6	14	17	26	30
43	28	29	33	42	45	53	3	11	14	23	27
45	26	27	31	40	43	51	1	9	12	21	25
48	23	24	28	37	40	48	69	6	9	18	22
49	22	23	27	36	39	47	68	5	8	17	21
50	21	22	26	35	38	46	67	4	7	16	20
54	17	18	22	31	34	42	63	0	3	12	16
57	14	15	19	28	31	39	60	68	0	9	13
58	13	14	18	27	30	38	59	67	70	8	12
60	11	12	16	25	28	36	57	65	68	6	10
64	7	8	12	21	24	32	53	61	64	2	6

3.3.5. Meddig érdemes az egyenleteinket vizsgálni?

A 3.3 fejezet feladatainak megoldását mindig egy prím vagy prímhatvány választásával kezdtük. Utána megnéztük, hogy modulo a prím megegyezhet-e a két oldal. Néha találtunk olyan prímet, ahol a két oldal nem volt egyenlő, így az eredeti egyenletnek nem lehetett megoldása. Fölmerül a kérdés, hogy igaz-e itt is a közmodás, hogy türelem rózsát terem. Azaz, igaz-e

az alábbi állítás:

(*) Ha egy diofantikus egyenletnek nincs egész megoldása, akkor van olyan prímszám, hogy modulo az a prím sincs megoldása.

Ennek a kérdésnek az eldöntése nem volt egyszerű. Egyrészt gondolhatja azt az ember, hogy modulo nagyobb prím több maradékosztály van, így nagyobb esély van arra, hogy valami nem áll elő különbségként. Másrészt az x^n polinom $\frac{p-1}{(n, p-1)} + 1$ értéket vesz föl, így az $y^3 - x^4 = 3$ egyenlet baloldalára összesen legalább $\frac{(p-1)^2}{12}$ helyettesítési érték adódik, amelyek nem mind különbözőek, ám átlagosan minden értéket $\frac{p-1}{12}$ -szer vesz fel. Mindkét érvelés mögött lehet logika.

Megkérdeztünk három matematikus kutatót a kédről. A feladatunk számelméleti jellegű, így először Zábrádi Gergely tanár urat és Harcos Gergely tanár urat kerestük meg. Mindketten a szakterületük világszerte elismert kutatói. Mindketten hamar visszajelezték, Zábrádi Gergely a következőket mondta:

Algebrai görbék méretére van egy tétel, Hasse-tétele. Elliptikus görbékre biztosan. A ti egyik görbétek elliptikus görbe. Azt mondja ki, hogy nagyjából annyi pontja van, mint amennyit elvár az ember. Az ettől való eltérés kicsi, gyökös. Szerintem van ilyen magasabb fokú egyenletekre is, a génusz segítségével. Nektek, ugye összesen $\frac{x}{3} \cdot \frac{x}{4}$, azaz négyzetesen sok értékek van, így a baloldal minden értéket sokszor felvesz

Harcos Gergely készített egy bizonyítást arra, hogy nagy prímek esetén a baloldal minden értéket fölvesz, majd megadott két hivatkozást a korlátra. Az egyik a Hasse-formula, a másik Weil tétele [23] specális alakú egyenletek megoldásszámáról. Ezek alapján kétoldaltól is megközelíthető a kérdés. mindkettőnek megvannak az előnyei és a korlátai. A Hasse-formula [8] általánosítása kétváltozós polinomokról szól, és génusz-elemszám formula néven ismert. Ez az a becslés, amire Zábrádi Gergely is utalt.

2. Tétel. (Hasse-Weil korlát) Legyen C egy $\mathbf{g}$ génuszú algebrai görbe, q egy prímszám. Jelölje $\#C(\mathbb{F}_q)$ a görbe pontjainak számát a q elemű test fölött. Ekkor

$$|\#C(\mathbb{F}_q) - (q + 1)| \leq 2\mathbf{g}\sqrt{q}$$

Algebrai görbén egy $F(x, y)$ kétváltozós (egész együtthatós) polinomot értünk, az algebrai görbe pontjai azok az (x, y) számpárok, amelyeket a polinomba helyettesítve 0-t kapunk. Tehát a mi $y^3 - x^4 = 3$ egyenletünk megoldásai az $F(x, y) = y^3 - x^4 - 3$ algebrai görbe pontjai. A megoldások száma pedig a pontok száma. Az hogy az egyenlet megoldható-e modulo p , az ugyanazt jelenti, hogy az algebrai görbe nem üres, azaz pontjainak száma legalább 1. Ha az abszolútérték jelet elhagyjuk, akkor a

$$\#C(\mathbb{F}_p) \geq p + 1 - 2\mathbf{g}\sqrt{p}$$

egyenlőtlenséghez jutunk, azaz ha

$$p + 1 - 2\mathbf{g}\sqrt{p} > 1$$

akkor a görbének van pontja. Ez az érték nem függ a konstanstól, ami az esetünkben 3. Átrendezve

$$p > 4\mathbf{g}^2$$

esetén a kifejezésünk felveszi a 3-t, sőt, minden értéket fölvesz modulo p .

