

10. Nogle diofantiske ligninger.

(10.1). I dette kapitel betragtes nogle diofantiske ligninger, specielt nogle af de ligninger, der kan behandles via kvadratiske talringe. Ligningerne har fået deres tilnavn efter matematikeren Diofant, der levede i Alexandria ca 200–284. Han interesserede sig for rationale løsninger til visse lineære ligninger. I forbindelse med de diofantiske ligninger omtalt her vil vi imidlertid underforstå, at det er ligninger, hvortil man søger *heltalsløsninger*, – i hvert fald hvis intet andet er nævnt. At *løse den diofantiske ligning* går principielt ud på følgende: (1) afgør, om ligningen har (heltals)løsninger; (2) (hvis den har løsninger) afgør, hvor mange løsninger den har; (3) hvis den kun har endelig mange løsninger, så bestem dem alle sammen; (4) hvis den har uendelig mange løsninger, så beskriv dem (sig noget begavet om dem!).

De mest berømte diofantiske ligninger indgår i følgende resultat:

Fermat's store Sætning. *For hver eksponent $n > 2$ har den diofantiske ligning,*

$$x^n + y^n = z^n, \quad \text{med } x, y, z > 0, \quad (10.1.1)$$

ingen løsninger.

Det generelle resultat, for alle $n > 2$, blev bevist af Andrew Wiles i 1995.

Enhvert naturligt tal $n > 2$ er deleligt enten med 4 eller med et ulige primtal p . Det følger let, at for at indse det generelle resultat er det nok at vise, at ligningen ikke har løsninger, når $n = 4$ og når $n = p$ er et ulige primtal. Vi viser umuligheden for $n = 4$, essentielt med Fermat's bevis, og for $n = 3$.

Yderligere behandler vi nogle diofantiske ligninger af formen $y^2 = x^3 + k$, og vi slutter kapitlet af med nogle ligninger af formen $x^2 - bxy + cy^2 = \pm p$.

Den diofantiske ligning (10.10.1) for $n = 2$ har som bekendt mange løsninger. Det første resultat herunder kan opfattes som en parameterfremstilling af løsningerne.

(10.2) Pytagoræiske tripler. *Løsningerne til den diofantiske ligning,*

$$x^2 + y^2 = z^2, \quad \text{med } (x, y) = 1, \quad x, y, z > 0, \quad y \text{ er lige,}$$

er netop talsættene (x, y, z) med følgende fremstillinger:

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2, \quad \text{hvor } 0 < b < a, \quad (a, b) = 1 \text{ og } ab \text{ er lige.}$$

Parret (a, b) er entydigt bestemt ved (x, y, z) .

Bevis. Antag, at (x, y, z) opfylder betingelserne. Af ligningen følger, at en fælles divisor i x, z også er divisor i y . Derfor er $(x, z) = 1$ og $(y, z) = 1$. Da y er lige og $(x, y) = 1$, er x og z ulige. Skriv nu ligningen på formen,

$$y^2 = (z - x)(z + x). \quad (10.2.1)$$

27. oktober 2008

Et tal $d > 1$, der er divisor i begge faktorer $z - x$ og $z + x$ på højresiden, er også divisor i summen $2z$ og i differensen $2x$; da $(x, z) = 1$, er $d = 2$. Omvendt er 2 divisor i begge faktorer, da x og z begge er ulige. Divideres begge faktorer med 2, bliver de primiske, og deres produkt bliver $(y/2)^2$, altså et kvadrat. Af Aritmetikkens Fundamentalsætning følger så, at hver af de dividerede faktorer må være et kvadrat, og vi får fremstillinger:

$$z - x = 2b^2, \quad z + x = 2a^2, \quad y^2 = 4a^2b^2, \quad \text{hvor } (a, b) = 1, \text{ og } 0 < b < a,$$

hvoraf

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2.$$

Og et af tallene a og b er lige, da x er ulige. Omvendt er det klart, at betingelserne på a, b medfører betingelserne på x, y, z , og at (a, b) er entydigt bestemt. \square

(10.3) Sætning. (Fermat) *Den diofantiske ligning,*

$$x^2 + y^4 = z^4, \quad x, y, z > 0, \quad (10.3.1)$$

har ingen løsninger. Specielt gælder, at ligningen $x^4 + y^4 = z^4$, altså Fermat's ligning (10.1.1) med $n = 4$, ikke har positive heltalsløsninger.

Bevis. Den anden påstand er en konsekvens af den første, thi hvis (x, y, z) løser den anden ligning, vil (x^2, y, z) løse den første.

Den første påstand vises ved 'descente infinie', der essentielt er fuldstændig induktion: Vi antager, at (10.3.1) har en løsning (x, y, z) . Vi viser, at vi her til kan bestemme en ny løsning (x_1, y_1, z_1) med kravet $z_1 < z$. Denne bestemmelse ville så kunne gentages, men det er naturligvis umuligt vedvarende at opfylde kravet, når tallene z skal være positive.

Bestemmelsen af den nye løsning sker i en række skridt:

(1) Vi kan antage, at $(y, z) = 1$. Sæt hertil $d := (y, z)$. Det følger så af ligningen, at $d^4 | x^2$, og dermed at $d^2 | x$. Derfor er $(x_1, y_1, z_1) := (x/d^2, y/d, z/d)$ også en løsning, og hvis $d > 1$ er $z_1 < z$.

(2) Da $(y, z) = 1$ følger det umiddelbart af ligningen, at $(x, y) = 1$ og $(x, z) = 1$.

(3) Tallet z må være ulige. Hertil reduceres ligningen modulo 4. Et kvadrat er kongruent med 0 eller 1. Hvis z var lige, ville højresiden være kongruent med 0, men så måtte begge kvadrater på venstresiden være kongruente med 0; specielt ville både x og y være lige, i modstrid med at $(x, y) = 1$.

(4) Nu deles i to tilfælde: y er lige og y er ulige.

