Kombinatorikus problémák véges testek feletti terekben

Matematika BSc, elemző szakirány

Szakdolgozat

Témavezető:
Sziklai Péter

Eötvös Loránd Tudományegyetem
Természettudományi kar

Veres Gergely

2025

NYILATKOZAT

Név: Veres Gergely

ELTE Természettudományi Kar, szak: matematika

NEPTUN azonosító: KVSM8J

Szakdolgozat címe:
Kombinatorikus problémák véges testek feletti terekben

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2024

Veres Gergely

a hallgató aláírása

Köszönetnyilvánítás

Köszönöm szépen a családomnak, akik végig támogattak mindennel és mindenben. Volt olyan időszak, amikor csak azért nem adtam fel, mert bizonyítani akartam nekik. Innen nézve, már csak az is segítség volt, hogy nyerhettem belőlük motivációt. Köszönöm szépen az egyetem oktatóinak, hogy munkájukkal értékes tudásra tehettem szert. Köszönöm szépen az egyetemen szerzett barátaimnak a közös tanulásokat és a korrepetálásokat. Továbbá köszönöm Sziklai Péter témavezetőmnek, hogy türelemmel állt hozzám.

Tartalomjegyzék

Bevezetés

Szakdolgozatomban a véges testekkel foglalkozom. Mik azok? Hogyan képzeljük el őket? Mire használhatóak? A téma egészét nézve hatalmas, ezért az alapjait tekintem át, illetve a különböző területeken való felhasználást nézem meg.
Az elején definiálom a véges testeket, megnézem honnan eredeteztethetőek, illetve bevezetek pár - hozzájuk szorosan kapcsolódó - fogalmat. Ezt követően a felhasználási területeket veszem szemügyre. Levezetésképpen pedig bemutatok egy kombinatorikai problémát, melyet *python* segítségével vizsgáltam.
A szakdolgozatomhoz több különböző forrásból merítettem ihletet, az irodalomjegyzéket a dokumentum végén helyeztem el.

1. fejezet

Véges testek

Az első fejezetben megnézzük mi a kongruencia, mik a véges testek, majd ezt kiegészítjük néhány fontos, hozzájuk kapcsolódó definícióval, tétellel. [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11]

1.1. Kongruencia

A kongruencia a számelmélet egyik alapfogalma. Az oszthatósággal és a maradékokkal való számolással foglalkozik. Egy reláció, ami megnézi, hogy egy adott számhoz képest két szám osztási maradéka egyenlő-e.

Definíció

Legyen $a, b \in \mathbb{Z}$ tetszőleges egész szám, $m \in \mathbb{N}$ zérótól különböző természetes szám. Azt mondjuk, hogy a kongruens b-vel modulo m, azaz hogy a és b egészek m-mel vett osztási maradéka egyenlő, ha

$$m \mid (a - b)$$

azaz

$$\exists k \in \mathbb{Z} : a = km + b$$

Jelölése:

$$a \equiv b \pmod{m}$$

Lehet találkozni a következő jelölésekkel is:

$$a \equiv b \ (m)$$

$$a \equiv b \mod m$$

$$a \equiv b \mod m\mathbb{Z}$$

$$a \equiv_m b$$

Ha a nem kongruens b-vel modulo m, azt mondjuk, inkongruens vele, és $a \not\equiv b \pmod{m}$ alakban jelöljük.
Megjegyzés: a mod matematikai maradékképző függvény, a maradékos osztás maradékát rendeli a számhoz.

1.1.1. Euler-Fermat tétel

Az Euler-Fermat tétel egy fontos eredmény a számelméletben. A tétel kimondja, hogy ha a és m egész számok, ahol $m > 0$ és a relatív prím n-hez, akkor:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Itt $\phi(m)$ az Euler-féle fí-függvény, amely azon m-nél kisebb pozitív egész számok számát adja meg, amelyek relatív prímek m-hez.
A tétel bizonyításához fontos ismernünk a redukált maradékrendszer fogalmát.
Legyen a maradékosztály (mod m). Redukált maradékosztálynak nevezzük a-t, ha a és m relatív prímek.

Bizonyítás

Legyen $r_1, r_2, \ldots, r_{\varphi(m)}$ redukált maradékrendszer modulo m. Az $(a, m) = 1$ feltétel miatt az $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ maradékosztályok is redukált maradékrendszert alkotnak modulo m. Ekkor minden $1 \leq i \leq \varphi(m)$-hez létezik egyetlen olyan $1 \leq j \leq \varphi(m)$, amelyre $ar_i \equiv r_j \pmod{m}$. Jelöljük ezt az r_j-t s_i-vel. Ekkor:

$$ar_1 \equiv s_1 \pmod{m}$$

$$ar_2 \equiv s_2 \pmod{m}$$

$$\vdots$$

$$ar_{\varphi(m)} \equiv s_{\varphi(m)} \pmod{m}$$

A kongruenciákat összeszorozva kapjuk:

$$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv s_1 s_2 \ldots s_{\varphi(m)} \pmod{m}$$

ahol $r_1, r_2, \ldots, r_{\varphi(m)}$ számok az $s_1, s_2, \ldots, s_{\varphi(m)}$ számok egy permutációját alkotják. Ezért a kongruenciát felírhatjuk így:

$$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv r_1 r_2 \ldots r_{\varphi(m)} \pmod{m}$$

Mivel $(r_i, m) = 1$, ezért a kongruencia mindkét oldalát leoszthatjuk az összes r_i-vel, amiből

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

adódik.

Az előzőekből látszik, hogy érdemes tudni két szám legnagyobb közös osztóját. Ennek kiszámolására pedig van egy hatékony módszer.

1.1.2. Euklideszi algoritmus

Az euklideszi algoritmus két egész szám legnagyobb közös osztóját (LNKO) határozza meg. Az algoritmus alapelve az, hogy az egyik számot a másikból vett maradékok segítségével redukáljuk, míg végül a maradék nullává válik.

Algoritmus lépései

Legyen adott két pozitív egész szám, a és b, ahol $a \geq b$:

1. Ha $b = 0$, akkor $\text{LNKO}(a, b) = a$.
2. Különben határozzuk meg a és b osztási maradékát: $r = a \mod b$.
3. Cseréljük le a-t b-re, és b-t r-re.
4. Ismételjük a folyamatot, amíg b nullává nem válik. Az utolsó nem nulla b érték lesz a legnagyobb közös osztó.

Példa

Számoljuk ki a 217 és 182 legnagyobb közös osztóját:

$$\begin{aligned} 217 \div 182 = 1 \quad \text{maradék: } 35 \\ 217 = 1 \cdot 182 + 35 \\ 182 \div 35 = 5 \quad \text{maradék: } 7 \\ 182 = 5 \cdot 35 + 7 \\ 35 \div 7 = 5 \quad \text{maradék: } 0 \\ 35 = 5 \cdot 7 + 0 \end{aligned}$$

Az utolsó nem nulla maradék 7, így ez a két szám legnagyobb közös osztója.

Bizonyítás

Az euklideszi algoritmus bizonyítása az osztási algoritmust és az LNKO tulajdonságait veszi alapul.

Segédtétel

Ha $a = bq + r$, akkor $\text{LNKO}(a, b) = \text{LNKO}(b, r)$.

Bizonyítás

1. **Oszthatóság**: Ha d osztja a-t és b-t, akkor d osztja r-t is.

$$r = a - bq \quad \text{szerint } d \text{ osztja } a - bq\text{-t, azaz } r\text{-t.}$$

2. **Fordítva**: Ha d osztja b-t és r-t, akkor d osztja a-t is.

$$a = bq + r \quad \text{szerint } d \text{ osztja } bq\text{-t és } r\text{-t, így } d \text{ osztja } a\text{-t is.}$$

Tehát minden közös osztója a-nak és b-nek közös osztója b-nek és r-nek, és fordítva. Ezért $\text{LNKO}(a, b) = \text{LNKO}(b, r)$. Ez alapján az euklideszi algoritmus minden lépése csökkenti az egyik bemeneti értéket, amíg az egyikük nullává nem válik, és az utolsó nem nulla érték lesz a legnagyobb közös osztó.

1.2. Véges testek

Definíció - test

A test egy olyan algebrai struktúra, melyen az összeadás és a szorzás műveletek vannak definiálva. Az összeadás asszociatív és kommutatív. Létezik 0 elem, melyre igaz, hogy $a + 0 = a$ minden a-ra. Emellett minden elemnek létezik additív inverze úgy, hogy $a + (-a) = 0$.
A szorzás is asszociatív és kommutatív, illetve létezik egy egységelem, melyre igaz, hogy $a \cdot 1 = a$. Emelett minden nemnulla elemnek létezik multiplikatív inverze úgy, hogy $a \cdot a^{-1} = 1$. Végül igaz a disztributivitás is: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Definíció - véges test

A véges test egy olyan test, melynek véges számú eleme van és rendelkezik egy test alapvető tulajdonságaival. Egy véges test rendje prím vagy prímhatvány. Minden p prímre és k egészre léteznek olyan testek, melyeknek rendje p^k és az azonos méretűek izomorfak egymáshoz. A $q = p^k$ elemszámú testet F_q-val jelöljük.

