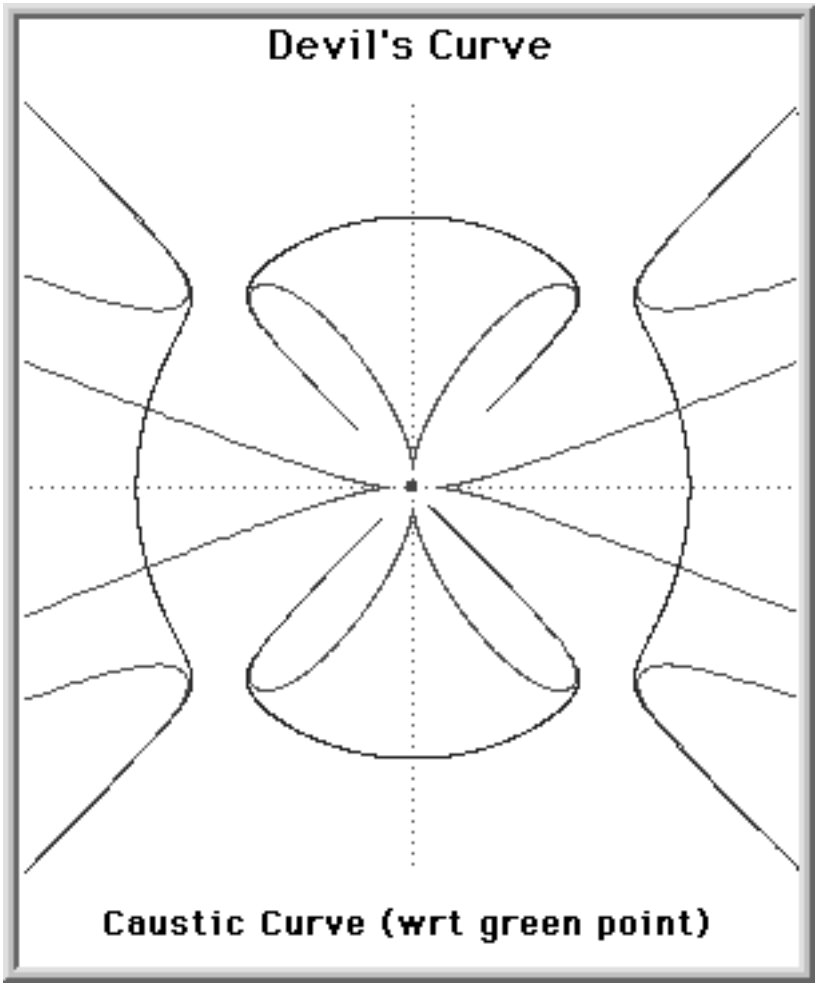
FAMØS

Fagblad for Aktuar, Matematik, -Økonomi og Statistik
12. årgang, nr. 3, marts 1999



FAMØS 12.3; marts 1999.
Fagblad for Aktuar-, Matematik-, Økonomi- og Statistikstuderende ved Københavns Universitet.

Deadline for næste nummer:
Torsdag den 29. april 1999

Indlæg modtages gerne og kan sendes til `famos@math.ku.dk` (meget gerne skrevet i LaTeX eller LaTeX 2_ε), eller afleveres på Matematisk Afdelings sekretariat i E 103.

FAMØS er et internt fagblad.

Fagbladet FAMØS
c/o Institut for matematiske fag
Matematisk Afdeling
Universitetsparken 5
2100 København Ø

World Wide Web adresse:
`http://www.math.ku.dk/famos/`

Tryk: HCØ Tryk

Oplag: 700 stk.

ISSN 1395-2145

Indhold

Leder

Velkommen til endnu et nummer af FAMØS. Siden sidst har fakultetet gennemført omfattende besparelser, men vi er her heldigvis stadig. Effekten af besparelserne bliver særdeles synlige i undervisningen. På Mat 1 er det fra efteråret slut med at have 4 øvelsestimer om ugen, og et par af gymnasielærerne udskiftes med fastansatte. På firepunkters kurserne på Matematik 2 og 3, bliver der fremover en fællestime med opgavegennemgang, og kun 2 almindelige øvelsestimer, derudover vil tre af de små Matematik 3 kurser (3AG, 3RE og 3NA) fremover kun køre hvert andet år.

En gruppe studerende på fakultet planlægger en demonstration 23. marts for at gøre opmærksom på, at besparelserne har ramt undervisningen særdeles hårdt. Der er allerede dukket plakater op om planerne, og der skal nok komme flere, så hvis du synes det er for galt at din undervisning bliver beskåret, så tag aktivt del i forberedelserne og/eller selve demonstrationen.

Studienævnet har afsluttet arbejdet med en ny studieordning for kandidatuddannelsen. Af nye ting er f.eks. et mere fleksibelt breddekrav, der betyder at man ikke længere nødvendigvis skal have Matematik 3AL, 3AN og 3GE. Endvidere skal der fremover gives en formel karakter for fagprojekter, og man skal have en 13-skala karakter i et antal andendelskurser svarende til mindst 8 punkter. Studieordningen ventes at træde i kraft 1. september, så hvis du er/bliver indskrevet på kandidatuddannelsen inden denne dato, gælder disse regler ikke umiddelbart for dig, men der er selvfølgelig overgangsregler.

Vores tegner er blevet færdig med sit studium, og derfor mangler vi hårdt en ny person til at lave tegninger til FAMØS. Hvis du kan tegne, så meld dig til redaktionen pr. e-post `famos@math.ku.dk`, hvis du selv har nogle ideer vil det være godt, men ellers sker det at andre i redaktionen får en idé til en tegning.[1] Almindelige redaktionsmedlemmer kan vi selvfølgelig også bruge. Lad være med at holde dig tilbage fordi du ikke tror, du kan særlig meget matematik, for det første kan du sikkert mere end du tror, og for det andet skal bladet også gerne være værd at læse for førsteårsstuderede. Det er heller ikke noget krav, at du er en stor LaTeX-haj, vi skal nok lære dig det du har brug for.

Rettelse: I annoncen fra IFF i sidste nummer, var der en e-post adresse på formanden Gyrd Foss, desværre var denne adresse forældet, den korrekte adresse er `gef@fak.hum.ku.dk`.

[1] Den første idé er faktisk allerede klar.

Med lov skal land bygges

Interview med Susan Rasmussen, der studerer jura. Interviewet er foretaget af Jens Barslund Mikkelsen til brug i „Studenterhåndbogen 1999“ udgivet af Forenede Studenterråd. FAMØS *trykker interviewet efter tilladelse fra Jens Barslund Mikkelsen og Susan Rasmussen som led i en artikelserie om, hvordan det er at læse på andre studier end matematikstudierne.*

Det er en fagligt engageret rus, man har over for sig, når man taler med Susan. Hun har fra studiestart være aktiv i Forenede Jurister, der er de jurastuderendes fag- og studenterpolitiske organisation.