(4a) Antag, at y er lige. Så er z og x begge ulige. Ligningen kan skrives

$$y^4 = (z^2 - x)(z^2 + x). \quad (10.3.2)$$

Venstresiden er delelig med $2^4 = 16$. De to faktorer på højresiden har tallet 2 som største fælles divisor; en af faktorerne er altså delelig med 8, og den anden er delelig med 2 og

ikke med 4. Idet vi et øjeblik tillader x at være negativ, og eventuelt erstatter x med $-x$, kan vi antage, at det er faktoren $z^2 + x$, der er delelig med 8. Af (10.3.2) og Aritmetikens Fundamentalsætning får vi derfor fremstillinger:

$$z^2 - x = 2a^4, \quad z^2 + x = 8b^4, \quad \text{med } a \text{ ulige.}$$

Den første ligning medfører, at $(z, a) = 1$. Ved addition af de to første ligninger får vi ligningen $z^2 = a^4 + 4b^4$, der omskrives til

$$4b^4 = (z - a^2)(z + a^2). \quad (10.3.3)$$

Af (10.3.3) og Aritmetikens Fundamentalsætning fås ligninger $z - a^2 = 2u^4$, $z + a^2 = 2v^4$. Subtraktion giver $a^2 = v^4 - u^4$, eller

$$a^2 + u^4 = v^4.$$

Sættet (a, u, v) er altså løsning til den oprindelige ligning. Øjensynlig er $a^2 < z$, og dermed er $2v^4 = z + a^2 < 2z$; specielt er $v < z$. Løsningen (a, u, v) opfylder altså det stillede krav.

(4b) Antag, at y er ulige. Da z er ulige, må x være lige. Skriv ligningen på formen,

$$x^2 = (z^2 - y^2)(z^2 + y^2).$$

Da $(y, z) = 1$, får vi fremstillinger $z^2 - y^2 = 2b^2$ og $z^2 + y^2 = 2c^2$. Sæt $a := yz$. Så er

$$c^4 - b^4 = (c^2 - b^2)(c^2 + b^2) = y^2 z^2 = a^2,$$

altså $a^2 + b^4 = c^4$. Derfor løser (a, b, c) den oprindelige ligning, og da $c^2 < b^2 + c^2 = z^2$ er $c < z$; det stillede krav er altså opfyldt. \square

(10.4) Påstand. Den diofantiske ligning,

$$x^2 + y^4 = 2z^4, \quad \text{med } x, y, z > 0, \quad (10.4.1)$$

har ingen løsninger.

Bevis. Beviset for påstanden er ved 'descente infinie', essentielt som det foregående bevis.

Antag, at (x, y, z) er en løsning. Vi bestemmer en ny løsning (u, v, w) med $w < z$.

- (1) Det kan antages, at $(y, z) = 1$. Heraf følger videre, at også $(x, z) = 1$.
- (2) Tallene x, y, z er alle ulige. Det indses ved at reducere ligningen modulo 4.
- (3) Omskriv ligningen til følgende:

$$z^4 = \left(\frac{y^2 + x}{2}\right)^2 + \left(\frac{y^2 - x}{2}\right)^2.$$

27. oktober 2008

Da $(y, z) = 1$, er de to kvadrater på højresiden primiske. Et af dem må være lige; idet vi et øjeblik tillader x at være negativ, kan vi eventuelt erstatte x med $-x$ og antage, at $(y^2 - x)/2$ er lige. Nu kan (10.2) anvendes. Det følger, at der findes fremstillinger $(y^2 + x)/2 = a^2 - b^2$, $(y^2 - x)/2 = 2ab$, $z^2 = a^2 + b^2$, med $(a, b) = 1$ og ab lige. Ved subtraktion og addition fås ligningerne:

$$x = a^2 - b^2 - 2ab, \quad y^2 = a^2 - b^2 + 2ab, \quad z^2 = a^2 + b^2.$$

(4) Tallet b må være lige. Vi har nemlig $y^2 + 2b^2 = (a + b)^2$, som kan betragtes modulo 4. Tallet y er ulige og hvis også b var ulige, ville $y^2 + 2b^2$ være kongruent med 3, i modstrid med at kvadratet $(a + b)^2$ må være kongruent med 0 eller 1.

(5) I ligningen $z^2 = a^2 + b^2$ fra (3) er b lige og $(a, b) = 1$. Altså findes fremstillinger,

$$a = c^2 - d^2, \quad b = 2cd, \quad z = c^2 + d^2, \quad \text{med } (c, d) = 1 \text{ og } cd \text{ lige.} \quad (10.4.2)$$

(6) Ligningen $y^2 = a^2 - b^2 + 2ab$ fra (3) kan skrives

$$2b^2 = (a + b - y)(a + b + y). \quad (*)$$

Her er $(a, b) = 1$, og da b er lige, er $a + b$ ulige. Yderligere er $a + b$ og y primiske, thi et primtal p , der er divisor i $a + b$ og i y , må være ulige, og divisor i $2b^2$ og dermed i b ; men p kan ikke både gå op i $a + b$ og i b , da $(a, b) = 1$.

De to faktorer på højresiden af (*) har altså 2 som største fælles divisor. Da venstresiden er delelig med 8, må en af de to faktorer være delelig 4 og den anden med 2 og ikke med 4. Idet vi et øjeblik tillader y at være negativ, og eventuelt erstatter y med $-y$, kan vi antage, at det er den anden faktor, der er delelig med 4. Nu følger det af (*), og Aritmetikkens Fundamentalsætning, at vi har fremstillinger $a + b - y = 2f^2$, $a + b + y = 4g^2$, $b = 2fg$, hvor $(f, g) = 1$ og f er ulige. Addition og subtraktion giver ligningerne,

$$a + b = 2g^2 + f^2, \quad y = 2g^2 - f^2, \quad b = 2fg, \quad \text{med } f \text{ ulige og } (f, g) = 1. \quad (10.4.3)$$