Állítás:

Minden véges test elemszáma prímhatvány.

Bizonyítás: Legyen az F véges test karakterisztikája p, ahol p egy prím (egy test karakterisztikája az a legkisebb pozitív egész p, amelyre $p \cdot 1 = 0$, ahol 1 a test egységeleme. Ez azt jelenti, hogy az 1-et p alkalommal összeadjuk). Az 1 többszörösei egy P nevű résztestet alkotnak, amely a legkisebb részteste F-nek. F egy vektortér P felett. Legyen $|F : P| = n$, ami azt jelenti, hogy F dimenziója n a P felett. F elemei egyértelműen felírhatók a P feletti vektortér n dimenziójának megfelelően. Ez azt jelenti, hogy létezik egy bázis $\{b_1, b_2, \ldots, b_n\}$ F-ben P felett. Minden F-beli elem $\lambda_1 b_1 + \lambda_2 b_2 + \ldots + \lambda_n b_n$ alakban írható fel, ahol $\lambda_i \in P$. Az F test elemei az összes lehetséges lineáris kombinációi a bázis vektoroknak a prímtest P elemeivel, ami azt jelenti, hogy minden λ_i p-féle lehet. Ezért F elemeinek száma p^n, mivel minden koordináta p különböző értéket vehet fel, és n koordinátánk van.

Történelmi áttekintés

A történelemben szétnézve egészen a 17. század közepéig vezethetjük vissza a matematika véges testekkel foglalkozó ágát, ám önálló tudományágként csak a 19. század végén lett elismert. Egy korai tétel, amely értelmezhető a véges testek nyelvén a kis Fermat-tétel (Pierre de Fermat, 1636). Fermat nem adott rendes bizonyítást a tételre. 1736-ig kellett várni, amikor is Leonhard Euler (1707-1783) bizonyította be a tétel igazságát. A 18. században további tételeket fedeztek fel, melyeket prím modulo kongruenciákban fejeztek ki. Ezeket a tételeket az előbb említett Euler, illetve Joseph-Louis Lagrange (1736-1813) és Adrien-Marie Legendre (1752-1833) fedezték fel. Ennek ellenére az első publikációt, amely a prím rendű véges testekkel foglalkozik, Carl Friedrich Gauss (1777-1855) adta ki. Gauss bevezette az előbb említett

kongruenciát, melynek használata és jelölése(≡) gyorsan elterjedt. Bizonyította, hogy egy n fokú egész polinomnak nem lehet n-nél több inkongruens gyöke modulo egy prím. Euler kimutatta, hogy az $x^n - 1 \equiv 0$ kongruencia modulo egy prím legfeljebb n gyököt tartalmazhat. Gauss megjegyzi, hogy Euler módszere könnyen általánosítható.
A véges testek témában korszakalkotó munkát végzett még Évariste Galois (1811-1832) francia matematikus. Kutatásai alatt kifejtette algebrai nézeteit, mellyel megalapozta a kombinatorikus algebra módszereit és az egyenletek algebrai megoldhatóságának kritériumát. Leghíresebb ránk maradt eredménye a Galois-elmélet. Az elmélet kapcsolatot nyújt a testelmélet és a csoportelmélet között.

Kis Fermat-tétel

Legyen p prím és $a \in \mathbb{Z}$ egész, mely p-hez relatív prím. Ekkor

$$a^{p-1} \equiv 1 \pmod{p}$$

Kiegészítés: Ez a tétel valójában egy általánosítása az Euler-Fermat tételnek úgy, hogy a modulo egy prím és így $\phi(p) = p - 1$.

Alapműveletek - modulo(5)

Nézzük meg F_5-re a véges test alapműveleteit!
F_5 5 elemből áll, ezek az 5-tel osztás utáni maradékosztályok: 0, 1, 2, 3, 4

Példák az alapműveletekre:

Összeadás: $3 + 4 = 7 \to 7 \pmod 5 = 2$, tehát $3 + 4 \equiv 2 \pmod 5$

Kivonás: $4 - 3 = 1 \to 1 \pmod 5 = 1$, tehát $4 - 3 \equiv 1 \pmod 5$

Szorzás: $4 \cdot 3 = 12 \to 12 \pmod 5 = 2$, tehát $4 \cdot 3 \equiv 2 \pmod 5$

Osztás: Az osztás egy fokkal bonyolultabb, mert ott meg kell találni az adott elem inverzét. $4 \div 3 \pmod 5$-nél először kell 3 inverze $\pmod 5$. Az inverz egy olyan x szám, melyre teljesül, hogy $3x \equiv 1 \pmod 5$. Megnézve a lehetséges megoldásokat látjuk, hogy x = 2 az inverz.

$$3 \cdot 2 = 6 \equiv 1 \pmod{5}$$

Ebből adódik:

$$4 \div 3 \pmod 5 = 4 \cdot 2 \pmod 5 = 8 \pmod 5 = 3$$

Ha osztunk modulóban, akkor az osztandót megszorozzuk az osztó inverzével.

1.3. Polinom F test felett

A következő néhány pontban megnézünk néhány fontos tudnivalót a kommutatív test feletti polinomokkal kapcsolatban.

Polinom

Az F feletti P polinom egy olyan $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ kifejezés, ahol az α_i együtthatók az F kommutatív test elemei. Két polinomot akkor tekintünk azonosnak, ha a megfelelő együtthatóik megegyeznek. Ha az előző kifejezésben α_n nem nulla, akkor n számot a polinom fokszámának nevezzük és (deg P)-vel jelöljük.
A polinom így még csak formális kifejezés, de természetes módon hozzárendelhetünk egy úgynevezett polinomfüggvényt, amelyet $F \to F$ definiálhatunk. A $\gamma \in F$ elemet egy polinomfüggvény gyökének nevezzük, ha a függvény γ helyen vett helyettesítési értéke 0. Egy polinom gyökein a hozzá tartozó polinomfüggvény gyökeit értjük. A $\gamma \in F$ elemet a P polinom k-szoros gyökének nevezzük, ha P-ből az $x - \gamma$ gyöktényező pontosan k-szor emelhető ki. Formálisan $P = (x - \gamma)^k g$, ahol a g polinomhoz tartozó polinomfüggvénynek a γ már nem gyöke. A nem nulla polinomoknak legfeljebb annyi gyöke van ahány foka.

Polinomok összege és szorzata

Legyen két polinom $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ és $\beta_0 + \beta_1 x + \ldots + \beta_n x^n$.
Ekkor a két polinom összege:

$$(\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)x + \ldots + (\alpha_n + \beta_n)x^n + \beta_{n+1}x^{n+1} + \ldots + \beta_k x^k$$

A két polinom szorzata:

$$\alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)x + \ldots + \left(\sum_{i+j=m} \alpha_i\beta_j\right) x^m + \ldots + \alpha_n\beta_k x^{n+k}$$

Irreducibilis polinomok

Irreducibilisnek nevezünk egy polinomot, ha csak konstans kiemelésével alakítható szorzattá. $P(x)$ irreducibilis egy változóban és egy adott test felett, ha nincs olyan $A(x)$ és $B(x)$, melyekre

$$P(x) = A(x) \cdot B(x)$$

ahol $A(x)$ és $B(x)$ fokszáma is legalább 1.

Példa:
$P(x) = x^2 + 1$ irreducibilis a valós számok felett, mert nem lehet felbontani két nem triviális polinom szorzatára. Ezzel szemben $P(x) = x^2 - 1$ nem irreducibilis a valós számok felett, mert felbontható $(x - 1) \cdot (x + 1)$ szorzatra.

Testbővítés

Legyen L test és K az L részteste. Ekkor L a K bővítése, míg K alaptest. Jele: $L|K$
Ha $L|K$ és $M|L$ egyszerre teljesül, akkor L neve közbülső test ezzel a jelöléssel: $M|L|K$
K az L valódi részteste, ha $L \neq K$ és $K \leq L$, akkor L a K valódi bővítése.
Ha L bővítése K-nak, akkor az L-nek mint K feletti vektortérnek a dimenzióját a testbővítés fokának nevezzük és $\deg(L : K)$-val jelöljük.

Egyszerű bővítés

Legyen K részteste L-nek és $\Theta \in L$ tetszőleges elem. Ekkor ez K-nak Θ-val való egyszerű bővítése, melyet $K(\Theta)$-val jelölünk.

Tétel

$K(\Theta)$ az L testnek az a legszűkebb részteste, amely a Θ elemet és a K testet tartalmazza, azaz

(i) $K(\Theta)$ az L testnek részteste;

(ii) $\Theta \in K(\Theta)$, $K \subseteq K(\Theta)$;

(iii) ha T részteste L-nek és $\Theta \in T$, $K \subseteq T$, akkor szükségképpen $K(\Theta) \subseteq T$.