Det endte med at blive jura

På spørgsmålet om hvorfor det blev jura, at Susan valgte som sit studium, svarer hun:

– Jeg havde en masse forskellige uddannelser, som jeg syntes så interessante ud. F.eks. var religionsvidenskab, litteraturvidenskab og statskundskab på tale, men jeg kunne ikke forestille mig i de jobs, som man kunne få med de uddannelser (måske lige undtaget statskundskab). Men så faldt valget på jura – ikke fordi jeg har planer om at skulle ud og sidde på et fint kontor med næsen begravet i Karnovs Lovsamling – fordi jeg tror, at jura kan give mig en ballast, jeg kan bruge i f.eks. socialt arbejde, hvilket interesserer mig. Jeg har gennem de sidste fem år været beskæftiget med ung til ung formidling som sexualist; jeg tog ud og talte med unge om følelser og kærlighedslivet, sex og sexuelle minoritetsgrupper. Derigennem har jeg mødt flere socialt belastede unge, hvilket har vakt min interesse for unges vilkår. Det her kommer nemt til at lyde som om, jeg vil bruge mit jurastudium til at redde verden – det er mit indtryk, at nogen læser jura for det – men sådan er det ikke. Jeg tror på, at jurastudiet kan give mig nogle kvalifikationer til at beskæftige mig med unges vilkår, som jeg ikke kan få nogen andre steder.

Men hvad er det for kvalifikationer, du får gennem jurastudiet?

– I bund og grund er det at læse jura at lære at fortolke love og regler, men det er også en viden om, hvordan man kan ændre love og regler. Jura er at lære en metode, en måde at tænke på. Vi har f.eks. nogle manuduktionstimer, hvor en sag bliver gennemgået set udelukkende med loven som baggrund. Det kan godt være lidt frustrerende, for der er mange andre aspekter end loven, der spiller ind på en sag. F.eks. er det ikke meningen, at man skal inddrage politiske aspekter, men mange gange er det oplagt at gøre det. At man personligt synes, at lovens ånd er forkert eller direkte imod éns ideologiske overbevisning (abortlovgivning er altid et godt diskussionsemne), kan jo ikke ændre på, hvordan en sag skal afgøres.

Det sociale er op til én selv

Susan har også nogle bemærkninger til studiemiljøet på jura:

– Første studieår har man undervisning 8–12, med manuduktion de to første timer (pensumgennemgang) og forelæsninger de to sidste. Forelæsningerne tager ofte udgangspunkt i sager, som alle har hørt om, men måske ikke rigtigt forstået, f.eks. tamilsagen, det er ret spændende. Manuduktion er holdundervisning og minder på den måde om gymnasiets undervisning. Det er også i manuduktionen, at der er mulighed for to-vejskommunikation mellem studerende og underviser. Det står i skarp kontrast til forelæsningerne, der udpræget er en-vejskommunikation: én forelæser og mellem 150 og 300 studerende. Til sådanne forelæsninger kan man godt savne lidt bedre plads, når man har været så uheldig at komme i sidste øjeblik og se sig henvist til den absolut sidste ledige plads: vindueskarmen.

– Lokalefaciliteterne på jura lader noget tilbage at ønske, og der har flere gange været påtaler fra arbejdstilsynet – vi ved ikke, om der sker nogle forbedringer her de kommende år. Hvis man ønsker social omgang med medstuderende er fredagsbarer og Jurahuset et godt sted at starte. Fredagsbarene arrangeres på skift af de 20 førsteårshold og er altid velbesøgte. Jurahuset indeholder Juridisk Laboratorium, der har computere, kopirum, søgebaser, skriverum, gruppelokaler, læsesale og frem for alt et veludstyret forskningsbibliotek.

– Man skal ikke forvente sig for meget af det sociale engagement efter det første års tid, fordi folk får andre ting at lave. Det er meget traditionsrigt at læse jura; f.eks. er der organisationen Juridisk Diskussionsklub, der er en gammel diskussionsklub, der også arrangerer ture til advokatkontorer og fester, bl.a. en årsfest, hvor de lejer Københavns Universitets festsal. Det er en gallamiddag.

Findes juridisk forskning?

Da jeg spørger Susan om juras ry for at være mere skoleagtig end andre universitetsuddannelser, bliver smilet lidt stift, inden hun svarer:

– Udadtil er jura ikke så forskningsbaseret som f.eks. fysik (vi mangler mænd i hvide kitler), og uddannelsen er da også overvejende en indføring i en særlig måde at tænke på, men der *er* juridisk forskning, f.eks. er regulering af „nye“ områder som regulering af internet et forskningsområde. Der er da også på det seneste blevet oprettet flere ph.d.-pladser på jura, men jurister får fortrinsvis beskæftigelse uden for universitetet.

Studenterpolitik

Susan har kort tid efter studiestart kastet sig over studenterpolitik.

– Jeg har gennem studenterpolitik fået mulighed for at få bedre socialt netværk, møde ældre studerende samt studerende fra alle mulige fag. Gennem studenterpolitik kan man opleve universitetsmiljøet fra en anden side. Her kan man være med til at påvirke sit eget studium i den retning, man ønsker, samt være med til at sikre og forbedre studievilkår.

Opgaveløsninger

Rasmus Borup Hansen

Opgave 1

Da Borpritzsky og Kowansky skal være de eneste medlemer af en af grupperne, må Rinturbar og Ruparov være i samme gruppe. Vulonlar må da være i en tredje gruppe, som også indeholder enten Numismatov eller Johannow. Den af Numismatov og Juhannow, der ikke er i gruppe med Vulonlar må så være i samme gruppe som Rinturbar og Ruparov, idet der skal være tre forskere i Rinturbars gruppe.

Opgave 2

Opgaven var at finde ud af, hvor stor en andel (procentdel) af alle heltal (som vi antager skrives i 10-talssystemet), som indeholder mindst ét 3-tal.

Hvis vi kun betrager heltal med n cifre, lader vi r_n betegne andelen af disse, der indeholder mindst ét 3-tal. Nu er

$$r_{n+1} = \frac{10^n + 9r_n 10^n}{10^{n+1}} = \frac{1 + 9r_n}{10},$$

hvoraf ses, at $r_n \to \infty$ for $n \to \infty$. Altså må svaret være 100%.

Opgave 3

Da produktet af børnenes aldre er 36, må de være (1,1,36), (1,2,18), (1,3,12), (1,4,9), (1,6,6), (2,2,9), (2,3,6) eller (3,3,4). Da x stadig er i tvivl efter at have fået oplyst summen af deres aldre, må det være (2,2,9) eller (1,6,6). Her kan vi udelukke den sidste mulighed, idet vi får oplyst, at der er et af børnene der er den ældste. Altså må børnenes aldre være 2 år, 2 år og 9 år.