(7) Af de to udtryk for b , i (10.4.2) og (10.4.3), følger specielt, at $fg = cd$. Da $(f, g) = 1$ og $(c, d) = 1$, følger det af Aritmetikkens Fundamentalsætning, at der findes tal v, w, s, t således, at

$$f = vt, \quad g = ws, \quad c = wt, \quad d = vs, \quad \text{med } (v, w) = 1 \text{ og } (s, t) = 1.$$

(8) Af (10.4.2) og (10.4.3) fås to udtryk for $a + b$, og det giver ligningen $c^2 - d^2 + 2cd = 2g^2 + f^2$, altså $2g^2 + d^2 - 2cd + f^2 - c^2 = 0$. Indsættelse heri af ligningerne fra (7) giver ligningen:

$$(2w^2 + v^2)s^2 - 2vwst + (v^2 - w^2)t^2 = 0. \quad (10.4.4)$$

Det er en andengradsligning i s, t , homogen af grad 2, med diskriminanten,

$$4v^2w^2 - 4(2w^2 + v^2)(v^2 - w^2) = 4(2w^4 - v^4).$$

27. oktober 2008

Da andengradsligningen har heltalsløsninger, må diskriminanten være et kvadrat. Derfor findes et helt tal u med $2w^4 - v^4 = u^2$, altså

$$u^2 + v^4 = 2w^4.$$

Efter et eventuelt fortegnsskift, kan det antages at $u, v, w > 0$. Altså er (u, v, w) en løsning (10.4.1). Af $tw = c < c^2 < c^2 + d^2 = z$ følger $w < z$. Den nye løsning (u, v, w) har altså mindre trediekoordinat, som ønsket. \square

(10.5) Ak og ve. Opdagede du, at der er noget helt galt med Påstand (10.4)? Det er jo aldeles trivielt, at $(x, y, z) = (1, 1, 1)$ løser ligningen! Hvor i „beviset“ går det galt? Vis, at man ved hjælp af „beviset“ kan bestemme uendelig mange løsninger til ligningen, ja faktisk alle løsningerne.

Svar. Det er lidt problematisk, at „beviset“ går ud fra at de indgående størrelser er positive. Det kan repareres, hvis nogle størrelser undervejs bliver negative, men den egentlige fejl sker fra skridt (3), hvor det antages, at begge kvadrater er forskellige fra 0. Det kan ikke udelukkes, at $y^2 - x = 0$, altså at $b = 0$. Det sker præcis, når $y^2 = x$. Da $(x, y) = 1$, er det altså, når $x = y = 1$. Det er derfor præcis i løsningen $(x, y, z) = (1, 1, 1)$, at argumentet bryder sammen.

Men det betyder på den anden side, at man ud fra enhver anden løsning efter endelig mange skridt kommer til løsningen $(1, 1, 1)$. Og faktisk kan proceduren gøres konstruktiv: Ud fra en løsning (u, v, w) , med positive og parvis primiske u, v, w , kan man essentielt rekonstruere (x, y, z) således:

Den homogene andengradsligning (10.4.4), for givne (u, v, w) , havde diskriminanten $4u^2 = (2u)^2$. De 4 løsninger (s, t) med $(s, t) = 1$ svarer til de to uforkortelige brøker s/t , bestemt ved den sædvanlig løsningsformel,

$$s/t = \frac{vw \pm u}{v^2 + 2w^2}$$

(nemlig med (s, t) også $(-s, -t)$). På højresiden er tælleren lige og nævneren ulige; da $(s, t) = 1$, følger det, at s er lige og t er ulige. Herefter bestemmes f, g, c, d som i (7), og videre, fra (10.4.2) og (10.4.3),

$$\begin{aligned} a &= w^2t^2 - v^2s^2, & b &= 2v w s t, & a + b &= 2w^2s^2 + v^2t^2, \\ z &= w^2t^2 + v^2s^2, & y &= 2w^2s^2 - t^2v^2. \end{aligned}$$

Endelig var x bestemt i (3) som $x = a^2 - b^2 - 2ab = 2a^2 - (a + b)^2$; med de fundne udtryk for a og $a + b$ kan det skrives $x = 2(w^2t^2 - v^2s^2)^2 - (2w^2s^2 + v^2t^2)^2$. Under brug af at $2w^4 - v^4 = u^2$ er det let at reducere udtrykket:

$$x = u^2(t^4 - 2s^4) - 8v^2v^2s^2t^2$$

27. oktober 2008

Ud fra løsningen $(u, v, w) = (1, 1, 1)$ fås $s/t = 2/3$ (idet den anden løsning $s/t = 0$ ikke kan bruges), og altså $(s, t) = (2, 3)$. Det giver løsningen $(239, 1, 13)$. Ud fra denne løsning som (u, v, w) fås $s/t = -2/3$ eller $s/t = 84/113$. De to værdier af (s, t) giver, henholdsvis, de nye løsninger:

$$(x, y, z) = (2750251, 1343, 1525), \quad \text{og} \quad (x, y, z) = (??, 2372159, 2165017).$$

Du må selv bestemme det manglende tal x i det sidste koordinatsæt.

(10.6) Sætning. *Den diofantiske ligning,*

$$x^3 + y^3 = z^3, \quad \text{med} \quad x, y, z \neq 0, \quad (10.6.1)$$

har ingen løsninger.

I beviset skal vi bruge, at med en 3' die enhedsrod $\rho = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$, hvor så $\rho^2 + \rho + 1 = 0$, kan vi faktorisere ligningens venstreside: for vilkårlige komplekse tal x, y gælder ligningen,

$$x^3 + y^3 = (x + y)(x + \rho y)(x + \rho^2 y). \quad (10.6.2)$$

Ligningen er nemlig trivielt opfyldt for $y = 0$; for $y \neq 0$ fås (10.6.2) ud fra ligningen $X^3 - 1 = (X - 1)(X - \rho)(X - \rho^2)$ ved at indsætte $X = -x/y$ og multiplicere med $-y^3$.