2. fejezet

Véges testek alkalmazása

Ebben a fejezetben megnézek néhány valódi területet, ahol alkalmazzák a véges testeket. A matematika nagyon sok részlegén nézelődhetnénk, de én most a kódoláselméleten belül a Reed-Solomon kódokat, a kriptográfián belül az elliptikus görbéken alapuló kriptográfiát, és a képfeldolgozáson belül a JPEG tömörítést fogom megnézni. [12] [13] [14] [15] [16] [17] [18] [19]

2.1. Reed-Solomon kódok

Irving S. Reed és Gustave Solomon 1960-ban publikálták "Polynomial Codes over Certain Finite Fields" című cikküket, mely a hibajavító kódokról szólt. Ezeket manapság Reed-Solomon kódoknak nevezzük és olyan területeken használatosak, mint az adattárolás vagy az adatátvitel. Ez egy olyan kódolási séma, ami egy változós polinomot használ az üzenet alapján, ahol csak egy rögzített értékkészlet ismert a kódoló és a dekódoló számára. Az eredeti dekóder n hosszú kódolt értékekből és k hosszú kódolatlan részhalmazok alapján polinomokat generál. A leggyakoribb polinomot választja helyesnek, de ez csak a legegyszerűbb esetekben alkalmazható.
Ezt kezdetben úgy oldották meg, hogy az eredeti sémát egy BCH-kódhoz hasonló sémává változtatták, amely egy fix polinomra alapult, amelyet mind a kódoló, mind a dekódoló ismert.

BCH kód

Bose–Chaudhuri–Hocquenghem kódok, továbbiakban BCH kódok a ciklus hibajavító kódok egy osztályát alkotják, amelyek polinomok segítségével kerülnek létrehozásra egy véges test felett. A BCH kódok egyik előnye, hogy könnyen dekódolhatók, egy algebrai módszerrel, amit szindróma dekódolásnak nevezünk.
A szindróma dekódolás egy olyan módszer, ahol az eredeti üzenetet egy hibajavító kóddal kódolják, ezzel redundanciát hozzáadva. Az adatok átvitele során keletkezhetnek hibák, így a kódolt üzenet különbözhet a vett üzenettől. A vett üzenet és a kódolt üzenet különbségét nevezzük szindrómának.
Röviden, a vett üzenetet (f) megszorozzuk egy paritásellenőrző mátrixszal(M), ebből megkapva a szindrómát(S).

$$S = M \cdot f$$

A BCH kódokat olyan területeken használják, mint például a műholdas kommunikáció, DVD-k, merevlemezek, USB flash meghajtók és vonalkódok.

Reed-Solomon kódok jellemzői

A Reed–Solomon kódok egy kódcsoportot alkotnak, ahol minden kódot három paraméter jellemez: egy ábécé mérete p, egy blokk hossza n, és egy üzenet hossza k, ahol $k < n \leq p$. Az ábécé szimbólumkészlete egy véges test F_p. A Reed–Solomon kód leggyakoribb paraméterezésében a blokkhossz általában az üzenet hosszának valamilyen konstans többszöröse, azaz a kódráta:

$$R = \frac{k}{n}$$

valamilyen konstans érték. Továbbá a blokkhossz egyenlő vagy eggyel kevesebb, mint az ábécé mérete, azaz

$$n = p \quad \text{vagy} \quad n = p - 1.$$

Üzenet Reed-Solomon alakja

Reed-Solomon (1960) eredeti konstrukciójában az üzenet $m = (m_0, \ldots, m_{k-1}) \in F^k$ leképeződik a q_m polinomra, ahol

$$q_m(a) = \sum_{i=0}^{k-1} m_i a^i.$$

Az m kódszó a q_m polinom n különböző pontján $a_0, \ldots, a_{n-1}$ F testen kerül kiértékelésre, és az értékek sorozata adja a megfelelő kódszót. Így a Reed–Solomon kód klasszikus kódoló függvénye $C : F^k \to F^n$ a következőképpen definiálható:

$$C(m) = \begin{bmatrix} q_m(a_0) \\ q_m(a_1) \\ \vdots \\ q_m(a_{n-1}) \end{bmatrix}.$$

Ez a C függvény lineáris leképezés, azaz teljesíti a $C(m) = Am$ feltételt, ahol az $n \times k$ mátrix A elemei F testből származnak:

$$C(m) = Am = \begin{bmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{k-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \cdots & a_{n-1}^{k-1} \end{bmatrix} \begin{bmatrix} m_0 \\ m_1 \\ \vdots \\ m_{k-1} \end{bmatrix}.$$

Ez a mátrix egy Vandermonde-mátrix(olyan mátrix, melynek minden sorában egy mértani sorozat elemei találhatók) F test felett. Más szóval, a Reed–Solomon kód lineáris kód, és a klasszikus kódolási eljárásban annak generátormátrixa az A.

Hibajavító képesség

Legyen a Reed-Solomon kód hossza p és dimenziója k. A kód képes akár t hibát is javítani, ahol t a következőképp néz ki:

$$t = \frac{p-k+1}{2}$$

Ez a lehető legjobb hibajavító képesség bármely ugyanolyan hosszúságú és dimenziójú kód esetében. Azokat a kódokat, amelyek elérik ezt az "optimális" hibajavító képességet, MDS kódoknak nevezik.

Generátor polinom megközelítés

A generátor polinom konstrukció egy a Reed-Solomon kódokhoz használt módszer. Ez a megközelítés a ciklikus kódok leírásának eszköze. Egy kódot ciklikusnak nevezünk, ha bármely kódszóra,

$$c = (c_0, c_1, c_2, \ldots, c_{n-2}, c_{n-1})$$

a ciklikusan eltolódott szó

$$c' = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$$

is kódszó.
Ha egy (n, k) kód ciklikus, akkor megmutatható, hogy a kód mindig definiálható egy generátor polinom

$$g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_{n-k} x^{n-k}$$

segítségével. Ebben a definícióban minden kódszót kódpolinomként értelmezünk.

$$(c_0, c_1, c_2, \ldots, c_{n-1}) \Rightarrow c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1}$$

c vektor egy kódszó a $g(x)$ által definiált kódban, akkor és csak akkor ha a megfelelő kódpolinom $c(x)$ osztható $g(x)$-el.
Legyen $m = (m_0, m_1, \ldots, m_{k-1})$ egy tömb k információs szimbólummal. Ezek a szimbólumok egy polinomhoz társíthatók $m(x) = m_0 + m_1 x + \ldots + m_{k-1} x^{k-1}$, amelyet $g(x)$-el való szorzás útján kódolunk:

$$c(x) = m(x)g(x)$$

A ciklikus Reed-Solomon kód konstrukciós folyamata a következő:
Tegyük fel, hogy szeretnénk egy t-hibajavító Reed-Solomon kódot építeni, amely $(p-1)$ hosszúságú és a GF(p)-ben lévő szimbólumokkal rendelkezik. A Galois test GF(p) nemnulla elemei megjeleníthetők egy a elem $(p-1)$ hatványaként.
A Reed-Solomon konstrukciós kritériuma a következő:
A t-hibajavító kód generátor polinomjának gyökei a egymást követő hatványainak kell lennie 2t.

$$g(x) = \prod_{j=1}^{2t} (x - a^j)$$

A kódpolinomok $2t$-től $(p-2)$ fokig terjedhetnek ($p-2$ fokú kódpolinom megfelel egy $p-1$ koordinátájú kódszónak). Következésképp a $2t$ fokú generátor polinommal rendelkező kód dimenziója $k = p - 2t - 1$.
Minden kódpolinomnak oszthatónak kell lennie a generátor polinommal. Ebből következik, hogy a kódpolinom gyökeinek ugyanazoknak a 2t hatványoknak kell lenniük, amelyek a $g(x)$ gyökeit alkotják.

2.2. Elliptikus görbéken alapuló kriptográfia

A kriptográfia a biztonságos kommunikáció egy eszköze. Algoritmussal titkosít adatokat, melyek egy titkos kulccsal visszafejthetők. Két féle titkosítás létezik. A titkos (szimmetrikus) és a nyilvánosn(publikus, asszimmetrikus) kulcsú titkosítás. A titkos kulcsú algoritmusok ugyanazokat a kulcsokat használják a nyílt szöveg titkosításához és a titkosított szöveg visszafejtéséhez. Ezzel szemben a publikus kulcsú algoritmusok egy kapcsolt kulcspárt használnak az üzenet titkosításához és visszafejtéséhez. Az elliptikus görbéken alapuló kriptográfia (ECC) egy publikus kulcsú kriptográfiai megközelítés, amely az elliptikus görbék algebrai struktúráján alapul, véges testek felett.

Ebben az esetben egy elliptikus görbe egy síkgörbe egy véges test felett, amely azokból a pontokból áll, amelyek kielégítik az alábbi egyenletet:

$$y^2 = x^3 + ax + b$$

Emellett tartalmaz egy végtelen pontot is, melyet ∞-nel jelölünk. Az itt szereplő koordinátákat egy adott véges testből kell választani. Ez a ponthalmaz, az elliptikus görbék csoportműveletével együtt, egy Abel-csoportot(kommutatív csoportot) alkot, ahol a végtelen pont az identitáselem.