Opgave 4

Der var nogle trykfejl i opgaven, så vi gentager den her. Lad $x_1 = x$, og lad $x_{i+1} = x^{x_i}$. Idet $\lim_{i\to\infty} x_i = 2$, skal vi finde x.

Vi har, at

$$2 = \lim_{i\to\infty} x_i = \lim_{i\to\infty} x_{i+1} = \lim_{i\to\infty} x^{x_i} = x^{\lim_{i\to\infty} x_i} = x^2,$$

hvorfor $x = \sqrt{2}$.

Opgave 5

Idet den gennemsnitlige ventetid på succes er lig den reciprokke successandsynlighed, kan vi forvente at skulle spise

$$1 + \frac{4}{3} + \frac{4}{2} + \frac{4}{1} = \frac{25}{3}$$

pakker cornflakes.

Opgave 6

Det ses nemt, at svaret er 42.

Opgaver

Opgave 1

Et kubisk stykke ost, er blevet delt i 27 mindre kuber (så det ligner en Rubik's terning). En mus begynder at spise osten fra et af hjørnerne, sådan at den spiser en hel af de små kuber, hvorefter den fortsætter med en af de tilstødende små kuber. Er det muligt for musen at slutte med at spise den (fra starten) midterste kube?

De to næste opgaver stammer fra dette års Georg Mohr konkurrence.

Opgave 2

En fisker har fanget et antal fisk. De tre tungeste udgør tilsammen 35% af fangstens samlede vægt. Dem sælger han. Herefter udgør de tre letteste tilsammen 5/13 af vægten af resten.

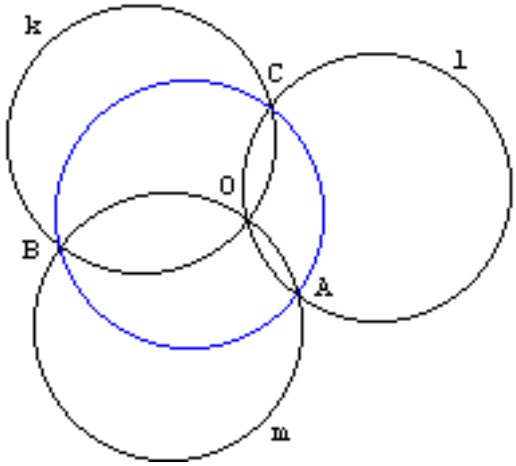
Hvor mange fisk fangede han?

Opgave 3

Findes der et tal hvis cifre er lutter 1-taller, og som 1999 går op i?

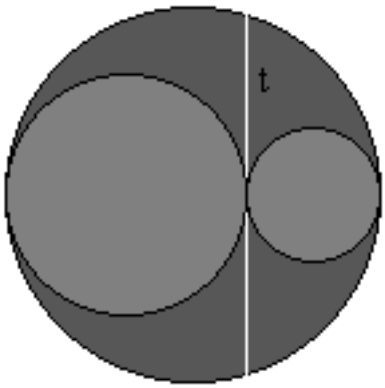
Opgave 4

Der er givet tre cirkler med radius r der alle går gennem punktet O. Disse tre cirkler skærer hinanden parvis i tre punkter A, B og C. Bevis at cirklen gennem A, B og C har radius r.



Opgave 5

To små cirkler ligger udenfor hinanden, men inden i en tredje større cirkel, sådan at alle tre tangerer hinanden parvis. Deres centre ligger på en ret linie. Lad r være radius i den store cirkel, og lad t være længden af den del af de to små cirklers fælles tangent der ligger inden i den store cirkel. Find arealet af det område der ligger inden i den store cirkel men uden for de små cirkler.



Om kongruenstal

Ian Kiming

Indledning

Lad d være et naturligt tal. Et klassisk, diofantisk problem - endda taget op til overvejelse af Diofant selv - består i at spørge efter rationale tal α, β, γ, hvis kvadrater er på hinanden følgende tal i en aritmetisk progression med modulus d; med andre ord: Der spørges efter rationale tal α, β, γ således, at:

$$(*) \qquad \gamma^2 - \beta^2 = \beta^2 - \alpha^2 = d \ .$$

Hvis $(*)$ har en løsning i rationale tal α, β, γ, kaldes d klassisk for et 'kongruenstal'. Mens forfattere i oldtiden og middelalderen var tilfredse med at kunne angive *eksempler* på kongruenstal (f.eks. (Fibonacci) $d = 5$, $\alpha = 31/12$, $\beta = 41/12$, $\gamma = 49/12$), må opgaven set fra et moderne synspunkt - såfremt problemet da overhovedet skal tages alvorligt - være at *karakterisere* kongruenstallene eller i det mindste at spørge efter en *algoritme*, der for givet d afgør, om d er et kongruenstal. Bemærk, at det på ingensomhelst måde er trivielt klart, at en sådan algoritme eksisterer: Hvis et givet d skal vises *ikke* at være et kongruenstal, skal - a priori - uendeligt mange muligheder for (α, β, γ) udelukkes.

Vi vil se, at det er muligt at give et partielt svar på disse spørgsmål og, at eksistensen af en fuld algoritme som ovenfor tilsyneladende hænger på et af de store, centrale, uløste problemer i moderne talteori, nemlig den såkaldte Birch- og Swinnerton-Dyer formodning (se nedenfor).

Øvelse 1: Vis, at d er et kongruenstal, hvis og kun hvis d er arealet af en retvinklet trekant med *rationale* kantlængder.

Lad os nu bemærke, at vi øjensynligt uden væsentlige indskrænkninger kan antage, at d er kvadratfrit. Af pladshensyn vil vi i denne artikel yderligere antage, at d er ulige; tilfældet, hvor d er lige kan behandles helt analogt. Altså:

$$d \in \mathbb{N}, \text{ kvadratfrit og ulige.}$$

Vi vil diskutere forskellige aspekter af følgende sætning af J. B. Tunnell (*Invent. math.* **72** (1983), 323-334):

Sætning: Definer:

$$c_d := \#\{(x,y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 32z^2 = d\}$$

$$-\tfrac{1}{2} \cdot \#\{(x,y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 8z^2 = d\}.$$

Da gælder:

$$c_d \neq 0 \Rightarrow d \text{ er ikke kongruenstal.}$$

Hvis Birch-Swinnerton-Dyer formodningen gælder, kan denne implikation vendes om.

Tunnell's sætning har diverse klassiske resultater om kongruenstalproblemet som umiddelbare konsekvenser og viser, at visse klassiske formodninger kan opnås som følger af Birch-Swinnerton-Dyer formodningen, men vi kommer af pladshensyn ikke ind på dette.