A Harcos Gergely tanár úr által említett másik összefüggés a Weil-korlát [23], ami más típusú, de tetszőleges változó számú polinomokról szól.

3. Tétel. Legyen

$$F(x_1, x_2, \dots, x_n) = a_1 x_1^{k_1} + a_2 x_2^{k_2} + \dots + a_n x_n^{k_n},$$

ahol egyetlen a_i sem 0. Legyen p prímszám és $d_i = (k_i, p-1)$.

$$p > ((d_1 - 1)(d_2 - 1) \dots (d_n - 1))^2,$$

akkor az $F(x_1, x_2, \dots, x_n) = a$ egyenletnek van megoldása modulo p minden $a \in \mathbb{Z}$ esetén.

A mi $y^3 - x^4 = 3$ egyenletünkre ez közvetlenül alkalmazható. Fölmerül a kérdés, hogy a két becslés ugyanazt a korlátot adja-e. Ehhez meg kellett valahogy tudnunk, mi az a génusz. Erről Pintér Gergő (!!!) tanár urat kérdeztük meg, aki a PhD dolgozatát algebrai geometriából írta. Ő elmesélte, hogy sokféle hasonló génusz fogalom van (pl: algebrai, affin, projektív), mindegyik kicsit más, mindegyik kicsit ugyanaz, egymásból nem feltétlenül számolhatóak, és egyáltalán nem könnyű őket kezelni. Amit biztosan lehet mondani, hogy

$$\mathbf{g} = \frac{1}{2}(d-1)(d-2) - P,$$

ahol d a polinom fokát, a P szám általában valamilyen pólusok számát jelöli, és ez az érték nagyon függ az egyenlettől. A mi feladatunkra ez a pólus a [12] könyv 5.57-es formulájával számolható. Kiszámolta a génusz értékeket a mi egyenleteinkre, ám nem a pólusok, hanem az úgynevezett Milnor-szám segítségével. Az így kapott becslés megegyezett a Weil-korlással.

Megpróbáltuk értelmezni a hallottakat. Itt leírjuk a fentiek értelmezését, koncentrálva a minket érdeklő kérdésre. A felsorolt fogalmakat és tételeket természetesen nem mind értjük, de a végső összefüggés érthető lesz és hasznos.

4. Tétel. Legyen $F(x, y)$ egy kétváltozós d -edfokú polinom. Itt fokszámon az összfokszámot értjük, azaz például $\deg(x^3y - 2xy^2) = 4$. Ekkor, ha

$$p > ((d-1)(d-2))^2,$$

akkor az $F(x, y) = a$ egyenletnek van megoldása modulo p minden $a \in \mathbb{Z}$ esetén.

Ennek a tételnek egy speciális esete, amikor a 3 tétel feltételei is teljesülnek. Ha a feladat " $x^n - y^k = \text{konstans}$ " alakú, akkor a korlát felírható olyan alakban is, hogy:

$$((n-1) \cdot (k-1))^2 < p.$$

Ennél nagyobb prímeke minden lehetséges megoldás előáll. Ez alapján tudunk becslést adni olyan p prímre, amelynél kisebb prímre érdemes csak vizsgálni, nagyobbra nem, mert minden eredmény előáll modulo p .

Tekintsük először az $y^3 - x^4 = a$ típusú egyenleteket. A felső korlát:

$$((3-1) \cdot (4-1))^2 = (2 \cdot 3)^2 = 36$$

Ez azt jelenti, hogy az $y^3 - x^4 = a$ típusú egyenleteket 36-nál kisebb prímeke érdemes vizsgálni, mert a 36-nál nagyobb prímeke minden megoldás előfordul.

A következő típusú egyenletek az $y^5 - x^4 = b$ alakúak. A felső korlát ekkor:

$$((5-1) \cdot (4-1))^2 = (4 \cdot 3)^2 = 144$$

Ez azt jelenti, hogy az $y^5 - x^4 = b$ típusú egyenleteket 144-nél kisebb prímeke érdemes csak vizsgálni, mert a 144-nél nagyobb prímeke minden megoldás előfordul.

