

Ugeseddel 15.

Program. Emnerne i den 15. (og sidste) uge, 12/5-15/5, er kvadratiske talringe og polynomier (fra RNG6 og POL4-5), altså en gentagelse af emnerne fra den 14. uge. og POL4-5. Ugens øvelser er: POL4: 1, 2, 3, 5; POL5: 1, 2; samt eksamensopgaver, som aftalt på de enkelte øvelseshold. Efter denne uge lægges en afsluttende ugeseddel 16 ud på nettet. Mandag i denne uge aftales også tidspunktet for spørgetimen inden den mundtlige eksamen. Spørgetime inden skriftlig eksamen aftales med instruktorerne på de enkelte øvelseshold.

I den 14. uge afsluttede jeg (næsten) gennemgangen af RNG6. Bemærk, at der på ugeseddel 14, som eksempel under Numeriske betingelser, to steder skulle have stået $\nu(a) := |N(a)|$.

Nøgleord: kvadratisk tal, kvadratisk talring, diskriminant, norm, diofantisk ligning, Pell's ligning, Euler's sætning, pytagoræiske 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 $x^2 + y^2 = z^2$: Vi finder de pytagoræiske talsæt (x, y, z) med givet z .

Det er i øvrigt ikke svært at *parametrisere* de pytagoræiske talsæt: Vi har $x^2 + y^2 = z^2$, hvis og kun hvis $(x/z)^2 + (y/z)^2 = 1$, så pytagoræiske 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 $(-1, t)$, $(0, t)$ 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 pytagoræiske talsæt $(u^2 - v^2, 2uv, u^2 + v^2)$. Det er ikke svært at vise, at alle primitive pytagoræiske 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) , der løser ligningen $x^2 + y^2 = z^2$. Det er dette sidste problem, som vi behandlede.

Kuglerne.

- *Normen*, bestemt ved $N(\alpha) = \alpha\alpha'$, er en afbildning $\mathbb{Z}[\xi] \rightarrow \mathbb{Z}$. Den er multiplikativ: $N(\alpha\beta) = N(\alpha)N(\beta)$.

- *Enheder*. ε er en enhed $\iff N(\varepsilon) = \pm 1$.

- *Divisorer*. $\delta \mid \alpha \implies N(\delta) \mid N(\alpha)$. Hvis $\delta \mid \alpha$, så er δ en ikke-triviell divisor i α præcis når $N(\delta)$ er ikke-triviell divisor i $N(\alpha)$.

- *Irreducibelt element og primelement*. Med $\pi = x + y\xi$ hvor $(x, y) = 1$ og $p =$ sædvanligt primtal gælder:

π er primelement $\implies N(\pi) = \pm$ primtal $\implies \pi$ er irreducibel. Hvis $\mathbb{Z}[\xi]$ er faktoriel, så gælder „ \iff “ begge steder. [Faktisk gælder der altid „ \iff “ i den første implikation (se det ekstra materiale på hjemmesiden), men det hører ikke med til pensum.]

p er irreducibel $\iff x^2 - bxy + cy^2 = \pm p$ har ingen løsninger i \mathbb{Z}^2 .

p er primelement $\iff z^2 - bz + c \equiv 0 \pmod{p}$ har ingen løsninger i \mathbb{Z} .

- *Euler's sætning*. Et primtal $p \equiv 1 \pmod{4}$ kan skrives som sum af to kvadrater, $p = x^2 + y^2$.

Hvornår var det nu det var? Leonhard Euler 1707–1783, Carl Friedrich Gauss 1777–1855, Pythagoras 580–500 (ca.).

Anders Thorup