Interessen for Tunnells sætning i sammenhæng med det måske udfra en umiddelbar betragtning relativt tilfældigt udseende problem $(*)$ koncentrerer sig - bortset fra den historiske interesse - i følgende 2 punkter: *(i)* Man beviser i den matematiske logik, at der ikke findes nogen generel algoritme til afgørelse af løsbarhed i *hele* tal til systemer af diofantiske ligninger (i.e. systemer af polynomiumsligninger i flere variable med heltallige koefficienter). Men det tilsvarende spørgsmål angående mulighederne for algoritmisk afgørelse af løsbarhed i *rationale* tal er endnu ikke afklaret. Selv specielle spørgsmål af denne type, der kan vise hvilke problemer, man er oppe imod, er derfor af en vis interesse. *(ii)* Som vi vil se nedenfor lurer der under overfladen af det 'uskyldigt' udseende problem $(*)$ en dyb, massiv struktur, som kun den moderne matematik er i stand til at håndtere. Og det er vel netop matematikkens egentlige opgave at afdække sådanne dybtliggende og a priori skjulte strukturer.

Omformulering

Lemma 1: $(*)$ har en løsning $(\alpha, \beta, \gamma) \in \mathbb{Q}^3$, hvis og kun hvis ligningen

$$y^2 = x^3 - d^2x$$

har en løsning i rationale tal x, y med $y \neq 0$.
Bevis: $\Rightarrow$: Sæt $x := (\alpha+\beta)(\beta+\gamma)$, $y := (\alpha+\beta)(\alpha+\gamma)(\beta+\gamma)$ og udnyt, at $d = (\gamma+\beta)(\gamma-\beta) = (\beta+\alpha)(\beta-\alpha)$.
$\Leftarrow$: Sæt $\alpha := (x^2 - 2dx - d^2)/(2y)$, $\beta := (x^2+d^2)/(2y)$, $\gamma := (x^2+2dx-d^2)/(2y)$.

I denne og vel at mærke *kun* i denne artikel vil vi definere en *elliptisk kurve* E (over $\mathbb{Q}$) som en ligning af formen $y^2 = x^3 + ax^2 + bx + c$, hvor $a, b, c \in \mathbb{Z}$, og hvor polynomiet $x^3 + ax^2 + bx + c$ har 3 forskellige rødder. Vi skriver:

$$(**) \qquad E: \quad y^2 = x^3 + ax^2 + bx + c \ ,$$

og vi vil betegne den specielle elliptiske kurve, der forekommer i Lemma 1, med E_d, altså:

$$(***) \qquad E_d: \quad y^2 = x^3 - d^2x \ .$$

Løsninger til $(**)$ i rationale tal x, y kaldes *rationale punkter* på E; til disse løsninger tilføjes 'kunstigt' et ekstra 'punkt', som betegnes O, og man sætter:

$$E(\mathbb{Q}) := \{O\} \cup \{(x,y) \in \mathbb{Q}^2 \mid \ y^2 = x^3 + ax^2 + bx + c\}.$$

Formålet med tilføjelsen af det ekstra punkt O er, at man i teorien for elliptiske kurver viser, at $E(\mathbb{Q})$ har en naturlig struktur som abelsk gruppe, hvor O spiller rollen

som neutralelement. Kompositionen i denne abelske gruppe betegner vi simpelthen med '+'; den kan angives eksplicit: Haves eksempelvis 2 løsninger $P_i = (x_i, y_i) \in \mathbb{Q}^2$, $i = 1, 2$, til $(**)$ med $x_1 \neq x_2$, fås en 3'de løsning $P_3 = P_1 + P_2 = (x_3, y_3) \in \mathbb{Q}^2$, hvor $x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - a - x_1 - x_2$, $y_3 = -\left(\frac{y_1 - y_2}{x_1 - x_2}\right) x_3 - \left(\frac{y_2 x_1 - y_1 x_2}{x_1 - x_2}\right)$ (kan checkes direkte som øvelse). Et andet eksempel på kompositionen er: $(x_1, y_1) + (x_1, -y_1) = O$, altså $(x_1, -y_1) = -P_1$.

Hvad kan vi sige om strukturen af $E(\mathbb{Q})$? En grundlæggende sætning i teorien for elliptiske kurver er Mordell's sætning (1922), der udsiger, at gruppen $E(\mathbb{Q})$ er *endeligt frembragt*. Af struktursætningen for endeligt frembragte, abelske grupper kan vi da slutte, at

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r \ ,$$

hvor $r \in \mathbb{N}_0$, T er en *endelig*, abelsk gruppe, og T og r er entydigt bestemte ved E. Gruppen T kaldes E's gruppe af (rationale) torsionspunkter og betegnes $E_{\text{tors}}(\mathbb{Q})$; denne gruppe består altså netop af elementerne af *endelig* orden i $E(\mathbb{Q})$. Tallet r kaldes E's *rang*, og vi betegner det med $r(E)$.

Lad os nu specialisere til vores specielle kurver E_d: Kan vi angive nogle rationale punkter på E_d? Det er let: Vi har øjensynligt $(0,0), (d,0), (-d,0) \in E_d(\mathbb{Q})$. Som vi nævnte ovenfor, har vi $-P = (x, -y)$, for $P = (x, y) \in E_d(\mathbb{Q})$, og for disse punkter gælder følgelig $2 \cdot P \ (= P + P) \ = O$, hvis og kun hvis $P \in \{(0,0), (d,0), (-d,0)\}$. Naturligvis har vi også $2 \cdot O = O$, da O er neutralelement i $E_d(\mathbb{Q})$. Vi kan altså slutte, at $U := \{O, (0,0), (d,0), (-d,0)\}$ er undergruppen i $(E_d)_{\text{tors}}(\mathbb{Q})$ bestående af elementerne af orden 2 i $E_d(\mathbb{Q})$. Med blot en lille smule teori for elliptiske kurver kan man på relativ simpel vis slutte, at vi faktisk har $U = (E_d)_{\text{tors}}(\mathbb{Q})$. Vi antyder en mulig bevismetode i den næste øvelse.

Øvelse 2: Betragt tilfældet, hvor d er et primtal ℓ. Den såkaldte Nagell-Lutz sætning specialiseret til kurven E_ℓ udsiger, at hvis $P = (x, y) \in E_\ell(\mathbb{Q})$ er et torsionspunkt, da gælder $x, y \in \mathbb{Z}$, og enten $2 \cdot P = O$ eller $y \mid 2\ell^3$. Slut heraf, at vi for et torsionspunkt (x, y) må have $y = 0$.

Vi er nu i stand til at omformulere vores kongruenstalproblem.

Lemma 2: (d er et kongruenstal) $\Leftrightarrow \ r(E_d) > 0$.

Bevis: Ifølge Lemma 1 er d et kongruenstal, netop hvis der findes $(x, y) \in E_d(\mathbb{Q})$ med $y \neq 0$. Vi karakteriserede ovenfor torsionspunkter (altså punkter af endelig orden) $(x, y) \in E_d(\mathbb{Q})$ ved betingelsen $y = 0$. Altså er d et kongruenstal, netop hvis $E_d(\mathbb{Q})$ har et element af uendelig orden. Men dette er jo ækvivalent med betingelsen $r(E_d) > 0$.