Tekintsük most az $y^7 - x^4 = c$ típusú egyenleteket. A felső korlát most:

$$((7-1) \cdot (4-1))^2 = (6 \cdot 3)^2 = 324$$

Ez azt jelenti, hogy az $y^7 - x^4 = c$ típusú egyenleteket 324-nél kisebb prímeke érdemes csak vizsgálni, 324-nél nagyobb prímeke minden megoldás előfordul.

Általában egy feladatmegoldó diáktól még egyetemi szinten sem várhatjuk el, hogy adott egyenletnél megnézzék a lehetséges értékeket 144-ig, vagy 324-ig minden alkalmas prímre. A tétel korlátja segítség mind a feladat megoldónak a megoldási módszerek alkalmazásában, mind a feladat kitűzőknek a megoldási módszerek kitalálásában.

Az eddig alkalmazott módszerrel nem jutottunk megoldáshoz, ezért más "trükköt" kell alkalmaznunk.

$y^7 = x^4 + 3$ - negyedik próbálkozás - Új módszer

Az egyenletünknek minden p -re van megoldása, így új trükkhöz kell folyamodnunk. Ebben a megoldásban próbáltuk ötvözni a kiindulási olimpiai feladat ötletét a kvadratikus maradékok bevonásával. Két esetet különböztetünk meg.

1. eset: Ha x páratlan

Hozzuk az egyenletet

$$y^7 = x^4 + 3$$

alakúra. Ha x páratlan, akkor x^4 is páratlan, és $x^4 \equiv 1 \pmod{8}$. Ekkor $(x^4 + 3)$ páros, és $x^4 + 3 \equiv 4 \pmod{8}$. Emiatt a bal oldalnak is párosnak kell lennie. Az y^7 akkor páros, ha y páros. Ha y páros, akkor $y^7 \equiv 0 \pmod{8}$. Ezzel ellentmondásra jutunk.

2. eset: Ha x páros

Hozzuk az egyenletet

$$y^7 - 1 = x^4 + 2$$

alakúra. Legyen $p \neq 2$ prím az $x^4 + 2$ egy prímosztója. A felírásból látható, hogy a -2 kvadratikusan maradék modulo p . Így a jobboldal minden prímosztója: $2, 8k + 1$ vagy $8k + 3$ alakú ezért ennek teljesülnie kell a bal oldalra is. Szorzattá alakítva a bal oldalt a következő kifejezéshez jutunk:

$$(y - 1) \cdot (y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = x^4 + 2$$

Ha x páros, akkor az $(x^4 + 2)$ is páros, és $x^4 + 2 \equiv 2 \pmod{8}$. Ez a baloldalra is teljesül. $y^7 \equiv 3 \pmod{8}$, ami csak akkor lehet, ha $y \equiv 3 \pmod{8}$. Ebben az esetben $(y - 1) \equiv 2 \pmod{8}$, és a másik tényező

$$3^6 + 3^5 + 3^4 + 3^3 + 3^2 + 3 + 1 \equiv 1 + 3 + 1 + 3 + 1 + 3 + 1 \equiv 5 \pmod{8}$$

Ezzel szintén ellentmondásra jutunk, tehát az egyenletnek nincs megoldása. $\square$

A fenti gondolatmenet egyik fő eleme a $y^6 + y^5 + y^4 + y^3 + y^2 + y + 1$ kifejezés 8-cal, vagy inkább 4-gyel vett maradéka. A módszer alkalmazható azokra az $y^n - x^4 = 3$ alakú egyenletekre, ahol $n \equiv -1 \pmod{4}$. Így például $y^3 - x^4 = 3$ egyenletnek sincs egész megoldása. $\square$

Ne gondoljuk, hogy egyszerű ilyen feladatokat készíteni a fentebb használt módszerek segítségével. Például az

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

egyenletnek megoldása $x = 2$ és $y = 5$.