Desuden skal vi i beviset udføre regninger i den kvadratiske talring $R := \mathbb{Z}[\rho]$. Vi beviser Sætning (10.6) ved at vise, at (10.6.1) ikke har løsninger med $x, y, z \in \mathbb{Z}[\rho]$.

Lad os minde om, at $R = \mathbb{Z}[\rho]$ er delringen af \mathbb{C} bestående af alle komplekse tal af formen $a + b\rho$, hvor $a, b \in \mathbb{Z}$. Det er velkendt, at R er et hovedidealområde (et PID); specielt er R en faktoriel ring (et UFD). Den 6'te enhedsrod $\zeta := 1 + \rho$ tilhører R , og enhederne i R er de 6 potenser ζ^i for $i = 0, \dots, 5$:

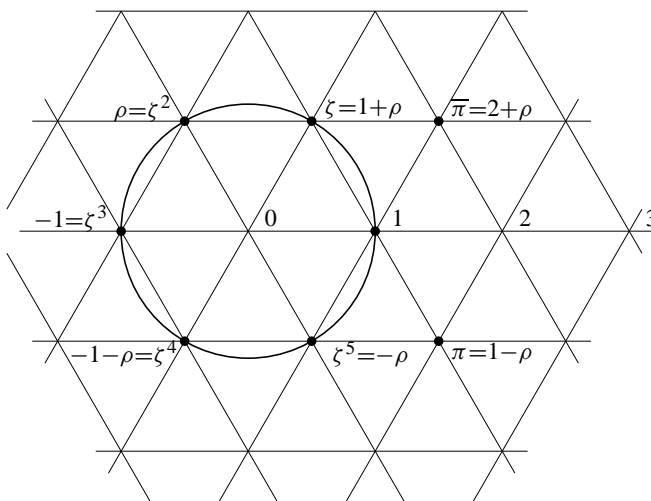
$$R^* : \quad \zeta^0 = 1, \quad \zeta = 1 + \rho, \quad \zeta^2 = \rho, \quad \zeta^3 = -1, \quad \zeta^4 = -\rho - 1, \quad \zeta^5 = -\rho.$$

Afbildningen $N: R \rightarrow \mathbb{R}$ defineres ved $N(\alpha) = |\alpha|^2$ (kvadratet på modulus af α). (Den kaldes med en klassisk sprogbrug for *normen*, selv om den jo ikke er en norm i vektorrumforstand.) Afbildningen er øjensynlig multiplikativ, med positive værdier når $\alpha \neq 0$. Videre har den som bekendt heltalsværdier for $\alpha \in R$; specielt er $|\alpha| \geq 1$ for alle $\alpha \neq 0$ i R . Det følger, og vi bruger det gentagne gange herunder, at hvis δ er divisor i α (i ringen R), og $\alpha \neq 0$, så er $|\delta| \leq |\alpha|$. (Hvis lighed gælder i denne ulighed, er δ endda en triviell divisor i α , dvs $\alpha = \varepsilon\delta$, hvor ε er en af de 6 enheder.)

I det følgende betragtes tallet $\pi := 1 - \rho = \frac{3}{2} - \frac{i}{2}\sqrt{3} \in R$.

Normen af π er $N(\pi) = \pi\bar{\pi} = 3$, og normen er altså specielt et (sædvanligt) primtal. Heraf følger som bekendt, at π er et primelement i R . Øjensynlig er $\bar{\pi} = 2 + \rho$. Udregningen $\bar{\pi} = 2 + \rho = (1 + \rho)(1 - \rho) = \zeta\pi$ viser, at det konjugerede tal $\bar{\pi}$ er associeret med π ; tallet 3 har i R primopløsningen,

$$3 = \pi\bar{\pi} = \zeta\pi^2.$$



Vi vil flere gange bruge følgende resultat:

Lemma. Hvis $\alpha \in R$ og $\pi \nmid \alpha$, så er $\alpha^3 \equiv \pm 1 \pmod{\pi^4}$.

Bevis. Hertil bemærkes først, at hovedidealet R_3 i R består af alle tal af formen $3a + 3b\rho$, hvor $a, b \in \mathbb{Z}$. Modulo R_3 er hvert tal $\alpha \in R$ derfor kongruent med et tal af formen $a + b\rho$, hvor $0 \leq a, b < 3$. Der er 3 muligheder for a og 3 muligheder for b , og altså 9 sideklasser modulo R_3 . Af ligningen $3 = \pi\bar{\pi}$ fremgår specielt, at $R\pi \subset R_3$. Derfor er antallet af sideklasser modulo $R\pi$ en ægte divisor i 9. Nu følger det nemt, at antallet må være 3. Ringen $R/R\pi$ har derfor 3 elementer, og så må den være isomorf med legemet $\mathbb{Z}/\mathbb{Z}3$. Specielt er hvert tal i R modulo $R\pi$ kongruent med et af de 3 tal 0 og ± 1 . Desuden følger det, lige som i Fermat's lille Sætning, at for hvert $\beta \in R$ er $\beta^3 \equiv \beta \pmod{R\pi}$.

Antag nu, at $\pi \nmid \alpha$. Så er $\alpha \equiv \pm 1 \pmod{\pi}$, så vi kan skrive $\alpha = \pm 1 + \beta\pi$ med $\beta \in R$. Binomialformlen og ligningen $3 = \zeta\pi^2$ giver, at

$$\alpha^3 = \pm 1 + 3\beta\pi \pm 3\beta^2\pi^2 + \beta^3\pi^3 = \pm 1 + \pi^3(\zeta\beta \pm \zeta\beta^2\pi + \beta^3).$$

I parentesen på højresiden er π divisor i $\pm\zeta\beta^2\pi$; yderligere er π divisor i $\zeta\beta - (\zeta\beta)^3 = \zeta\beta + \beta^3$. Derfor er parentesen delelig med π . Med faktoren π^3 foran parentesen følger det, at $\alpha \equiv \pm 1 \pmod{\pi^4}$, som påstået. \square

Antag nu, at (10.6.1) har en løsning med $x, y, z \in R$. Vi vil føre dette til en modstrid. For det første følger det klart af ligningen, at hvis to af tallene x, y, z i R har en fælles primfaktor, så vil dette primelement også være divisor i det tredje af tallene. Vi kan derfor, efter at have divideret x, y, z med eventuelle fælles primfaktorer antage, at x, y, z er parvis primiske.