L-rækker, spidsformer og mudularitet

Vi betragter igen den generelle elliptiske kurve $(**)$. Lad p være et primtal. Til parret (E, p) er knyttet et helt tal $a_p(E)$, der kommer til at spille en afgørende rolle i det følgende. Vi angiver definitionen af $a_p(E)$ 'for næsten alle p': Da ligningen $(**)$ har *heltallige* koefficienter, giver det mening at opfatte den som en ligning med koefficienter i det endelige legeme $\mathbb{F}_p$, i.e.: Vi opfatter a, b, c som liggende i

$\mathbb{Z}/\mathbb{Z}p = \mathbb{F}_p$. Man kan vise, at polynomiet $x^3 + ax^2 + bx + c \in \mathbb{F}_p[X]$ for alle pånær endeligt mange primtal p har 3 forskellige rødder (i en eller anden endelig udvidelse af $\mathbb{F}_p$); *antag*, at dette er tilfældet for det givne p; da defineres:

$$a_p(E) := p - \#\{(x,y) \in \mathbb{F}_p^2 \mid \ y^2 = x^3 + ax^2 + bx + c\} \ .$$

I de endeligt mange tilfælde, hvor 2 eller 3 af rødderne i $x^3 + ax^2 + bx + c$ over $\mathbb{F}_p$ falder sammen, har man også en definition af $a_p(E)$, men denne kan ikke mere forklares i elementære termer (hvilket vi derfor må undlade at gøre). Som vi snart skal se spiller følgen af tal $(a_2(E), a_3(E), a_5(E), a_7(E), a_{11}(E), \ldots)$ en fundamental rolle for strukturen af E, specielt for strukturen af $E(\mathbb{Q})$. Imidlertid rækker det ikke kun at kende endeligt mange af disse tal $a_p(E)$; vi må derfor finde en måde at 'pakke' den information, der ligger i hele rækken af $a_p(E)$'er, sammen i et nyt objekt. Dette nye objekt er E's såkaldte L-række. Der findes (uendeligt) mange andre strukturer i talteorien, der har L-rækker knyttet til sig. Det simpleste eksempel på en L-række er Riemann's zeta-funktion:

$$(\sharp) \qquad \zeta(s) := \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ primtal}} (1 - p^{-s})^{-1} \ ,$$

med sin udvidede version:

$$\Lambda(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) \ ,$$

hvor Γ er den sædvanlige gamma-funktion. Som bekendt konvergerer $(\sharp)$ absolut for $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$, og her definerer $\Lambda(s)$ en holomorf funktion af s. Denne kan fortsættes meromorft til hele den komplekse plan, hvor den har simple poler i 0 og 1 og tilfredsstiller funktionalligningen $\Lambda(s) = \Lambda(1-s)$.

Definitionen af L-rækken for E, $L(E,s)$, er analog:

$$(\sharp\sharp) \qquad L(E,s) := \prod_{p \text{ primtal}} \left(1 - a_p(E) \cdot p^{-s} + p^{1-2s}\right)^{-1} \ ,$$

og vi har også her en udvidet version:

$$\Lambda(E,s) := N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s) \ ,$$

hvor N_E er et vist naturligt tal knyttet til E, hvis definition vi ikke kommer ind på (N_E er E's såkaldte 'fører'). Benytter man Hasse-Weil-vurderingerne, der siger, at $\mid a_p(E) \mid < 2\sqrt{p}$, kan man slutte, at $(\sharp\sharp)$ konvergerer absolut for $s \in \mathbb{C}$, $\mathrm{Re}(s) > 2$ og definerer en holomorf funktion af s i dette område. I dette område kan vi så gange paranteserne i $(\sharp\sharp)$ ud, og finder under benyttelse af den geometriske række $(1-q)^{-1} = 1 + q + q^2 + \ldots$:

$$L(E,s) = \sum_{n=1}^{\infty} a_n(E) \cdot n^{-s} \ ,$$

hvor $a_1(E) := 1$, $a_{mn}(E) := a_m(E)a_n(E)$ for $(m,n) = 1$, $a_{p^2}(E) := a_p(E)^2 - p$, osv..

Kunne det måske være tilfældet, at $\Lambda(E,s)$ har en analytisk fortsættelse til hele den komplekse plan $s \in \mathbb{C}$, hvor den tilfredsstiller en funktionalligning analog til funktionalligningen for Riemann's zeta-funktion? Dette er et overordentligt meget mere kompliceret spørgsmål end det tilsvarende spørgsmål for Riemann's zeta-funktion, fordi svaret afhænger af, om E er 'modulær', - et begreb, som vi nu kort vil forklare: Lad $N \in \mathbb{N}$. En *spidsform af vægt* 2 *og niveau* N er en holomorf funktion f på 'den øvre halvplan' $\{\tau \in \mathbb{C} \mid \ \mathrm{Im}(\tau) > 0\}$ med følgende egenskaber: *(i)* $f(\tau) = (c\tau + d)^{-2} f\left(\frac{a\tau+b}{c\tau+d}\right)$ for alle $a,b,c,d \in \mathbb{Z}$ med $N \mid c$ og $ad - bc = 1$; *(ii)* $\exists \nu \in]0,2[$: $f(\tau) = O(\mathrm{Im}(\tau)^{-\nu})$ for $\mathrm{Im}(\tau) \to 0+$, uniformt m.h.t. $\mathrm{Re}(\tau)$. En sådan spidsform er et specielt eksempel på en *modulform* af vægt 2 og niveau N, - definitionen af en sådan er det samme som ovenstående bortset fra, at der kun forlanges $\nu > 0$ i betingelse *(ii)*. En spidsform f har en Fourier-udvikling:

$$f(\tau) = \sum_{n=1}^{\infty} a_n(f) \cdot e^{2\pi i n \tau} \ ,$$

hvor $a_n(f)$ er visse komplekse tal. Teorien for spidsformer er klassisk, og man kan 'let' (dvs. kun under brug af klassiske metoder, såsom kompleks analyse) vise eksempelvis følgende: Defineres:

$$\Lambda(f,s) := N^{s/2}(2\pi)^{-s}\Gamma(s) \sum_{n=1}^{\infty} a_n(f) \cdot n^{-s} \ ,$$

da konvergerer $\Lambda(f,s)$ absolut for $\mathrm{Re}(s) > 2$, har holomorf fortsættelse til hele $s \in \mathbb{C}$, og tilfredsstiller her funktionalligningen:

$$(\sharp\sharp\sharp) \qquad \Lambda(f,s) = -\Lambda(\hat{f}, 2-s) \ ,$$

hvor $\hat{f}(\tau) := N^{-1}\tau^{-2} f\left(\frac{-1}{N\tau}\right)$, som også er en spidsform af vægt 2 og niveau N.

