Euklideszi gyűrű: Olyan kommutatív, egységelemes, nullosztómentes R gyűrű, amelyben megadható egy $f : R \to \mathbf{N}$ függvény, amelyre $f(u) = 0 \iff u = 0$, és minden $b \neq 0, a \in R$-hez létezik olyan $c, d \in R$, hogy $a = bc + d$, ahol $f(d) < f(b)$. Ilyen gyűrűk pl. $\mathbf{Z}$, itt $f(u) = |u|$; $T[x]$, itt $f(0) = 0$ és $f(u) = \deg u + 1$, ha $u \neq 0$; a Gauss-egészek gyűrűje, itt $f(u) = N(u)$. Euklideszi gyűrűben mindig igaz a számelmélet alaptétele (általános bizonyítás hamarosan).

Ideál: Egy (tetszőleges) R gyűrűben egy olyan $I \neq \emptyset$ részhalmaz, amely zárt az R-beli összeadásra, ellentettképzésre és tetszőleges R-beli elemmel bármelyik ldalról történő szorzásra, azaz $a, b \in I$ és $r \in R$ esetén $a+b, -a, ra, ar \in I$. Az összeadásra és ellentettképzésre vonatkozó zártság helyettesíthető azzal, hogy I zárt a kivonásra.

Generált ideál: Ha $H \subseteq R$, akkor a H által generált ideál az a legszűkebb olyan ideál, ami H-t tartalmazza, jele (H). Ez tehát ideál, tartalmazza H-t, és ha egy J ideál tartalmazza H-t, akkor $(H) \subseteq J$. (H) nem más, mint az összes, a H-t tartalmazó ideál metszete. Az egy elem által generált ideálok a főideálok. Kommutatív, egységelemes gyűrűben a (c) főideál a c összes többszöröseiből áll, azaz $(c) = \{rc \mid r \in R\}$. Hasonlóan, $(c_1, \ldots, c_k) = \{r_1c_1 + \ldots + r_kc_k \mid r_j \in R\}$.

40. (a) Mutassuk meg, hogy az $\alpha = a + bi\sqrt{2}$ komplex számok, ahol a, b egészek, egy R kommutatív, egységelemes, nullosztómentes gyűrűt alkotnak (a $\mathbf{C}$-beli összeadásra és szorzásra).
(b) Definiáljuk R-ben a normát: $N(a + bi\sqrt{2}) = a^2 + 2b^2 = |\alpha|^2 = \alpha \cdot \overline{\alpha}$. Lássuk be, hogy $N(\alpha\beta) = N(\alpha)N(\beta)$.
(c) Határozzuk meg R egységeit.
(d) Igazoljuk, hogy R euklideszi gyűrű.
(e) Az (e1) $1 + i\sqrt{2}$; (e2) $1 + 2i\sqrt{2}$; (e3) $1 + 3i\sqrt{2}$ közül melyek felbonthatatlanok R-ben?

41. (a) Lássuk be, hogy a páratlan nevezőjű törtek egy kommutatív, egységelemes, nullosztómentes R gyűrűt alkotnak.
(b) Mik az egységek és mik a felbonthatatlanok?
(c) R-ben (egységszeresektől eltekintve) csak véges sok felbonthatatlan van. Hol bukik meg itt az euklideszi bizonyítás arról, hogy végtelen soknak kellene lennie?
(d) Bizonyítsuk be, hogy R-ben érvényes a számelmélet alaptétele, sőt euklideszi gyűrű.

42. Oldjuk meg az alábbi diofantikus egyenleteket:
(a) $(x^2 - 2)(x^2 + 7) = y^3$; (b) $x^2 + 1 = y^3$; (c) $x^2 + 2 = y^3$.

43. Hány ideál van az alábbi gyűrűkben: (a) $\mathbf{C}$; (b) $\mathbf{C}[x]$; (c) $\mathbf{Z}_{20}$?

44. Mely m-ekre alkotnak a 0 és a nullosztók ideált $\mathbf{Z}_m$-ben?

45. Igaz vagy hamis? (I, J ideálok R-ben.)
(a) $I \cap J = 0 \Rightarrow I = 0$ vagy $J = 0$.
(b) R nullosztómentes, $I \cap J = 0 \Rightarrow I = 0$ vagy $J = 0$.

46. Lássuk be:
(a) Testnek csak a két triviális ideálja van.
(b) Ha R egységelemes, kommutatív és csak a két triviális ideálja van, akkor R test.

47. (a) Mutassuk meg, hogy $\mathbf{Z}[x]$-ben a 2 és x polinomok lnko-ja nem áll elő $2f+xg$ alakban semmilyen f, g egész együtthatós polinomokkal.
(b) Igazoljuk, hogy $\mathbf{Z}[x]$ nem euklideszi gyűrű (azaz nemcsak arról van szó, hogy a fokszám szerint nincs maradékos osztás, hanem egyáltalán nincs olyan függvény, amely szerint megvalósítható lenne).

48. Legyen $R = \mathbf{R}[x]$ és I ideál R-ben.
(a) Lássuk be, hogy két I-beli polinom lnko-ja is szükségképpen I-beli.
(b) Hány I-nek eleme (b1) π; (b2) $100x$; (b3) $x^2 - 1$; (b4) $x^2 + 1$?

Vizsgáljuk meg a fenti kérdéseket $R = \mathbf{Z}[x]$-ben is.