Vi noterer dernæst, at et af tallene x, y, z må være deleligt med π . I modsat fald følger det nemlig af Lemmaet, at modulo π^4 er hver af potenserne x^3, y^3 , og z^3 kongruent med ± 1 ; af ligningen følger derfor, modulo π^4 , at med passende fortegnvalg er $\pm 1 \pm 1 \mp 1 \equiv 0$. Værdien af $\pm 1 \pm 1 \mp 1$ er ± 1 eller ± 3 ; specielt er værdien ikke 0. Derfor er

$$|\pi^4|^2 \leq |\pm 1 \pm 1 \pm 1|^2,$$

men det er en modstrid, thi venstresiden er $3^4 = 81$, og højresiden er højst $(1 + 1 + 1)^2 = 9$.

27. oktober 2008

I løsningen er altså tallene x, y, z parvis primiske og ét af dem er deleligt med π . Vi kan antage, at $\pi \mid z$, thi hvis fx $\pi \mid x$, så er antagelserne opfyldt for $(z, -y, x)$, som øjensynlig også løser ligningen.

Vi kan altså om løsningen $(x, y, z) \in R^3$ antage, at (10.6.1) gælder, og desuden, at tallene er parvis primiske, altså at $(x, y) = 1$, og at $\pi \mid z$. Modstriden er nu en konsekvens af det følgende resultat.

(10.7) Lemma. For hver enhed ε i $R = \mathbb{Z}[\rho]$ har ligningen, for elementer $x, y, z \in R$,

$$x^3 + y^3 = \varepsilon z^3, \quad \text{med } xyz \neq 0, \quad (x, y) = 1, \quad \text{og } \pi \mid z, \quad (10.7.1)$$

ingen løsninger.

Bevis. I beviset betegner vi, for hvert tal $\alpha \neq 0$ i R , med $v(\alpha)$ det antal gange π forekommer i primopløsningen af α . Beviset er ved „descente infinie“ efter $n := v(z)$: Vi antager, at der er givet en (tænkt) løsning (x, y, z) til (10.7.1) (med et givet ε), og konstruerer en ny løsning (x', y', z') til en ligning af formen (10.7.1) (evt. med et andet ε) og med $v(z') < v(z)$.

Vi bemærker først, at der må gælde $\pi^2 \mid z$, altså at $n \geq 2$. Venstresiden i (10.7.1) er nemlig kongruent modulo π^4 med $\pm 1 \pm 1$ og højresiden er kongruent med 0 modulo π^3 . Altså er $\pm 1 \pm 1$ delelig med π^3 . Det følger, som ovenfor, at $\pm 1 \pm 1 = 0$. Derfor er venstresiden delelig med π^4 . Altså er z^3 delelig med π^4 , og så må z være delelig med π^2 .

Nu anvender vi faktoriseringen (10.6.2), her med $x, y, z \in R$, og får ligningen,

$$(x + y)(x + \rho y)(x + \rho^2 y) = x^3 + y^3 = \varepsilon z^3. \quad (10.7.2)$$

Primopløsning af venstresiden fås ved at primopløse de tre parenteser, og primopløsning af højresiden fås ved at primopløse z . I primopløsningen må altså alle primfaktorer forekomme med eksponent delelig med 3, og alle primfaktorerne er primfaktorer i z . For at bestemme eventuelle primfaktorer, der er fælles for to af parenteserne, betragtes differenserne:

$$\begin{aligned} (x + y) - (x + \rho y) &= (1 - \rho)y = \pi y, \\ (x + y) - (x + \rho^2 y) &= (1 + \rho)(1 - \rho)y = \zeta \pi y, \\ (x + \rho y) - (x + \rho^2 y) &= \rho(1 - \rho)y = \rho \pi y. \end{aligned}$$

Her er ρ og ζ enheder og $\pi \nmid y$. Primfaktorerne i parenteserne er divisorer i z , og specielt ikke divisorer i y . Heraf ses, at det eneste primelement, der kan gå op i to af parenteserne, er π . Desuden ses, at primelementet π , som jo går op i z og derfor går op i parenteserne, må gå op i alle tre, præcis 1 gang i to af parenteserne og derfor $3n - 2$ gange i den tredje.

Der er symmetri mellem de tre parenteser, idet vi i ligningen kan erstatte y med ρy eller med $\rho^2 y$. Derfor kan vi antage, at det er den 3'die parentes $x + \rho^2 y$, der er delelig med π^{3n-2} . Ved at sammenligne primopløsningerne på de to sider af (10.7.2) ses nu, at bortset fra multiplikation med faktoren π og en eventuel enhed er hver af de tre parenteser en tredje

27. oktober 2008

potens, af parvis primiske tal i R . Med enheder $\varepsilon_j \in R^*$ og elementer $x', y', z' \neq 0$ i R har vi altså ligninger af følgende form:

$$x + y = \varepsilon_1 \pi x'^3, \quad x + \rho y = \varepsilon_2 \pi y'^3, \quad x + \rho^2 y = \varepsilon_3 \pi z'^3, \quad (10.7.3)$$

hvor $(x', y') = 1$. Desuden er $\pi \mid z'$, idet $v(\pi z'^3) = 3n - 2$ giver $v(z') = n - 1$, og vi har vist, at $n \geq 2$.