Den elliptiske kurve E siges at være *modulær*, hvis der findes en spidsform f af vægt 2 og niveau N_E således, at $a_n(E) = a_n(f)$, $\forall n \in \mathbb{N}$. I så fald er øjensynligt $\Lambda(E,s) = \Lambda(f,s)$ for $\mathrm{Re}(s) > 2$. Af $(\sharp\sharp\sharp)$ følger da med lidt ekstra arbejde, hvor man viser, at der *i dette tilfælde* gælder $\hat{f} = \pm f$:

Sætning 1: Lad E være en modulær elliptisk kurve over $\mathbb{Q}$. Da kan $\Lambda(E,s)$ fortsættes holomorft til hele $s \in \mathbb{C}$, og tilfredsstiller her funtionalligningen:

$$\Lambda(E,s) = \sigma(E) \cdot \Lambda(E, 2-s) \ ,$$

med et vist (af E afhængigt) fortegn $\sigma(E) \in \{\pm 1\}$.

Den berømte *Taniyama-Shimura-formodning* siger, at enhver elliptisk kurve over $\mathbb{Q}$ er modulær. Som mange læsere måske vil vide, blev denne formodning bevist for en stor klasse af elliptiske kurver af Andrew Wiles i 1995. Ved en første konfrontation kan T.-S.-formodningen forekomme overordentligt mystisk: Tallene $a_p(E)$ har at gøre med antallet af løsninger modulo p til $(**)$; hvorfor i alverden skulle disse tal have noget med Fourierkoefficienterne af en periodisk holomorf funktion at gøre? *Noget* af mystikken forsvinder, hvis man ved, at en spidsform i virkeligheden er et betydeligt meget mere abstrakt (repræsentationsteoretisk, algebraisk-geometrisk)

objekt. Intuitivt kunne man sige, at den holomorfe funktion f ovenfor blot er en af ∞ mange af det virkelige objekts inkarnationer (de øvrige står i 1-1 korrespondance med mængden af primtal). Vi vil hermed sige, at den 'rigtige' spidsform er et langt mere struktureret objekt, end definitionen ovenfor lader ane, og at T.-S.-formodningen fra denne højere synsvinkel ganske vist stadig fremstår som en dyb, men langt mere naturlig og mindre overraskende formodning.

Angående T.-S.-formodningen er situationen i øjeblikket den, at man sandsynligvis kan forvente et bevis for formodningen uden indskrænkninger indenfor en overskuelig fremtid (5-10 år). Eksempelvis ved man nu (Wiles, Taylor-Wiles, Diamond-Kramer): *Antag, at polynomiet $x^3 + ax^2 + bx + c$ i $(**)$ har 3 forskellige rationale rødder. Da er E modulær.* Specielt kunne vi heraf slutte følgende om vores specielle kurver E_d:

Sætning 2: Kurven E_d er modulær.

At bruge Wiles' store sætning til at bevise sætning 2 er i virkeligheden et massivt teoretisk overkill; grunden er, at kurverne E_d tilhører en speciel klasse af elliptiske kurver, hvis teori er simplere end i det generelle tilfælde (men ikke simpel): Kurverne E_d er såkaldte CM-kurver (CM = 'Complex Multiplication'); det betyder groft sagt, at disse kurver har nogle ekstra, exceptionelle 'endomorfier': Et eksempel på, hvad der menes med dette, kan fås af følgende observation: Lad (x, y) være en løsning i komplekse tal til $(***)$; da er også $(-x, iy)$ en løsning. For CM-kurver - og altså specielt for kurverne E_d - kan modularitet bevises v.hj.a. mere klassiske teorier i algebraisk talteori og algebraisk geometri (for kendere af de finere dele af algebraisk talteori kan vi oplyse, at $\Lambda(E_d, s)$ kan udtrykkes via en vis grössen-karakter på det tilhørende CM-legeme $\mathbb{Q}(i)$).

Lad nu f_d betegne den spidsform af vægt 2 (og niveau N_{E_d}), som opfylder $a_n(E_d) = a_n(f_d)$, og hvis eksistens er sikret af sætning 2. Vi har altså: $\Lambda(E_d, s) = \Lambda(f_d, s)$ for $s \in \mathbb{C}$, og det giver mening at studere opførslen af $\Lambda(E_d, s)$ i (en omegn af) symmetripunktet $s = 1$ for $s \mapsto 2 - s$. Dette fører os naturligt til næste afsnit.

Birch- og Swinnerton-Dyer formodningen og Waldspurgers sætning

Antag, at kurven E er modulær. Vi kan da meningsfuldt tale om nulpunktsordenen af den holomorfe funktion $\Lambda(E, s)$ i punktet $s = 1$. Denne orden kaldes E's *analytiske rang*, og betegnes $r_{an}(E)$. Den svage form af Birch-Swinnerton-Dyer-formodningen siger:

Formodning (Birch-Swinnerton-Dyer, svag form): $r(E) = r_{an}(E)$.

Den stærke form af formodningen er den svage form + en præcis angivelse af værdien $\Lambda^{(r)}(E, 1)$, $r := r_{an}(E) = r(E)$, udtrykt ved visse fundamentale analytiske og algebraisk-aritmetiske invarianter knyttet til E. B.-Sw.-D.-formodningen er den næste store udfordring i teorien for elliptiske kurver efter, at Taniyama-Shimura-formodningen nu er faldet mere eller mindre på plads. Hvilke grunde har vi nu til at tro på B.-Sw.-D.-formodningen? Der kan nævnes 3 grunde, ordnet efter faldende vægt:

(1). Formodningen understøttes af et stort eksperimentelt datamateriale: Der findes algoritmer til bestemmelse af $r_{an}(E)$, og selvom der ikke kendes nogen algoritme til bestemmelse af $r(E)$, der *beviseligt* fungerer i ethvert tilfælde, så kan $r(E)$ alligevel bestemmes i mange tilfælde. Man kan således for mange kurver checke, om $r_{an}(E) = r(E)$, hvilket er blevet gjort (endda er den stærke form af formodningen blevet testet for mange kurver; i øvrigt kan det nævnes, at B.-Sw.-D.-formodningen faktisk opstod i slutningen af 1960'erne på grundlag af sådanne eksperimenter).
(2). Følgende sætning ('big theorem'):

Sætning 3 (V. Kolyvagin, 1990, se *Grothendieck Festschrift, vol. II*): Lad E være en modulær elliptisk kurve over $\mathbb{Q}$ og antag, at $r_{an}(E) \leq 1$. Da er $r_{an}(E) = r(E)$.

