Véges testek (p végig ugyanaz a prímszám):

(i) *Elemszám*: $|T| = p^k$, ahol p prím és minden p^k-hoz pontosan egy p^k elemű T létezik (izomorfizmustól eltekintve).

(ii) *Additív szerkezet*: Bármely elemet önmagával p-szer összeadva 0-t kapunk (azaz a karakterisztika p).

(iii) *Multiplikatív szerkezet*: Van olyan $\alpha \in T$, amelynek hatványaiként T összes nem nulla eleme előáll (azaz a nem nulla elemek multiplikatív csoportja ciklikus): $T = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^k-2}\}$ és $\alpha^{p^k-1} = 1$.

(iv) *Testbővítés*: T-nek van egy $\mathbf{Z}_p$-vel izomorf részteste (a prímtest) és T ennek (pl.) α-val történő bővítése. A bővítés foka, azaz T-nek mint $\mathbf{Z}_p$ feletti vektortérnek a dimenziója k, ami egyúttal az α foka $\mathbf{Z}_p$ felett.

(v) *Faktorgyűrű*: $T \cong \mathbf{Z}_p[x]/(f)$, ahol f egy k-adfokú irreducibilis polinom $\mathbf{Z}_p$ felett (pl. α minimálpolinomja). T elemei tehát az f-fel való osztási maradékoknak (azaz legfeljebb $k-1$-edfokú polinomoknak) tekinthetők és a műveleteket is ennek megfelelően végezzük.

70. (a) Egy n elemű testben mi lesz egy elem n-edik hatványa?
(b) És a $2n-1$-edik hatványa?
(c) Melyik nevezetes tétel adódik (a)-ból az $n = p$(=prím) esetben?

71. Mennyi egy véges testben az összes elem összege, illetve a nem nulla elemek szorzata?

72. Hány részteste van egy 3^{101} elemű testnek?

73. Konstruáljunk (a) 25; (b) 27 elemű testet.

74. Határozzuk meg az összes véges testet, amelyben tagonként lehet négyzetre emelni: $(a+b)^2 = a^2 + b^2$ teljesül minden a, b elemre. Oldjuk meg az analóg problémát négyzetek helyett köbökre is. (*) Mi a helyzet p-edik hatványokra, ahol p prím? (Nézzük meg először egy konkrét p-re, pl. 7-re.)

75. Mely véges testekben van olyan $c \neq d$ elem, amelyre $c+c+c+c = d$ és $d+d+d+d = c$?

76. Mely véges testekben lehet minden elemből négyzetgyököt vonni, azaz mikor lesz minden $a \in T$-re az $x^2 = a$ egyenlet megoldható?

77. Hány olyan elempár van T-ben, amelyek egymás köbgyökei, ha T elemszáma
(a) 17^{1111}; (b) 7^{1111}?

78. Megoldható-e az $x^2 + x + 1 = 0$ egyenlet, ha T elemszáma (a) 27; (b) 125; (c) 343?

79. Adjuk meg az összes negyedfokú irreducibilis polinomot $\mathbf{Z}_2$ felett.

80. Igazoljuk, hogy ha p prím és $0 < j < p^k$, akkor $\binom{p^k}{j}$ osztható p-vel.