Multipliser den første ligning i (10.7.3) med 1, den anden ligning med ρ , og den tredje med ρ^2 , og læg sammen. På venstresiden bliver resultatet 0, fordi $1 + \rho + \rho^2 = 0$. På højresiden er hvert led deleligt med π ; dividerer højresiden med π . Resultatet bliver en ligning, med nye enheder ε_j ,

$$0 = \varepsilon_1 x'^3 + \varepsilon_2 y'^3 + \varepsilon_3 z'^3.$$

Efter eventuel division med ε_1 kan det antages, at $\varepsilon_1 = 1$. Flyt så leddet med z'^3 over på den anden side af lighedstegnet. Resultatet bliver en ligning af formen,

$$x'^3 + \varepsilon_2 y'^3 = \varepsilon' z'^3. \quad (10.7.4)$$

Her er π divisor i z' , men ikke i x' og y' . Som ovenfor følger det, at $\pm 1 \pm \varepsilon_2 = 0$, altså at $\varepsilon_2 = \pm 1$. Erstatte om nødvendigt y' med $-y'$, kan vi i (10.7.4) antage, at $\varepsilon_2 = 1$. Ligningen har så form som den i (10.7.1). Vi har set, at $(x', y') = 1$, og at $\pi \mid z'$. Altså opfylder (x', y', z') betingelserne i (10.7.1), med enheden ε' i stedet for ε . Yderligere så vi undervejs, at $v(z') = v(z) - 1$.

Hermed er den lovede nye løsning konstrueret. □

(10.8) Sætning. *Følgende diofantiske ligning har ingen løsninger:*

$$y^2 = x^3 + 7. \quad (10.8.1)$$

Bevis. Ligningen kan også skrives sådan:

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4). \quad (10.8.2)$$

Påstanden vises ved en kongruensbetragtning: Antag, at (x, y) løser (10.8.1), og betragt ligningen modulo 4. Ventresiden er kongruent med 0 eller 1 modul 4. Hvis x er lige, så er højresiden kongruent med 3, og hvis $x \equiv 3 \pmod{4}$, så er $x^3 \equiv x \equiv 3$, og højresiden er kongruent med $3 + 7 \equiv 2$, igen i modstrid med ligningen. Altså er $x \equiv 1 \pmod{4}$.

Da $x \equiv 1 \pmod{4}$, er faktoren $x + 2$ på højresiden af (10.8.2) kongruent med 3 modulo 4. Derfor har $x + 2$ en primfaktor $p \equiv 3 \pmod{4}$. Da p er divisor i venstresiden, er $y^2 \equiv -1 \pmod{p}$. Derfor er $\left(\frac{-1}{p}\right) = 1$, og så følger det af Reciprocitetssætningen, at $p \equiv 1 \pmod{4}$, i modstrid med at p var valgt med $p \equiv 3 \pmod{4}$. □

(10.9) Sætning. Af de to diofantiske ligninger (med $y \geq 0$),

$$(a) \quad y^2 = x^3 - 2, \quad (b) \quad y^2 = x^3 - 4, \quad (10.9.1)$$

har (a) kun løsningen $(x, y) = (3, 5)$ og (b) kun de to løsninger $(x, y) = (2, 2)$ og $(5, 11)$.

Bevis. (a) Vi bemærker først, at i en heltalsløsning (x, y) til (10.9.1)(a) må x være ulige, thi hvis x er lige, vil også y være lige; modulo 4 er så venstresiden kongruent med 0 og højresiden kongruent med 2.

I resten af beviset for (a) udnytter vi den kvadratiske talring $R := \mathbb{Z}[i\sqrt{2}]$, bestående af tal af formen $a + bi\sqrt{2}$ med $a, b \in \mathbb{Z}$. Det er velkendt, at R er et PID. Enhederne ± 1 er de eneste enheder i R . Normen er bestemt ved $N(a + bi\sqrt{2}) = a^2 + 2b^2$. Ligningen kan skrives $y^2 + 2 = x^3$, altså $N(y + i\sqrt{2}) = x^3$. I R kan vi faktorisere:

$$(y + i\sqrt{2})(y - i\sqrt{2}) = y^2 + 2 = x^3, \quad (10.9.2)$$

og vi sammenligner primopløsningerne af ligningens to sider. De to parenteser på venstresiden er primiske. Antag nemlig, at δ er divisor i begge tallene $y \pm i\sqrt{2}$. Da er δ divisor i differensen $2i\sqrt{2}$, og heraf følger, at normen af δ er divisor i normen af $2i\sqrt{2}$, altså at $N(\delta)$ er divisor i 8. På den anden side var δ divisor i $y + i\sqrt{2}$, og heraf følger, at normen af δ er divisor i normen af $y + i\sqrt{2}$. Den sidste norm er, ifølge ligningen (10.9.2), lig med x^3 . Altså er $N(\delta)$ divisor både i 8 og i det ulige tal x^3 . Følgelig er $N(\delta) = 1$. Altså er $\delta = \pm 1$ en enhed i R . Derfor er de to parenteser primiske.

I ligningen (10.9.2) er højresiden en 3' die potens. Af entydigheden af primopløsningerne følger derfor, at hver af de to parenteser er en 3' die potens i R . Specielt er $y + i\sqrt{2}$ en tredie potens. Med tal $u, v \in \mathbb{Z}$ har vi altså en ligning,

$$y + i\sqrt{2} = (u + vi\sqrt{2})^3.$$

Brug binomialformlen på ligningens højreside, og sammenlign koefficienterne til 1 og til $i\sqrt{2}$ på ligningens to sider. Det giver to ligninger,

$$y = u^3 - 6uv^2 = u(u^2 - 6v^2), \quad \text{og} \quad 1 = -2v^3 + 3u^2v = v(3u^2 - 2v^2).$$

Af ligningen $1 = v(3u^2 - 2v^2)$ i \mathbb{Z} følger, at begge faktorer må være ± 1 . Først fås altså $v = \pm 1$, og dernæst $3u^2 - 2 = \pm 1$. Her er $3u^2 - 2 = -1$ udelukket, og følgelig er $v = +1$ og $3u^2 - 2 = 1$, dvs $u = \pm 1$. Nu fås $y = \pm(1 - 6)$, altså $y = \pm 5$. Da $y \geq 0$, følger det, at $y = 5$, og så er $x^3 = 5^2 + 2$, dvs $x = 3$, som påstået.