(3). B.-Sw.-D.-formodningen er et lille hjørne af et gigantisk, men uhyre kohærent formodningsnetværk (Beilinson-formodningerne), der forbinder algebraisk-aritmetiske egenskaber ved bestemte typer af talteoretiske objekter (så kaldte 'motiver') med den analytiske opførsel af tilknyttede L-funktioner i specielle punkter. Dette store formodningssystem generaliserer diverse helt klassiske sætninger eksempelvis om Riemann's zeta-funktion, men har på den anden side også ikke-klassiske konsekvenser, der i nogle tilfælde (som ved B.-Sw.-D.) kan bekræftes i det mindste partielt. Som minimum kan man derfor sige, at dette formodningssystem er en god arbejdshypotese.

Bemærk, at hvis vi kun interesserer os for nulpunktsordenen af $\Lambda(E,s)$ i $s = 1$, da kan vi ligeså godt diskutere nulpunktsordenen af (den meromorfe funktion) $L(E,s)$ i dette punkt, eftersom $\Lambda(E,s)$ kun adskiller sig fra $L(E,s)$ ved faktoren $(2\pi/\sqrt{N_E})^{-s}\Gamma(s)$. Af lemma 2 og sætning 3 kan vi da konkludere:
Lemma 3: $L(E_d,1) \neq 0 \Rightarrow$ (d er ikke kongruenstal). Hvis B.-Sw.-D.-formodningen gælder, kan denne implikation vendes om.

Et bevis for Tunnell's sætning fås derfor, hvis man viser:

$$(\flat) \qquad L(E_d,1) \neq 0 \;\Leftrightarrow\; c_d \neq 0\ .$$

Vi skitserer nu, hvordan man kan reducere beviset for ($\flat$) til en endelig mængde regning (det skitserede argument er lidt anderledes og bedre generaliserbart end argumentet i Tunnell's artikel) : Vi interesserer os for værdierne $L(E_d,1)$ hørende til familien af kurver $(E_d)_{d \text{ ulige, kvadratfri}}$; disse værdier er $L(f_d,1)$, hvor $(f_d)_{d \text{ ulige, kvadratfri}}$ er familien af til (E_d) hørende spidsformer. Den afgørende pointe er nu, at f_d'erne alle fremgår af 'grundformen' f_1 hørende til E_1 ved en proces, der teknisk kaldes 'twist': Det præcise udsagn er, at der for Fourierkoefficienterne af f_d og f_1 gælder følgende sammenhæng:

$$a_n(f_d) = \left(\frac{d}{n}\right) a_n(f_1)\ ,\ \text{hvis } (n,2d) = 1,$$

hvor $\left(\frac{d}{\cdot}\right)$ er det sædvanlige Legendre-symbol, altså (eksempelvis) for primtal ℓ, $(d,\ell) = 1$: $\left(\frac{d}{\ell}\right) = 1$, hvis d er et kvadrat i $\mathbb{F}_\ell$, og ellers $= -1$. For en familie af spidsformer, der fremgår af en grundform ved sådanne 'twists', gælder der - under bestemte tekniske forudsætninger, der er opfyldte i det foreliggende tilfælde - en dyb og ret beset temmelig mystisk sætning af Waldspurger ('big theorem', se *J. Math.*

pures et appl. **60** (1981), 375-484), som vi ikke formulerer i sin fulde generalitet men kun i sin specialisering til den foreliggende familie (f_d): Waldspurger's sætning siger her, at værdierne $L(f_d, 1)$ kan udtrykkes ved $L(f_1, 1)$ og Fourierkoefficienterne i en spidsform af vægt $3/2$ (se (♭♭♭) nedenfor for det præcise udsagn); men hvad er nu en spidsform af vægt $3/2$? Man kan *næsten* gætte det af definitionerne i foregående afsnit: En *spidsform af vægt* $3/2$ *og niveau* N er en holomorf funktion g på den øvre halvplan $\{\tau \in \mathbb{C} \mid \ \mathrm{Im}(\tau) > 0\}$ med:
(i) $\exists \nu \in]0, 3/2[$: $g(\tau) = O(\mathrm{Im}(\tau)^{-\nu})$ for $\mathrm{Im}(\tau) \to 0+$, uniformt m.h.t. $\mathrm{Re}(\tau)$; *(ii)* $g(\tau) = \chi(c,d)(c\tau + d)^{-3/2} g\left(\frac{a\tau+b}{c\tau+d}\right)$ for alle $a, b, c, d \in \mathbb{Z}$ med $N \mid c$ og $ad - bc = 1$, hvor der tages hovedværdien af kvadratroden, og hvor $\chi(c,d)$ er et vist fortegn $\in \{\pm 1, \pm i\}$, hvis præcise afhængighed af c, d er irrelevant i denne sammenhæng. En sådan funktion g har også en Fourierudvikling:

$$g(\tau) = \sum_{n=1}^{\infty} b_n(g) \cdot e^{2\pi i n \tau} \ . \tag{♭♭}$$

Det præcise udsagn fra Waldspurger's sætning specialiseret til familien (f_d) er: Der findes en spidsform g af vægt $3/2$ og niveau 128 - lad os sige med Fourierudvikling (♭♭) - således, at:

$$b_1(g)^2 L(f_d, 1)\sqrt{d} = b_d(g)^2 L(f_1, 1) \ ; \tag{♭♭♭}$$

formen g er ikke entydigt bestemt ved kravet (♭♭♭), men (♭♭♭) er opfyldt, hvis g for ethvert ulige primtal p er egenform for en vis operator (kaldet en Hecke-operator) T_{p^2} med tilhørende egenværdier $a_p(f_1)$, hvor T_{p^2} er en lineær operator virkende på det komplekse vektorrum $S_{3/2}(128)$ af spidsformer af vægt $3/2$ og niveau 128. Nu er rummet $S_{3/2}(128)$ *endelig-dimensionalt* (faktisk er $\dim S_{3/2}(128) = 3$), og der findes algoritmer til konstruktion af en basis for dette rum, hvorved vi mener, at Fourierkoefficienterne for en basis kan konstrueres op til en hvilken som helst grænse, der ønskes. Videre kan virkningerne af operatorerne T_{p^2} angives eksplicit som virkninger på følgerne af Fourierkoefficienter for en basis. Af den nævnte endelig-dimensionalitet kan man trække den konsekvens, at det krav, der stilles til vores ukendte form $g \in S_{3/2}(128)$ - altså at $T_{p^2} g = a_p(f_1) g$ for alle ulige primtal -, kan vises eller afvises at være opfyldt for en given kandidat g ved for endeligt mange ulige primtal p (i det foreliggende tilfælde rækker det at tage $p \in \{3, 5\}$) at teste, om T_{p^2} giver den ønskede virkning på g's Fourierkoefficienter op til en vis eksplicit angivelig grænse. At finde et $g \in S_{3/2}(128)$ således, at (♭♭♭) gælder, er således reduceret til en endelig mængde lineær algebra. Man kan på denne måde verificere, at vi har (♭♭♭), hvis g betegner følgende form:

$$g(\tau) := \sum_{x,y,z=-\infty}^{\infty} (-1)^z \cdot e^{2\pi i \tau \cdot (2x^2 + (4y+1)^2 + 8z^2)} \ . \tag{♮}$$

At denne funktion virkelig er et element i $S_{3/2}(128)$, er i princippet standard 19. århundredes-viden: Beviset kan føres ved klassisk Fourieranalyse (Poisson-summation) analogt til beviset for den klassiske *theta-transformationsformel*:

$$\theta\left(-\frac{1}{4\tau}\right) = \sqrt{\frac{2\tau}{i}}\theta(\tau) \ ,$$

hvor $\theta(\tau) := \sum_{n=-\infty}^{\infty} e^{2\pi i n^2 \tau}$, for $\mathrm{Im}(\tau) > 0$.