Irodalomjegyzék

- [1] ALAN H. SCHOENFELD(2017), Thoughts on Pólya, Problem Solving and Where They Can Lead You in A Life's Time for Mathematics Education and Problem Solving. 370–377 WTM-Verlag https://www.edition-buchshop.de/buchshop-artikel-a_life%E2%80%99s_time_for_mathematics_education_and_problem_solving-2494.htm
- [2] Beke, Manó https://en.wikipedia.org/wiki/Emanuel_Beke
- [3] BRUNER, JEROME SEYMOUR(1960), The Process of education. Mass.: Harvard University Press. Cambridge
- [4] B. SZÉNÁSSY(1992), History of Mathematics in Hungary until the 20th Century, Berlin
- [5] CSÁNYI PETRA, FÁBIÁN KATA, SZABÓ ZSANETT(2016), Hogyan építsünk számelméletet? TDK dolgozat.
- [6] P. CSÁNYI, K. FÁBIÁN, CS. SZABÓ AND ZS. SZABÓ(2015), Number theory vs Hungarian high- school textbooks: The fundamental theorem of arithmetic, *Teaching Mathematics and Computer Science* **13**, no. 2 (2015), 219-223.
- [7] Competitions of students staying behind, http://matek.fazekas.hu/index.php?option=com_content&view=article&id=303&Itemid=268
- [8] DAVENPORT, HAROLD; HASSE, HELMUT (1935), "Die Nullstellen der Kongruenz-zetafunktionen in gewissen zyklischen Fällen. (On the zeros of the congruence zeta-functions in some cyclic cases)" *Journal für die reine und angewandte Mathematik* (1935) 151-182.
- [9] DR. KÁNTOR SÁNDORNÉ: Tudós matematikatanárok Hajdú, Szabolcs és Szolnok megye középiskoláiban (1850–1948) (<http://mek.oszk.hu/07200/07238/html/>) (in Hungarian)
- [10] Hungarian Problem Book, translation by Elvira Rapaport, <https://es.scribd.com/document/322771120/Hungarian-Problem-Book-I-Number-11-Bk-1-E-Rapaport>

- [11] Hungarian Problem Book (1963), see eg. amazon.com/Hungarian-Problem-Book-Number-English/dp/0883856115 Hungarian Problem Book I. Based on the Eötvös Competitions, 1894-1905 (120 pp.); Hungarian Problem Book II. Based on the Eötvös Competitions, 1906-1928 (128 pp.). József Kürschák. Revised and edited by G. Hajós, G. Neukomm, and J. Surányi. Translated from the Hungarian revised edition (1955) by Elvira Rapaport. Random House, New York; Singer, Syracuse, N. Y., 1963.
- [12] J.W.P. HIRSCHFELD, G. KORCHMAROS, F. TORRES(2009), Algebraic Curves over a Finite Field. 132–135
- [13] Kerettanterv 5-8. osztály. (2012), https://kerettanterv.oh.gov.hu/02_melleklet_5-8/index_alt_isk_felso.html (2020. május 08.)
Kerettanterv 9-12. osztály. (2012), https://kerettanterv.oh.gov.hu/03_melleklet_9-12/index_4_gimn.html
- [14] MARLIES BAETEN, FILIP DOCHY, KATRIEN STRUYVEN(2008) Students' approaches to learning and assessment preferences in a portfolio-based learning environment, *Instructional Science*, **36** 359-374.
- [15] MCLEOD, S. A.(2019), Bruner - learning theory in education. *Simply Psychology* <https://www.simplypsychology.org/bruner.html>
- [16] Mikola, Sándor https://hu.wikipedia.org/wiki/Mikola_S%C3%A1ndor
- [17] (2012), Nemzeti Alaptanterv.
https://ofi.oh.gov.hu/sites/default/files/attachments/mk_nat_20121.pdf
- [18] Problems of the oldest mathematical competitions of modern age in Hungary. http://matek.fazekas.hu/images/versenyek/orszagos/kurschak/ek_competitions_18942003.pdf
- [19] Rátz, László https://en.wikipedia.org/wiki/L%C3%A1szl%C3%B3_R%C3%A1tz
- [20] REUBEN HERSH and VERA JOHN-STEINER: A visit to Hungarian mathematics, *The Mathematical Intelligencer*, **15** (2) (1993) 13-26. https://www.researchgate.net/publication/226053312_A_visit_to_Hungarian_mathematics

- [21] VON H. DAVENPORT UND H. HASSE(1935), Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *Journal für die reine und angewandte Mathematik* (1935) 151-182. <http://www.digizeitschriften.de/dms/img/?PID=GDZPPN002173123>
- [22] Wieschenberg, A. (1990). The birth of Eotvos Competition. *The College Mathematics Journal*, 21 (4), 286–293.
- [23] WEIL, ANDRÉ(1949), Numbers of solutions of equations in finite fields, *Bulletin of the American Mathematical Society*, **55** (5): 497–508, doi:10.1090/S0002-9904-1949-09219-4 <https://www.projecteuclid.org/euclid.bams/1183513798>
- [24] WOOD, D. J., BRUNER, J. S., ROSS, G.(1976). The role of tutoring in problem solving. *Journal of Child Psychiatry and Psychology*, 17(2), 89-100.
- [25] <https://www.imo-official.org/problems/IMO2006SL.pdf>
- [26] <http://www.mategye.hu/download/cserepek/cserepek.pdf> (in Hungarian)
- [27] <http://medvematek.hu/en/>