Beviset for (b) er tilsvarende, men udnytter Gauss's talring $\mathbb{Z}[i]$. Også $\mathbb{Z}[i]$ er som bekendt i PID, med enhederne $\{\pm 1, \pm i\}$. I $\mathbb{Z}[i]$ er tallet 2 specielt: Det har primopløsningen $2 = (1+i)(1-i) = (-i)(1+i)^2$, og det er enheden $-i$, gange kvadratet på primelementet $1+i$. Ligningen kan skrives,

$$(y + 2i)(y - 2i) = y^2 + 4 = x^3. \quad (10.9.3)$$

De to faktorer på venstresiden er konjugerede. En fælles divisor for de to faktorer må også være divisor i differensen, dvs i 2^2i ; en fælles divisor må altså være en potens af $1 + i$ (med eksponent højst 4). Det følger nu, at det eneste primelement (bortset fra associering), der kan være divisor i begge faktorer, er $1 + i$, og $1 + i$ forekommer med samme eksponent i primopløsningen af de to faktorer.

Da højresiden er et tredie potens følger det, at bortset fra en enhed er begge faktorer på venstresiden trediepotenser. Da gruppen af enheder har orden 4, primisk med 3, er hver enhed en tredie potens (det checkes naturligvis også let direkte for hver af de 4 enheder). Derfor er hver faktor på venstresiden en trediepotens. Der findes altså en ligning, med $u, v \in \mathbb{Z}$,

$$y + 2i = (u + iv)^3.$$

Sammenligning af koefficienterne til 1 og til i giver:

$$y = u^3 - 3uv^2 = u(u^2 - 3v^2), \quad 2 = 3u^2v - v^3 = (3u^2 - v^2)v.$$

Entydighed af (sædvanlig) primopløsning giver, i den sidste ligning, at begge faktorer på højresiden er ± 1 eller ± 2 .

Hvis $v = \pm 1$, må den anden faktor være ± 2 , dvs $3u^2 - 1 = \pm 2$; heraf fås $u^2 = 1$ (idet $3u^2 = -1$ kan forkastes). Og så er $y = \pm(1 - 3)$, dvs $y = 2$ og $(x, y) = (2, 2)$.

Hvis $v = \pm 2$, må den anden faktor være ± 1 , dvs $3u^2 - 4 = \pm 1$; heraf fås $u^2 = 1$ (idet $3u^2 = 5$ kan forkastes). Og så er $y = \pm(1 - 12)$, dvs $y = 11$ og $(x, y) = (5, 11)$. \square

(10.10). Betragt en kvadratisk talring $\mathbb{Z}[\xi]$, hvor det irrationale tal ξ er rod i andengrads-polynomiet $X^2 + bX + c$ med hele koefficienter b, c ; antagelsen om at ξ er irrational, er ækvivalent med at diskriminanten $D := b^2 - 4c$ ikke er et kvadrat. Lad videre p være et (sædvanligt) primtal.

Som bekendt gælder da, at p er reducibel i $\mathbb{Z}[\xi]$, hvis og kun følgende diofantiske ligning har løsninger:

$$x^2 - bxy + cy^2 = \pm p, \quad (10.10.1)$$

og p er ikke et primelement, hvis og kun hvis følgende kongruens har løsninger:

$$z^2 - bz + c \equiv 0 \pmod{p}. \quad (10.10.2)$$

Den velkendte konsekvens er, at hvis ligningen har løsninger, så har kongruensen løsninger, og hvis ringen er UFD, så gælder „hvis og kun hvis“.

Det er let at undersøge kongruensen: Hvis $p = 2$ har kongruensen løsninger, hvis og kun hvis b eller c er lige. Antag, at p er ulige. Så er 2 invertibel i \mathbb{F}_p ; modulo p kan vi derfor omskrive kongruensen til følgende ligning i \mathbb{F}_p :

$$\left(z - \frac{b}{2}\right)^2 - \left(\frac{b}{2}\right)^2 + c = 0, \quad \text{eller} \quad (2z - b)^2 = D.$$

I \mathbb{F}_p har den sidste ligning øjensynlig én løsning, hvis $p \mid D$. Hvis $p \nmid D$, har den sidste ligning, og altså kongruensen (10.10.2), løsninger, hvis og kun hvis $\left(\frac{D}{p}\right) = 1$.

Sætning. Antag, at den kvadratisk talring $\mathbb{Z}[\xi]$ er et UFD. Da har den diofantiske ligning (10.10.1) med et ulige primtal p løsninger, hvis og kun hvis $p \mid D$ eller $\left(\frac{D}{p}\right)=1$. Den sidste betingelse er opfyldt, hvis og kun hvis $\left(\frac{D}{p}\right) = 1$, og specielt gælder, at eventuel løsbare af ligningen kun afhænger af restklassen af p modulo D .

Bevis. Den første del af påstanden er vist ovenfor, den sidste del følger umiddelbart af Reciprocitetssætningen. \square

(10.11) Bemærkning. Løsninger (x, y) til ligningen $x^2 - bxy + cy^2 = \pm p$ svarer til fremstillinger $p = \pm\pi\pi'$, hvor $\pi = x + y\xi$. Da p er et primtal, må en sådan fremstilling nødvendigvis være en primopløsning i $\mathbb{Z}[\xi]$ af tallet p . Ligningen har altså i almindelighed flere løsninger, svarende til at man i primopløsningen kan ombytte π og π' og multiplicere π med en enhed (og π' med den konjugerede enhed) i $\mathbb{Z}[\xi]$. Enhederne i $\mathbb{Z}[\xi]$ bestemmes som bekendt ved at løse den diofantiske ligning,

$$u^2 - buv + cv^2 = \pm 1; \quad (10.11.1)$$

heltalsløsninger (u, v) svarer til enheder $\varepsilon = u + v\xi \in \mathbb{Z}[\xi]$.

