

Session 7a-7b.

Program. Tirsdag den 6/6 er overskriften „Kvadratiske talringe“, med materiale fra RNG6; øvelser fra RNG6: 2, 3, 4, 5, 9, 11; Eks.opg.

Fredag den 9/6 er overskriften „Polynomier; endelige legemer“, med materiale fra POL4-5; øvelser fra RNG6: 8, 13; POL4: 1, 2, 3, 5; Eks.opg.

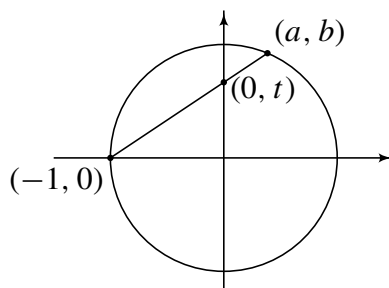
Pensum. Det officielle pensum findes nu fra kurssets hjemmeside. Bemærk, at pensum er en anelse mindre end først annonceret, idet bl.a. afsnittene om Noether's isomorforisætninger er røget ud af pensum.

Nøgleord: Kvadratisk tal, kvadratisk talring $R = \mathbb{Z}[\xi]$, konjugering, normen $N: R \rightarrow \mathbb{Z}$, Gauss' talring $\mathbb{Z}[i]$, diofantisk ligning, karakterisering af enheder og Pell's ligning $x^2 - bxy + cy^2 = \pm 1$ (eller $N(\alpha) = \pm 1$).

Og et par yderligere **nøgleord**, du kan prøve dig selv med efter tirsdagens undervisning: Euklidisk ring; karakterisering af primelement og irreducible elementer; Pell's ligning $N(\alpha) = \pm 1$, Euler's sætning (om $x^2 + y^2 = p$), antal løsninger til ligningen $x^2 + y^2 = k$, pythagoræiske talsæt.

Kommentar. At Gauss' talring $\mathbb{Z}[i]$ er faktoriel (=UFD), medfører Euler's sætning: ethvert primtal $p \equiv 1 \pmod{4}$ er en sum af to kvadrater, $p = x^2 + y^2$. Det medfører også resultater om ligningen $x^2 + y^2 = k$. Og specielt om ligningen $x^2 + y^2 = z^2$: Vi finder de pythagoræiske talsæt (x, y, z) med givet z .

Det er i øvrigt ikke svært at *parametrisere* de pythagoræiske talsæt: Vi har $x^2 + y^2 = z^2$, hvis og kun hvis $(x/z)^2 + (y/z)^2 = 1$, så pythagoræiske talsæt svarer til punkter (a, b) på enhedscirklen med positive rationale koordinater, nemlig $a = x/z$ og $b = y/z$. Punktet $(a, b) \neq (-1, 0)$ på cirklen svarer til tallet $t \in \mathbb{R}$ bestemt ved at $(-1, 0)$, $(0, t)$ og (a, b) ligger på ret linie.



Med givet t bliver $a = (1 - t^2)/(1 + t^2)$, $b = 2t/(1 + t^2)$, og $t \in \mathbb{Q}$, hvis og kun hvis $a, b \in \mathbb{Q}$. Med $t = v/u$ får vi $a = (u^2 - v^2)/(u^2 + v^2)$ og $b = 2uv/(u^2 + v^2)$ og dermed det pythagoræiske talsæt $(u^2 - v^2, 2uv, u^2 + v^2)$. Det er ikke svært at vise, at alle primitive pythagoræiske talsæt (x, y, z) , hvor y er lige, er af denne form. Fx svarer $(3, 4, 5)$, $(5, 12, 13)$, og $(15, 8, 17)$ til, henholdsvis, $t = 1/2$, $t = 2/3$, og $t = 1/4$.

Bemærk, at parameterfremstillingen *ikke* fortæller, for et givet z , hvor mange primiske par (x, y) (om overhovedet nogen), der løser ligningen $x^2 + y^2 = z^2$. Det er dette sidste problem, som vi behandler.