Domain paraméterek

A domain paraméterek fontos szerepet játszanak az elliptikus görbéken alapuló kriptográfiai rendszerekben. Meghatározzák az elliptikus görbe jellemzőit, melyeken az adott kriptográfiai műveletek végrehajtódnak. Elemei:

- **Véges Test**: Ez általában egy prímrendű vagy kettőhatvány rendű test.
- **Az Elliptikus Görbe Egyenlete**: Fontosak a görbét meghatározó egyenlet együtthatói. Ha az egyenlet: $y^2 = x^3 + ax + b$, akkor az a és a b értékek. Az elliptikus görbe rendje k az a szám, amely tartalmazza az adott görbén lévő összes pontot, beleértve a végtelen pontot is.
- **Alappont (G)**: Egy specifikus pont a görbén, mely az összes kriptográfiai művelet kiindulópontja.
- **Rend (n)**: Az alappont rendje, ami azt jelöli, hogy mekkora az a legkisebb pozitív egész szám, amelyre igaz, hogy $n \cdot G = \infty$

- **A Cofaktor (h)**: Egy egész szám, amely a görbe rendjének és az alappont rendjének hányadosa ($h = k/n$).
- **Privát és Publikus Kulcsok**: A kriptográfiai műveletek végrehajtásához szükséges kulcsok.

Ezek biztosítják, hogy a kriptográfiai rendszer biztonságos és hatékony legyen, valamint hogy a különböző eszközök és szoftverek megfelelően tudjanak együttműködni.

ECC Algoritmusok

Elliptic Curve Digital Signature Algorithm (ECDSA): Az ECDSA hatékonyabb más aláírási algoritmusokhoz képest. Ennek oka, hogy kisebb kulcsokat használ, mégis ugyanolyan szintű biztonságot nyújt. A következőképp müködik:
Van egy matematikai egyenlet, amely rajzol egy görbét. Választunk egy véletlen pontot ezen a görbén, melyet kiindulási pontnak nevezünk. Ezután generálunk egy véletlen számot, ez lesz a privát kulcs. Összeszorozva a véletlen számot és a kiindulási pontot kapunk egy második pontot a görbén, ez lesz a publikus kulcs.

Elliptic-curve Diffie–Hellman (ECDH): Az ECDH egy "key agreement" protokoll, amely lehetővé teszi két fél számára, hogy egy megosztott titkot állapítsanak meg egy nem biztonságos csatornán keresztül. Mindkettő privát-publikus kulcspárral rendelkezik. Ez a megosztott titok közvetlenül használható kulcsként vagy más kulcs generálásához. Ezt követően a kulcs vagy a származtatott kulcs használható a későbbi kommunikációk titkosítására egy szimmetrikus-kulcsú rejtjelezővel.

Elliptic Curve Integrated Encryption Scheme (ECIES): Az ECIES egy publikus kulcsú hitelesített titkosítási rendszer. Használ egy úgynevezett "key-derivation function"-t (KDF), hogy az Elliptic-curve Diffie–Hellman (ECDH) protokollal megosztott titokból külön kulcsokat generáljon a szimmetrikus titkosításhoz és az üzenethitelesítési kódhoz (MAC). A titkosítás, általában egy AES (Advanced Encryption Standard) algoritmus segítségével történik.

ECC Előnyei

- **Gyors kulcsgenerálás:** Elég biztonságosan előállítani egy véletlen egész számot egy adott tartományban. Bármely egész szám a tartományban érvényes ECC titkos kulcsot képvisel.
- **Kisebb kulcsméret:** Az ECC lehetővé teszi kevesebb kulcs használatát a nem-EC titkosításokkal szemben.
- **Kisebb számítási teljesítmény:** Mivel az ECC kulcs rövidebb, a számítási teljesítmény is kisebb.
- **Magas biztonság:** Egy 256 bites ECC publikus kulcs hasonló biztonságot nyújt, mint egy 3072 bites RSA publikus kulcs. Az ECC segítségével kisebb kulcsokkal érhető el ugyanolyan szintű biztonság.

2.3. JPEG tömörítés

A JPEG veszteséges tömörítési formát használ, amely a diszkrét koszinusz transzformáción (DCT) alapul. Ez a matematikai művelet minden képkockát vagy testet átalakít a térbeli (2D) tartományból a frekvenciatartományba. Egy emberi pszichovizuális rendszerre alapozott észlelési modell, elveti a magas frekvenciájú információkat, azaz az éles átmeneteket és a színárnyalatokat. A transzformációs tartományban az információ csökkentésének folyamatát kvantálásnak nevezik. Egyszerűen fogalmazva, a kvantálás egy módszer arra, hogy egy nagy számértékű skálát optimálisan lecsökkentsünk kisebbre. A kvantált együtthatókat ezután sorrendbe rakják és becsomagolják az eredmény bitfolyamba. A tömörítési módszer általában veszteséges, ami azt jelenti, hogy az eredeti kép információinak egy része elveszik és nem állítható helyre, ez befolyásolhatja a képminőséget.

Diszkrét Koszinusz Transzformáció - DCT

A DCT alapelve, hogy a jelet szinusz és koszinusz hullámok kombinációjaként ábrázolja.

Lépései:

1. **Bemeneti Adatok Előkészítése:** A bemenet egy $N \times N$ méretű mátrix, amely a jelet reprezentálja.

2. **DCT Számítása:** A DCT egy $N \times N$ mátrixon az alábbi képlet segítségével számítható:

$$X_{k,l} = \frac{1}{4}\alpha(k)\alpha(l)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} x_{i,j}\cos\left[\frac{\pi}{N}\left(i+\frac{1}{2}\right)k\right]\cos\left[\frac{\pi}{N}\left(j+\frac{1}{2}\right)l\right]$$

   ahol:

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{N}} & \text{ha } u = 0 \\ \sqrt{\frac{2}{N}} & \text{különben} \end{cases}$$

   Az $x_{i,j}$ az eredeti mátrix elemeit jelenti, míg $X_{k,l}$ a DCT mátrix elemeit.

3. **Kvantálás:** A DCT mátrixot kvantálják, azaz a frekvenciakomponenseket egy előre meghatározott kvantálási mátrix segítségével redukálják.

4. **Tömörítés:** A kvantált DCT mátrixot tömörítik, például a JPEG esetében Huffman-kódolással.

Huffman-kódolás

A karaktereket gyakoriságuk szerint növekvő sorrendbe rendezzük. A gyakoriságokat többnyire százalékban adjuk meg. Ezután egy bináris fát építünk fel lépésről-lépésre a következő módon.

1. Kiválasztjuk a sorozat két legkisebb gyakoriságú elemét, amely egy háromcsúcsú bináris fa két levele lesz, majd ezekhez hozzárendelünk egy gyökeret, amelyet a két gyakoriság összegével címkézünk meg.

2. Ezután a két vizsgált elemet kitöröljük a sorozatból, és azok összegét beszúrjuk az érték szerinti megfelelő helyre.

3. Folytatjuk az előző műveletet mindaddig, amíg van elem a sorozatban. A folytatásnál felhasználjuk a már meglévő csúcsokat is, csak újabb elemeknél hozunk létre újabbakat.

Az így felépített fában a levelek az eredeti karaktereknek és azok gyakoriságának felelnek meg. Az eredményül kapott fában minden csúcs esetében címkézzük meg 0-val a belőle kiinduló bal oldali élt, 1-gyel pedig a jobb oldalit. A gyökértől egy adott levélig egyetlen út halad. Ezen út éleihez rendelt 0 és 1 címkéket sorrendben összeolvasva, megkapjuk a levélhez rendelt karakter kódját. Látható, hogy a gyakoribb karakterek kódja rövidebb, míg a kevésbé gyakoribbaké hosszabb lesz.

3. fejezet

Kombinatorikus feladat véges testben

Ha F egy véges test, akkor $F \times F$-re gondolhatunk a véges test felett definiált síkként, melyet tehát F-fel koordinátáztunk. Szokás ezt véges affin síknak hívni. Itt az egyenesek az $y = a \cdot x + b$ lineáris egyenletek (x, y) megoldáshalmazai, ill. az $x = c$ egyenletű "függőleges" egyenesek. Minden egyenesnek $|F|$ pontja van. Párhuzamossági egyenesosztályok: az azonos "a" együtthatójú (meredekségű) egyenesekből állnak. Ez tehát $|F|$ számú párhuzamossági egyenesosztály, és egy továbbit alkotnak még a "függőleges" egyenesek.

Ha F rendje egy p prím, akkor a fent definiált affin síkot AG(2,p)-nek hívjuk. Ha adott egy $f(x)$ polinom, akkor annak grafikonja az $\{(x, f(x)) : x \in F\}$ ponthalmaz.

A síkon definiálhatjuk a "grafikon alatti" pontokat, kihasználva, hogy nem csak modulo p, hanem a szokásos egész számok körében is gondolkozhatunk:

$$U_f = \{(x, y) : 0 \leq x \leq p - 1, 0 \leq y < f(x)\},$$

ahol a rendezést az egész számok körében értjük. Ez a definíció nagyon furcsának tűnik, hogy keverjük a véges testek és az egész számok világát, de az fog kiderülni, hogy bizonyos esetekben ez a ponthalmaz, a véges test felett értelmezve, érdekes szabályos tulajdonságokkal rendelkezik. Erről szól a dolgozat ezen fejezete, mely a [20] cikken alapszik.