Ligningen (10.10.1) er i en vis forstand to ligninger, nemlig én ligning, hvor højresiden er $+p$ og én, hvor højresiden er $-p$; at (10.10.1) gælder, betyder at en af disse to ligninger er opfyldt. Tilsvarende svarer (10.11.1) til to ligninger.

I det *imaginære tilfælde*, dvs hvis $D < 0$, er $x^2 - bxy + cy^2 = N(x + y\xi)$ altid positiv. I dette tilfælde svarer (10.10.1) altså til ligningen med højresiden $+p$, og (10.11.1) er kun interessant med højresiden $+1$. Yderligere er der kun 9 værdier af diskriminanten D for hvilke talringen $\mathbb{Z}[\xi]$ er et UFD, nemlig følgende:

$$-3, -4, -7, -8, -11, -19, -43, -67, -163,$$

og det er altså kun for disse 9 værdier af D , at sætningen kan anvendes. For $D = -3$ består enhederne af de 6. enhedsrødder, for $D = -4$ er det de 4. enhedsrødder, og for $D < -4$ er der kun de trivielle enhedsrødder ± 1 .

Fx følger det, svarende til $D = -8$, at de ulige primtal af formen $p = x^2 + 2y^2$ netop er de primtal p , for hvilke $\left(\frac{p}{8}\right) = 1$, dvs at p er kongruent med 1 eller 3 modulo 8.

Og svarende til $D = -19$ følger det: primtallene af formen $p = x^2 - xy + 5y^2$ er netop primtallene p for hvilke $\left(\frac{p}{19}\right) = 1$ (samt $19 = 1^2 - 1 \cdot 2 + 5 \cdot 2^2$).

I det *reelle tilfælde*, altså hvis $D > 0$, er det mere kompliceret: Af de to ligninger i (10.10.1) kan den ene, eller den anden, eller begge, være opfyldt. Ligningen (10.11.1), til bestemmelse af enhederne i $\mathbb{Z}[\xi]$, kaldes *Pell's ligning*. Med højresiden $+1$ er det den *egentlige Pell'ske ligning*; med højresiden -1 kaldes ligningen også den *ikke-Pell'ske ligning*. Man kan vise, at den egentlige Pell'ske ligning altid har uendelig mange løsninger og at den ikke-Pell'ske ligning har enten ingen eller uendelig mange løsninger.

Hvis den ikke-Pell'ske ligning, dvs (10.11.1) med højresiden -1 , har løsninger, så gælder, at hvis en af ligningerne i (10.11.1) har løsninger, så har de begge løsninger. Hvis derimod

den ikke-Pell'ske ligning ikke har løsninger, så er det højst en af ligningerne i (10.10.1), der kan løses.

Man ved ikke, om der er uendelig mange positive værdier af D for hvilke ringen $\mathbb{Z}[\xi]$ er UFD. Det er ikke svært at vise, at hvis $\mathbb{Z}[\xi]$ er et UFD, så må D være kvadratfri som diskriminant. De første kvadratfri diskriminanter er følgende:

$$5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 40, 41, 44, 53, 56, 57, 60, 61, \dots$$

og af dem er det kun talringene svarende til $D = 40$ og $D = 60$, der ikke er UFD.

Fx ses, svarende til $D = 8$, at den ikke-Pell'ske ligning $x^2 - 2y^2 = -1$ har løsninger, fx $(x, y) = (1, 1)$. Heraf følger, at de ulige primtal p , der kan skrives på formen $p = x^2 - 2y^2$ netop er de primtal p , for hvilke $\left(\frac{p}{8}\right) = 1$, dvs at $p \equiv \pm 1 \pmod{8}$, og det er de samme primtal, der kan skrives på formen $p = -x^2 + 2y^2$.

Og svarende til $D = 12$ fås: Den ikke-Pell'ske ligning $x^2 - 3y^2 = -1$ har ingen løsninger. En af ligningeren $x^2 - 3y^2 = \pm p$ (og ikke begge) har løsninger, hvis og kun hvis $\left(\frac{p}{12}\right) = 1$ (eller $p = 2, 3$).

(10.12) Opgaver.

1. Bestem den manglende koordinat x i løsningen angivet i (10.5).
2. Marker på figuren i (10.6) punkterne svarende til primelementer associerede med π .
3. Vis for en enhed ε i $\mathbb{Z}[\rho]$, at ligningen $x^3 + y^3 = \varepsilon \zeta^3$ med $x, y, z \neq 0$ ikke har løsninger i $\mathbb{Z}[\rho]$.
4. Vis, for et primtal p , at $\left(\frac{p}{12}\right) = 1$, hvis og kun hvis $p \equiv \pm 1 \pmod{12}$. Bestem de første 8 primtal p , der kan skrives på formen $p = \pm(x^2 - 3y^2)$. Ser du mønsteret på fortegnet? Kan du bevise, at det forholder sig sådan?
5. Antag, at p er et primtal med $p \equiv 5 \pmod{8}$. Vis, at den kvadratiske talring $\mathbb{Z}[\sqrt{2p}]$ ikke er et UFD. [Vink: kongruensen $x^2 - 2p \equiv 0 \pmod{p}$ har løsninger (nemlig $x = 0$), men (regn modulo 8) ligningen $x^2 - 2py^2 = \pm p$ har ingen løsninger.]
6. Antag, at p og q er ulige primtal med $q \equiv 1 \pmod{4}$ og $\left(\frac{p}{q}\right) = -1$. Vis, at den kvadratiske talring $\mathbb{Z}[\sqrt{pq}]$ ikke er et UFD. [Vink: Se på ligningen $x^2 - pqy^2 = \pm p$ og på kongruensen $x^2 - pqy^2 \equiv \pm p$ modulo p og modulo q .]
7. *Bestem alle positive rationale løsninger (x, y) til ligningen $x^y = y^x$.