Kommentar. Ringen $\mathbb{Z}[X]$ af polynomier med heltalskoefficienter er *ikke* et hovedidealområde. Fx er det let at se, at polynomierne med lige konstantled er et ideal, og at dette ideal

ikke er et hovedideal. Gauss' sætning udsiger, at ringen $\mathbb{Z}[X]$ er faktoriel. Denne ring er altså et eksempel på et UFD, der ikke er et PID. Der er naturligvis en sammenhæng mellem polynomier i $\mathbb{Z}[X]$ og i $\mathbb{Q}[X]$, som er nøjere beskrevet i POL4 (kursorisk). Eisenstein's kriterium tillader at slutte, at en række polynomier i $\mathbb{Z}[X]$ og i $\mathbb{Q}[X]$ er irreducible. Fx følger det, at der i $\mathbb{Q}[X]$ er irreducible polynomier af enhver positiv grad. Det samme gælder i øvrigt i ringen $\mathbb{F}_p[X]$.

Kuglerne.

- *Enhederne* i $R = \mathbb{Z}[\xi]$ er elementerne α med $N(\alpha) = \pm 1$.
 - *Divisorer.* Antag, at $\delta | \alpha$. Så er $N(\delta) | N(\alpha)$, og δ er triviel divisor α præcis når $N(\delta)$ er triviel divisor $N(\alpha)$.
 - *Primelement og irreducibelt element.* Betragt $\pi = x + y\xi$ med $(x, y) = 1$, og sædvanligt primtal p . Da gælder:
 - (1) π er primelement $\iff N(\pi) = \pm(\text{sædvanligt primtal})$.
 - (2) p er primelement $\iff z^2 - bz + c \equiv 0 \pmod{p}$ ikke har løsninger.
 - (3) p er irreducibel $\iff x^2 - bxy + cy^2 = \pm p$ ikke har løsninger.
 - *Euler's sætning.* Et primtal $p \equiv 1 \pmod{4}$ kan skrives som sum af to kvadrater, $p = x^2 + y^2$.
 - *Ligningen $x^2 + y^2 = k$,* hvor k har primopløsning $k = 2^l q_1^{n_1} \cdots q_r^{n_r} p_1^{m_1} \cdots p_s^{m_s}$ med $q_j \equiv 3 \pmod{4}$ og $p_i \equiv 1 \pmod{4}$, har løsninger, netop når alle eksponenter n_j er lige; og „så“ har ligningen præcis $4(m_1 + 1) \cdots (m_s + 1)$ løsninger (x, y) .
 - *Ligningen $x^2 + y^2 = k^2$,* med k som ovenfor, har primitive løsninger, netop når $l = n_1 = \cdots = n_r = 0$; og så har ligningen 2^{s-1} essentielt forskellige løsninger.
 - *Diofantiske ligninger* er ligninger, hvortil man søger heltalsløsninger (eller rationale løsninger). Eksempler er ligningerne $x^n + y^n = z^n$, som ikke kan løses med naturlige tal, når $n > 2$, og ligningen $x^2 + bxy + cy^2 = k$ (for givne $a, b, k \in \mathbb{Z}$). Den sidste ligning svarer til at bestemme tal $\alpha = x + y\xi \in \mathbb{Z}[\xi]$ med $N(\alpha) = k$. Specielt, for $k = \pm 1$, fremkommer Pell's ligning $x^2 + bxy + cy^2 = \pm 1$, der svarer til at bestemme enheder ($N(\alpha) = \pm 1$) i talringen $\mathbb{Z}[\xi]$.
 - *Primtal er primelementer,* i $\mathbb{Z}[X]$.
 - *Gauss' sætning.* $\mathbb{Z}[X]$ er UFD og – mere generelt: R er UFD $\implies R[X]$ er UFD.
 - *Eisenstein's irreducibilitetskriterium,* for $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ i $\mathbb{Z}[X]$: Hvis $p | a_{n-1}, \dots, p | a_0$ og $p^2 \nmid a_0$ (for et primtal p), så er $f(X)$ irreducibelt (i $\mathbb{Z}[X]$ og i $\mathbb{Q}[X]$).
- Hvornår** var det nu det var? Pythagoras 580–500 (ca.), Diophantus 200–284, John Pell 1611–1685, Leonhard Euler 1707–1783, Carl Friedrich Gauss 1777–1855, Ferdinand Gotthold Max Eisenstein 1823–1852.

På sigt: Onsdag den 14/6 er sidste undervisningsdag. Det er en erstatning for Store Bededagsundervisningen, og undervisningen afholdes efter fredagsskema. Overskriften er „Polynomier; endelige legemer“, med materiale fra POL4-5; øvelser fra POL5: 1, 2; Eks.opg. .