3.1. Feladat

Legyen egy F_p véges test, ahol p prím. Legyenek $a \cdot x + b$ párhuzamossági osztályok az F_p véges testen belül. Nevezzük metszési számnak azon pontok számát, melyek a vizsgált függvény alatt és a párhuzamossági osztályok metszetében helyezkednek el.
Vizsgáljuk meg, milyen metszési számokat kapunk különböző függvényekre!

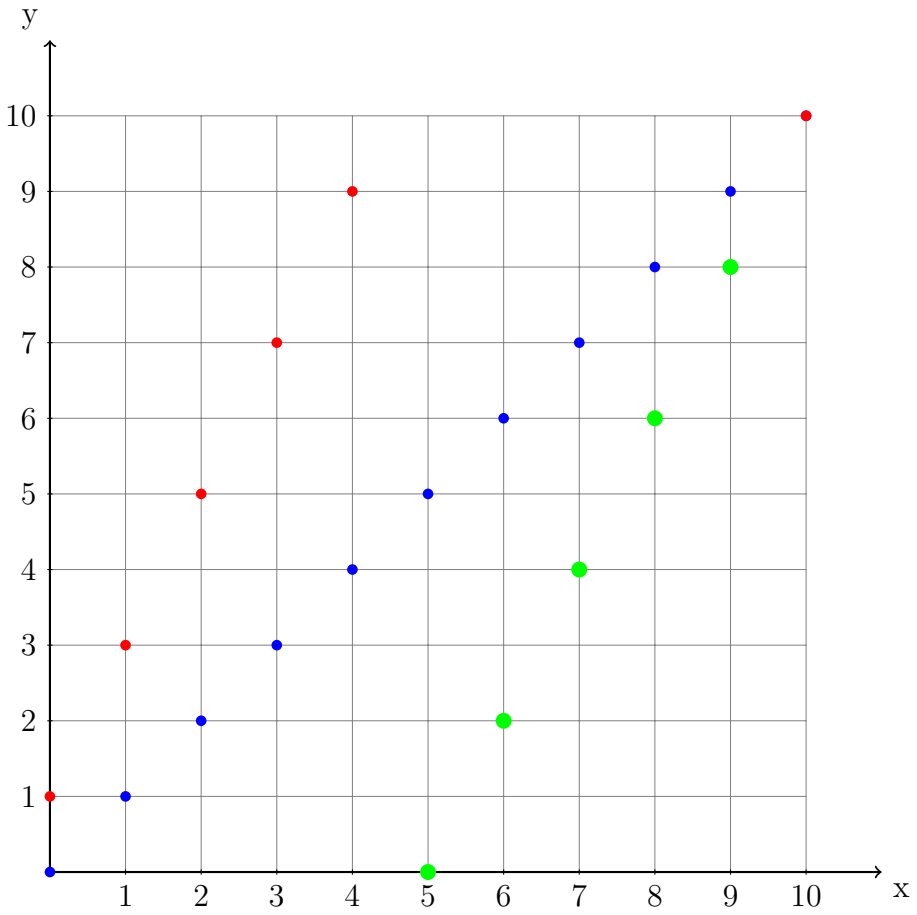
A feladat megoldásához Pythont használtam, a kódok egy részét megjelenítem. Az ábrákon és táblázatokban $p = 11$-gyel fogok dolgozni, mert úgy vélem, ennél nagyobb p-re az ábra mérete miatt nehezebben átlátható lenne a lényeg.

3.1.1. $y = x$

```
def metsz(p):
    mer = []
    for a in range(1, p):
        ind = []
        for b in range(0, p):
            x = 0
            for i in range(1, p):
                if ((b + (i * a)) % p) < i:
                    x = x + 1
            ind.append(x)
        mer.append(ind)
    return mer

metsz(p)
```

Nézzük meg F_{11} véges testet. Ábrázoljuk $y = x$ függvényt és $a \cdot x + b$ párhuzamossági osztályból $a = 2$ meredekségű és $b = 1$ tengelymetszetű egyenest.



Az ábrán a kék pontok jelölik a függvényt, esetünkben $y = x$-et. A piros pontok az $y = 2 \cdot x + 1$ egyenest jelölik. A zöld pontok pedig az $y = x$ alatt elhelyezkedő és $2 \cdot x + 1$ -et metsző pontok.
Leolvasható, hogy erre a konkrét egyenesre a metszési szám: 5
Végigfuttatva az a meredekségeket és a b tengelymetszeteket, az alábbi táblázatot

kapjuk.

$a\backslash b$	0	1	2	3	4	5	6	7	8	9	10
1	0	1	2	3	4	5	6	7	8	9	10
2	5	5	5	5	5	5	5	5	5	5	5
3	5	5	5	5	5	5	5	5	5	5	5
4	5	5	5	5	5	5	5	5	5	5	5
5	5	5	5	5	5	5	5	5	5	5	5
6	5	5	5	5	5	5	5	5	5	5	5
7	5	5	5	5	5	5	5	5	5	5	5
8	5	5	5	5	5	5	5	5	5	5	5
9	5	5	5	5	5	5	5	5	5	5	5
10	5	5	5	5	5	5	5	5	5	5	5

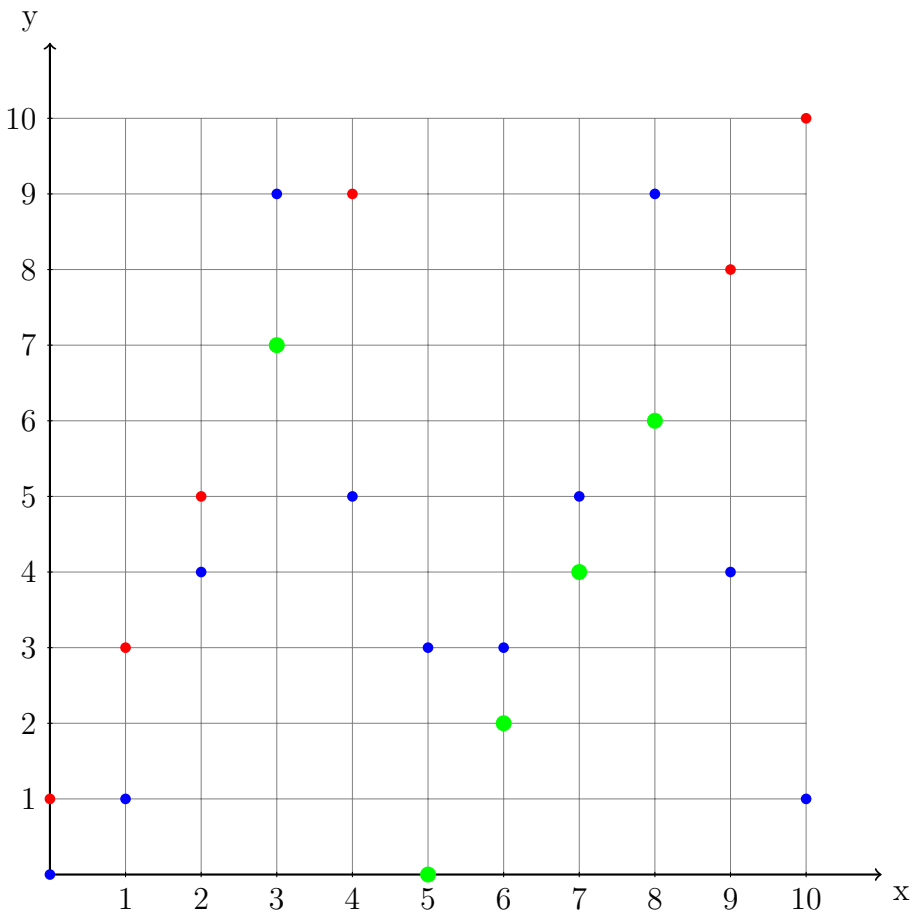
3.1. táblázat. Metszési számok $y = x \pmod{11}$

A táblázat első oszlopában a meredekségek, az első sorában pedig a tengelymetszetek találhatók. A későbbi táblázatokat is ilyen módon jelenítem meg.
Észrevehető, hogy $(a = 1)$-et leszámítva az összes metszési szám $((p-1) \div 2)$. Az 1 meredekségű osztályra kapott eredmény egyértelmű, hiszen ennél az esetnél csak az $y = x + b$ függvényt futtatjuk különböző tengelymetszetekből, így ezek párhuzamosak $(y = x)$-el. Az 1-nél nagyobb meredekségeknél az egyenesek többször "mennek végig" a testen. Az ismétlődés miatt ugyanaz a pontok eloszlása, csak nagyobb meredekségre az egyenes többször "megy végig".
Más p-t megvizsgálva is ezt a sémát lehet észrevenni. A metszési számok minden esetben $(a = 1)$-nél 0-tól $(p-1)$-ig növekvő sorrendben vannak. A többi metszési szám pedig minden esetben $((p-1) \div 2)$.

3.1.2. $y = x^2$

A kódon itt nem változtattam $y = x$ -hez képest, csak kicseréltem a legbelső ciklus elágazásában az i feltételt i^2-re.

Nézzük meg F_{11} véges testet. Ábrázoljuk $y = x^2$ függvényt és $a \cdot x + b$ párhuzamossági osztályból $a = 2$ meredekségű és $b = 1$ tengelymetszetű egyenest.



Az ábrán a kék pontok jelölik a függvényt, esetünkben $y = x^2$-et. A piros pontok $2 \cdot x + 1$ egyenest jelölik. A zöld pontok pedig az $y = x^2$ alatt elhelyezkedő és $2 \cdot x + 1$ -et metsző pontok. Ebben az esetben a metszési szám: 5

Vizsgáljuk meg, észrevehető-e valamilyen érdekes minta a metszési számoknál!

$a \backslash b$	0	1	2	3	4	5	6	7	8	9	10
1	4	3	2	3	4	5	4	5	5	4	5
2	4	5	4	3	2	3	4	5	4	5	5
3	2	3	4	5	4	5	5	4	5	4	3
4	3	2	3	4	5	4	5	5	4	5	4
5	4	5	5	4	5	4	3	2	3	4	5
6	4	5	5	4	5	4	3	2	3	4	5
7	3	2	3	4	5	4	5	5	4	5	4
8	2	3	4	5	4	5	5	4	5	4	3
9	4	5	4	3	2	3	4	5	4	5	5
10	4	3	2	3	4	5	4	5	5	4	5

3.2. táblázat. Metszési számok $y = x^2 \pmod{11}$

Soronként észrevehető egy ismétlődés. **Minden sorban ugyanazok a metszési számok vannak, ugyanabban a sorrendben, csak máshonnan indítva.** Tehát ez a ponthalmaz a 0 ill. 1 meredekségek kivételével minden párhuzamossági osztályt ugyanabban a mintázatban metsz! A jobb átláthatóság érdekében sárgára színeztem a "kezdőpontokat".
A $((p-1) \div 2)$ meredekségig megfigyelhető kezdőpontok fordított sorrendben megismétlődnek $((p-1) \div 2)$ után. Ez minden p-re igaz. A metszési számok mintájáról eszünkbe juthat x^2 függvény szimmetriája.

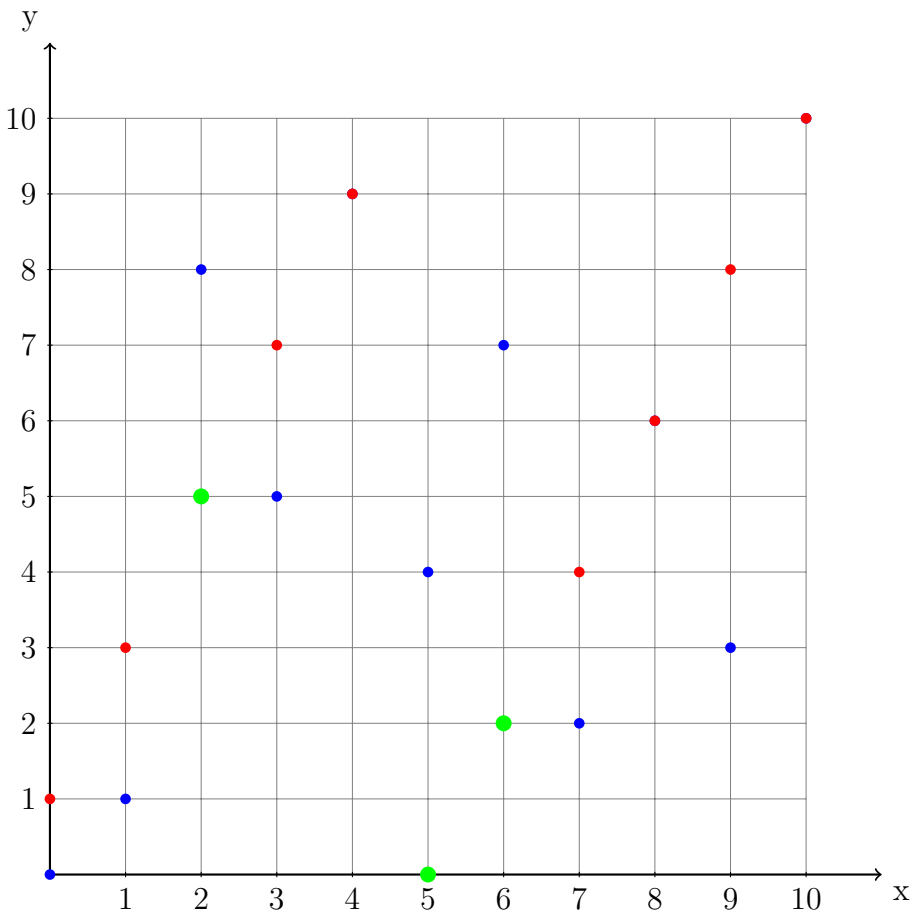
3.1.3. $y = x^3$

```
def phalmaz(p):
    ph = []
    for i in range(1, p):
        j = 0
        while j < i**3 % p:
            ph.append([i, j])
            j = j + 1
    return ph

def algo(p, h):
    m1 = []
    for a in range(1, p):
        m2 = []
        for b in range(0, p):
            x = 0
            for i in range(1, p):
                szp = [i, ((b + (i * a)) % p)]
                if szp in h:
                    x = x + 1
            m2.append(x)
        m1.append(m2)
    return m1

h = phalmaz(p)
algo(p, h)
```

Nézzük meg F_{11} véges testet. Ábrázoljuk $y = x^3$ függvényt és $a \cdot x + b$ párhuzamossági osztályból $a = 2$ meredekségű és $b = 1$ tengelymetszetű egyenest.



Az ábrán a kék pontok jelölik a függvényt, esetünkben $y = x^3$-öt. A piros pontok $2 \cdot x + 1$ egyenest jelölik. A zöld pontok pedig az $y = x^3$ alatt elhelyezkedő és $2 \cdot x + 1$ -et metsző pontok. Ebben az esetben a metszési szám: 3

Tekintsük meg, milyen metszési mintázatot találunk!

$a \backslash b$	0	1	2	3	4	5	6	7	8	9	10
1	4	4	4	5	6	5	4	5	6	6	6
2	5	3	4	5	5	5	5	5	6	7	5
3	4	5	4	4	4	5	6	6	6	5	6
4	4	5	6	6	5	5	5	4	4	5	6
5	4	3	3	4	4	5	6	6	7	7	6
6	5	6	6	7	5	5	5	3	4	4	5
7	5	6	6	6	7	5	3	4	4	4	5
8	5	5	6	4	4	5	6	6	4	5	5
9	4	4	5	4	5	5	5	6	5	6	6
10	5	5	3	3	4	5	6	7	7	5	5

3.3. táblázat. Metszési számok $y = x^3 \pmod{11}$

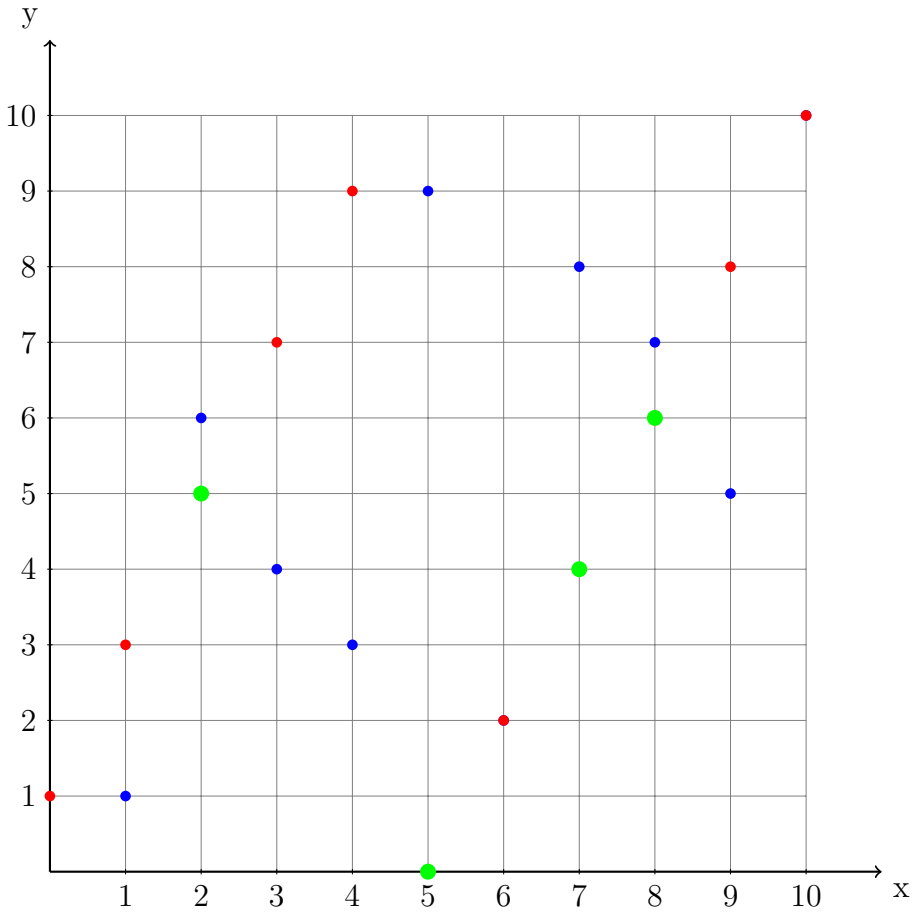
Az előző két függvénytől nem eltérve, itt is észrevehető egy minta.
$((p-1) \div 2)$-t a továbbiakban s-sel jelölöm. $b = s$ esetén minden a-ra és p-re a metszési szám s. Ettől a ponttól távolodva pedig ellentétes a differencia. A megfelelő indexszekkel felírva a következőképp néz ki.
Legyen a meredekség fix. Amennyiben $b[i]$ értéke x, úgy $b[p-1-i]$ értéke $(s-x+s)$, ahol $s-x$ a differencia. A metszési számok mintája hasonlít az x^3 függvény alakjához és tulajdonságaihoz.

3.1.4. $y = \frac{1}{x}$

Az $\frac{1}{x} \mod p$ azt az egész számot jelenti, amelyet x-szel szorozva 1-et kapunk modulo p. Ezért az x^3-nél használt kódomat kiegészítettem úgy, hogy kiszámolja $n \cdot x \equiv 1 \pmod{p}$ esetén mennyi n.

```
1 n = 0
2     while ((n * i) % p) != 1:
3       n = n + 1
```

Nézzük meg F_{11} véges testet. Ábrázoljuk $y = \frac{1}{x}$ függvényt és $a \cdot x + b$ párhuzamossági osztályból $a = 2$ meredekségű és $b = 1$ tengelymetszetű egyenest.



Az ábrán a kék pontok jelölik a függvényt, esetünkben $y = \frac{1}{x}$-et. A piros pontok $2 \cdot x + 1$ egyenest jelölik. A zöld pontok pedig az $y = \frac{1}{x}$ alatt elhelyezkedő és $2 \cdot x + 1$

-et metsző pontok. Ebben az esetben a metszési szám: 4

Nézzük meg a metszési számokat!

$a\backslash b$	0	1	2	3	4	5	6	7	8	9	10
1	4	3	4	5	4	5	6	5	6	7	6
2	5	4	3	4	5	5	5	6	7	6	5
3	4	5	4	5	6	5	4	5	6	5	6
4	4	5	4	3	4	5	6	7	6	5	6
5	4	5	6	7	6	5	4	3	4	5	6
6	5	4	5	5	6	5	4	5	5	6	5
7	5	6	7	6	6	5	4	4	3	4	5
8	5	5	4	5	4	5	6	5	6	5	5
9	4	3	4	3	4	5	6	7	6	7	6
10	5	6	6	5	4	5	6	5	4	4	5

3.4. táblázat. Metszési számok $y = \frac{1}{x} \pmod{11}$

Megvizsgálva a táblázatot látható, hogy itt is hasonló a szabály, mint x^3-nél, csak a metszési számok nem ugyanazok.

3.2. Négyzetek eloszlása prímmodulóval

Legyen q egy prímszám hatványa, F_q a q rendű véges test, és jelölje $AG(2,q)$ a q rendű Desargues-i affin síkot. (A Desargues-i affin sík egy olyan affin sík, amely megfelel a Desargues-tételnek. A Desargues-tétel kimondja, hogy ha két háromszög egy pontra nézve perspektív, akkor egy egyenesre nézve is perspektív.) Jelölje ℓ_∞ azt az egyenest, amely kiegészíti az $AG(2,q)$-t egy projektív síkká. (A projektív sík egy geometriai struktúra, amely kiterjeszti az affin síkot azzal, hogy hozzáad egy "végtelen távoli" ℓ_∞ egyenest és annak pontjait.) Az ℓ_∞ pontjait gyakran irányoknak nevezik, mivel ezek megfelelnek az $AG(2,q)$ egyenesei meredekségeinek. Ezeket az irányokat (d)-vel jelöljük, ahol $d \in F_q \cup \{\infty\}$. A d meredekségű affin egyenesek pontosan azok az egyenesek, amelyek egyenlete

$$Y = dX + b, \text{ illetve } X = c \text{ egyenes egyenlet esetén } d = \infty.$$

Legyen $p > 2$ egy prímszám. Ebben a szakaszban Q és N rendre az F_p nem nulla négyzeteinek és nem-négyzeteinek halmazait jelölik. Az F_p kvadratikus karaktere a következő függvényként van definiálva:

$$\chi : F_p \to \mathbb{R} : x \mapsto \begin{cases} 1 & \text{ha } x \in Q, \\ 0 & \text{ha } x = 0, \\ -1 & \text{ha } x \in N. \end{cases}$$

Természetesen értelmezhetjük χ-t mint $\mathbb{Z} \to \mathbb{R}$ függvényt. A kvadratikus karakter összege egy intervallum felett korlátozott.

Pólya-Vinogradov egyenlőtlenség:

Bármely két egész szám a és b esetén

$$\left|\sum_{x=a}^{b}\chi(x)\right| \leq \sqrt{p}\ln(p).$$

Ennek egyfajta ellenpárja a következő: Létezik egy $b \in F_p$ elem, hogy

$$\left|\sum_{x=1}^{b}\chi(x)\right| \geq \frac{1}{2\pi}\sqrt{p}.$$

Legyen $\nu : F_p \to \mathbb{N}$ az a függvény, amely F_p egy elemét hozzárendeli a hozzá tartozó egész számhoz $\{0,\ldots,p-1\}$-ből. Legyen p egy páratlan prím, és legyen $n = |N \cap \left\{1,\ldots,\frac{p-1}{2}\right\}|$. Ekkor

$$\sum_{x\in Q}\nu(x) = \begin{cases} p\frac{(p-1)}{4} & \text{ha } p \equiv 1 \pmod 4, \\ pn & \text{ha } p \equiv -1 \pmod 8, \\ p(\frac{n}{3}+\frac{p-1}{6}) & \text{ha } p \equiv 3 \pmod 8. \end{cases}$$

A Pólya-Vinogradov egyenlőtlenség alkalmazásával az $\left\{1,\ldots,\frac{p-1}{2}\right\}$ intervallumra a következő korlátot kapjuk n-re.

Legyen $n = |N \cap \left\{1,\ldots,\frac{p-1}{2}\right\}|$. Ekkor

$$\left|n - \frac{p-1}{4}\right| \leq \frac{1}{2}\sqrt{p}\ln(p),$$

és így

$$\left|\sum_{x\in Q}\nu(x) - p\frac{(p-1)}{4}\right| \leq \begin{cases} 0 & \text{ha } p \equiv 1 \pmod 4, \\ \frac{1}{2}\sqrt{p}\ln(p) & \text{ha } p \equiv -1 \pmod 8, \\ \frac{1}{6}\sqrt{p}\ln(p) & \text{ha } p \equiv 3 \pmod 8. \end{cases}$$

3.3. Parabola alatti pontok

Legyen

$$S = (x,y) \in F_p^2 \mid y < \alpha x^2 + \beta x + \gamma,$$

ahol $\alpha \in F_p^*, \beta, \gamma \in F_p$

Definiáljuk a vetítő függvényt: legyen $pr_{S,d} : F_p \to \mathbb{N}$, amely b-hez hozzárendeli az S pontjainak számát az $Y = dX + b$ egyenesen, ha $(d) \neq (\infty)$, vagy az $X + b = 0$ egyenesen, ha $(d) = (\infty)$.

Tétel. Legyen $f(X) = X^2$, ami egy másodfokú polinom $\mathbb{F}_p$ felett, ahol $p > 2$ prímszám. Tekintsük az alábbi halmazt:

$$S = \{(x, y) \in \mathbb{F}_p^2 \mid 0 \leq y < f(x)\},$$

azaz az $Y = f(X)$ parabola alatti pontokat. Tetszőleges $d \in \mathbb{F}_p^*$ és $b \in \mathbb{F}_p$ esetén:

$$\mathrm{pr}_{S,d}(b) = \mathrm{pr}_{S,1}\left(b + \frac{(d-1)(d+1)}{4}\right).$$

Továbbá, $\mathrm{pr}_{S,d}$ képe egy olyan intervallum, amelynek hossza $\frac{\sqrt{p}}{2\pi}$ és $\sqrt{p}\ln(p)$ között helyezkedik el.

Bizonyítás. Bizonyítanunk kell, hogy bármely b értékre

$$\mathrm{pr}_{S,d}\left(b + \frac{(d-1)(d+1)}{4}\right)$$

független $d \in \mathbb{F}_p^*$ választásától. Ez az érték megegyezik az alábbi egyenlőtlenség megoldásainak számával:

$$dX + b + \frac{(d-1)(d+1)}{4} < X^2.$$

Alkalmazzuk a lineáris transzformációt $X' = X - \frac{d-1}{2}$, hogy az egyenlőtlenséget ekvivalensen átfogalmazzuk:

$$X' + b + \delta_d(X') < X'^2 + \delta_d(X'),$$

ahol

$$\delta_d(X') = (d-1)X' + \frac{(d-1)^2}{4}. \qquad (*)$$

Jelölje $N_{d,b}$ a (*) egyenlőtlenség megoldásainak halmazát. Be kell bizonyítanunk, hogy $|N_{d,b}|$ független $d \in \mathbb{F}_p^*$ választásától. Mivel tudjuk, hogy $\sum_{b\in\mathbb{F}_p} |N_{d,b}| = |S|$ minden d-re, elegendő igazolni, hogy bármely b-re:

$$|N_{d,b+1} \setminus N_{d,b}| = |N_{d,b+1} \cap N_{d,b}| - |N_{d,b} \setminus N_{d,b+1}|$$

független $d \in \mathbb{F}_p^*$-tól. Vegyük észre, hogy

$$x \in N_{d,b+1} \setminus N_{d,b} \iff x + b + \delta_d(x) = -1 \quad \text{és} \quad f(x) + \delta_d(x) \neq 0,$$

$$x \in N_{d,b} \setminus N_{d,b+1} \iff x + b + 1 = f(x) \quad \text{és} \quad f(x) + \delta_d(x) \neq 0.$$

Jelölje k azon megoldások számát, amelyekre $x + b + 1 = f(x)$. Mivel $d \neq 0$, létezik egyértelmű megoldás x_0-ra, amelyre $x + b + \delta_d(x) = -1$.

Először tegyük fel, hogy x_0 megoldása az $f(x) + \delta_d(x) = 0$ egyenletnek. Ekkor ez megoldása az $x + b + 1 = f(x)$-nek is, tehát

$$|N_{d,b+1} \setminus N_{d,b}| = 0, \quad |N_{d,b} \cap N_{d,b+1}| = k - 1.$$

Ha x_0 nem megoldása az $f(x) + \delta_d(x) = 0$-nak, akkor

$$|N_{d,b+1} \setminus N_{d,b}| = 1, \quad |N_{d,b} \cap N_{d,b+1}| = k.$$

Ahhoz, hogy a fentebbi egyenlőség teljesülését igazoljuk, meg kell mutatnunk, hogy az $X + b + 1 = f(X)$ egyenletnek nincs olyan megoldása, amelyre $f(X) + \delta_d(X) = 0$. Ha lenne ilyen, akkor $x + b + \delta_d(x) = -1$, ami azt jelenti, hogy $x = x_0$, és ez ellentmond annak, hogy $f(x_0) + \delta_d(x_0) \neq 0$.

Ebből arra következtetünk, hogy mindkét esetben:

$$|N_{d,b+1} \setminus N_{d,b}| - |N_{d,b} \setminus N_{d,b+1}| = 1 - k,$$

ami valóban független a $d \in \mathbb{F}_p^*$ választásától.

Vegyük észre, hogy k az $f(X) - X - b - 1 = 0$ másodfokú egyenlet gyökeinek számát jelöli. Ezért k az $4b + 5$ diszkrimináns kvadratikus karakterétől függ. Konkrétan:

$$1 - k = -\chi(4b + 5).$$

Ez azt jelenti, hogy $N_{d,b}$ és $N_{d,b+1}$ különbsége $1-k$, és $|1-k| \leq 1$, tehát a $\mathrm{pr}_{S,d}$ képe egy intervallumban szereplő összes egész számot tartalmazza. Továbbá, bármely $a, b \in \mathbb{F}_p$ esetén:

$$\Big||N_{d,b}| - |N_{d,a}|\Big| = \left|\sum_{x=a+1}^{b} \chi(4x+1)\right| =$$

$$= \left|\sum_{x=a+\frac{5}{4}}^{b+\frac{1}{4}} \chi(x)\right|.$$

Ezért a $\mathrm{pr}_{S,d}$ képe által alkotott intervallum hossza egyenlő a fenti összeg maximális értékével. A 3.2-ben leírt eredmények alapján tudjuk, hogy ennek maximális értéke $\frac{\sqrt{p}}{2\pi}$ és $\sqrt{p}\ln(p)$ között van.

Tétel: Legyen S a parabola alatti ponthalmaz $AG(2,p)$-ben, ahol $p > 2$ prím. Ekkor

$$|S| - \left\lfloor \frac{p^2}{2} \right\rfloor \leq c_p \sqrt{p} \ln(p),$$

ahol

$$c_p = \begin{cases} 1 & \text{ha } p \equiv 1 \pmod 4, \\ 2 & \text{ha } p \equiv -1 \pmod 8, \\ \frac{4}{3} & \text{ha } p \equiv 3 \pmod 8. \end{cases}$$

Továbbá, $|S|$ p-vel osztható.

A tétel szerint egy adott ponthalmaz mérete osztható p-vel, ahol p egy prím. A pontok számát $|S|$ úgy számíthatjuk ki, hogy figyelembe vesszük a parabola alatti összes pontot az affin síkban. A $\left\lfloor \frac{p^2}{2} \right\rfloor$ kifejezés a parabola alatti pontok közelítő száma, amikor p nagy. A tétel egy korrekciós tényezőt ad meg, amely figyelembe veszi a pontok tényleges számát, és azt mondja ki, hogy a különbség a közelítő szám és a valós szám között legfeljebb $c_p\sqrt{p}\ln(p)$ lehet. A c_p konstans értéke attól függ, hogy p milyen maradékot ad, amikor 4 vagy 8 maradékosztályára osztjuk. Összességében a parabola alatti pontok számára ad becslést.

Összegzés

A szakdolgozat során megvizsgáltam a véges testek elméletét és néhány alkalmazását, különös figyelmet fordítva a függvénygrafikonok alatti területek vizsgálatára véges testek feletti síkokon. A véges testek fontos szerepet játszanak a modern algebra és a számítástudomány területén, különösen a kriptográfia, a kódoláselmélet és a számelmélet alkalmazásaiban.
Az első fejezetben bemutattam a véges testek alapvető tulajdonságait és megnéztem néhány definíciót, tételt.
Ezt követően megvizsgáltam a véges testek különböző alkalmazásait. A kódoláselméletben és kriptográfiában betöltött szerepük kiemelkedő, hiszen lehetővé teszik a hatékony és biztonságos adatátvitelt és adatvédelmet.
Végül pedig a függvénygrafikonok alatti ponthalmazok vizsgálatával foglalkoztam véges testek felett definiált síkokon. Elemeztem egy adott feladatot, melyre eredményként érdekes mintákat kaptam.
Összességében megállapíthatjuk, hogy a véges testek és azok alkalmazásai nagyon fontosak a modern matematika és informatika több területén.

Irodalomjegyzék

[1] Weisstein, Eric W., *Finite Field*, https://mathworld.wolfram.com/FiniteField.html.

[2] Gonda János, *Véges testek*, 2011, https://www.inf.elte.hu/dstore/document/296/GondaJanos-VegesTestek15.pdf.

[3] *Kis Fermat-tétel*, https://hu.wikipedia.org/wiki/Kis_Fermat-ttel.

[4] *Finite Fields*, https://en.wikipedia.org/wiki/Finite_field.

[5] *Véges test elemszáma*, https://ewkiss.web.elte.hu/wp/wordpress/wp-content/uploads/2018/10/Alg3a_print_9.pdf.

[6] Gary L. Mullen and Daniel Panario, *Handbook of Finite Fields*, Page 40-45, 2013, Chapman & Hall.

[7] *Évariste Galois*, https://hu.wikipedia.org/wiki/variste_Galois.

[8] Freud Róbert, *Lineáris Algebra(Javított és bővített kilencedik kiadás)*, Page 344-384, 2024.

[9] *Irreducibilis polinomok*, https://eta.bibl.u-szeged.hu/1538/3/irreducibilitas.pdf.

[10] *Kongruencia*, https://hu.wikipedia.org/wiki/Kongruencia.

[11] *Euklideszi algoritmus*, https://hu.wikipedia.org/wiki/Euklideszi_algoritmus.

[12] *Reed-Solomon error correction*, https://en.wikipedia.org/wiki/ReedSolomon_error_correction.

[13] *BCH code*, https://en.wikipedia.org/wiki/BCH_code.

[14] Stephen B. Wicker and Vijay K. Bhargava cikke, *An Introduction to Reed-Solomon codes*, Stephen B. Wicker, School of Electrical and Vijay K. Bhargava, Computer Engineering Georgia Institute of Technology, Atlanta, Georgia 30332. and Department of Electrical and Computer EngineeringUniversity of Victoria Victoria, British Columbia, Canada V8W 2Y2

[15] *Elliptic curve cryptography*, https://en.wikipedia.org/wiki/Elliptic-curve_cryptography.

[16] *ECC algoritmusok*, https://www.geeksforgeeks.org/blockchain-elliptic-curve-cryptography/.

[17] *JPEG*, https://en.wikipedia.org/wiki/JPEG.

[18] *Diszkrét koszinusz transzformáció*, https://hu.wikipedia.org/wiki/Diszkrt_koszinusz-transzformci.

[19] *Huffman-kódolás*, https://hu.wikipedia.org/wiki/Huffman-kdols.

[20] Sam Adriaensen and Zsuzsa Weiner, *Points below a parabola in affine planes of prime order*, 2024.