Vi kan nu let afslutte beviset for Tunnell's sætning: Tallet $L(f_1, 1)$ kan beregnes numerisk; det er givet ved den uendelige række:

$$L(f_1, 1) = 2 \cdot \sum_{n=1}^{\infty} a_n(f_1) n^{-1} e^{-\pi n/\sqrt{8}} \ ,$$

så man beregner, at $L(f_1, 1) = 0,655514\ldots \neq 0$. For vores form g givet ved ($\natural$) haves $b_1(g) = 1 \neq 0$. Da g tilfredsstiller ($\flat\flat\flat$), fås således

$$L(E_d, 1) = L(f_d, 1) \neq 0 \Leftrightarrow b_d(g) \neq 0 \ ,$$

så ($\flat$) følger, hvis vi viser, at $b_d(g) = c_d$. Lad:

$$\begin{aligned} u_d &:= \#\{(x,y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 32z^2 = d\} \\ &= \#\{(x,y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 8z^2 = d, \ z \text{ lige}\} \ , \\ v_d &:= \#\{(x,y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 8z^2 = d, \ z \text{ ulige}\} \ ; \end{aligned}$$

da er $c_d = u_d - \frac{1}{2} \cdot (u_d + v_d)$, altså $2c_d = u_d - v_d$. Men nu har vi også:

$$\begin{aligned} u_d = \ & \#\{(x,y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 8z^2 = d, \ z \text{ lige}, \ y \text{ af form } 4t+1\} \\ & + \#\{(x,y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 8z^2 = d, \ z \text{ lige}, \ y \text{ af form } 4t+3\} \\ = \ & \#\{(x,y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 8z^2 = d, \ z \text{ lige}, \ y \text{ af form } 4t+1\} \\ & + \#\{(x,-y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 8z^2 = d, \ z \text{ lige}, \ y \text{ af form } 4t+1\} \\ = \ & 2 \cdot \#\{(x,y,z) \in \mathbb{Z}^3 \mid \ 2x^2 + y^2 + 8z^2 = d, \ z \text{ lige}, \ y \text{ af form } 4t+1\} \ , \end{aligned}$$

og tilsvarende for v_d, hvoraf sluttes $u_d - v_d = 2b_d(g)$.

Eksempel

Betragt tallet 751 (primtal). Vi har, at $751 \equiv 7 \ (8)$, i.e. 751 giver rest 7 ved division med 8. Hvis man bemærker, at kvadratet på et ulige, helt tal er $\equiv 1 \ (8)$, ser man da, at ingen af ligningerne $2x^2 + y^2 + 32z^2 = 751$ og $2x^2 + y^2 + 8z^2 = 751$ har en løsning i hele tal x, y, z. Tallet c_{751} fra Tunnell's sætning er således $= 0$. Af *beviset* for Tunnell's sætning følger derfor, at $L(E_{751}, 1) = 0$ (alternativt kan dette vises på følgende måde: Der findes en algoritme til bestemmelse af fortegnet $\sigma(E)$ fra sætning 1; benyttes denne, finder man, at $\sigma(E_{751}) = -1$; af sætning 1 følger da $L(E_{751}, 1) = 0$). Nu er det således, at man for en modulær elliptisk kurve E v.hj.a. af tallene $a_n(E)$ kan udtrykke tallet $L'(E, 1)$ ved en hurtigt konvergerende uendelig række. Jeg beslutter mig for et beregningsmæssigt overkill og forlanger 1000 led af denne uendelige række hørende til E_{751} og hvert led beregnet med 100 decimalers nøjagtighed. Efter knapt 2 sek. regnetid oplyser min computer mig, at $L'(E_{751}, 1) = 10,89225888\ldots$. Den nævnte uendelige række konvergerer så hurtigt, at man heraf rigorøst kan slutte, at $L'(E_{751}, 1) \neq 0$. Vi har følgelig $r_{an}(E_{751}) = 1$. Ifølge Kolyvagin's sætning (sætning 3 ovenfor) er da $r(E_{751}) = 1$. Ifølge lemma 2 er derfor 751 et kongruenstal. På helt tilsvarende vis viser man, at 1063 (primtal) også er et kongruenstal.

Øvelse 3: Vi beviste altså netop eksistensen af rationale tal α, β, γ med den egenskab, at $\gamma^2 - \beta^2 = \beta^2 - \alpha^2 = 751$. Men kan vi også faktisk *angive* et eksempel på sådanne rationale tal α, β, γ? Nu, man konstaterer, at:

$$\left(\frac{99126392479}{2323841520}\right)^2 - \left(\frac{75963556321}{2323841520}\right)^2 = \left(\frac{75963556321}{2323841520}\right)^2 - \left(\frac{41411134879}{2323841520}\right)^2 = 751.$$

Øvelsen består i at tænke over, hvorledes man finder sådan en løsning. Eventuelle læsere, der let finder denne eller en anden løsning, og som derfor ikke forstår eksemplets og øvelsens pointe, kan i stedet betragte tilfældet $d = 1063$. (Se eventuelt kommende algebraseminar).

Grupper med lutter normale undergrupper

Asger Grunnet

Indledning

Da jeg i sin tid læste 3AL (efter Christian U. Jensens noter fra 1993) stødte jeg på følgende bemærkning:

> „Quaterniongruppen har en bemærkelsesværdig egenskab. Den er ikke abelsk, men samtlige undergrupper er normale."

Som bekendt er alle undergrupper i en abelsk gruppe normale, men det omvendte gælder altså ikke. Nu har jeg altid været nysgerrig, så jeg kunne ikke lade være med at spekulere over hvilke andre grupper der har denne egenskab. Det viser sig at der, i en vis forstand, faktisk ikke findes andre end quaterniongruppen. Hvad der rent faktisk gælder, vil jeg vente lidt med at afsløre. (De der ikke kan vente, kan springe direkte til sætning 3 og få afklaret spørgsmålet med det samme.)

Jeg vil kalde en endelig gruppe G *pseudoabelsk*, hvis G ikke er abelsk, men alle undergrupper i G er normale. Det er mit mål i det følgende at bestemme alle pseudoabelske grupper. (Bemærk at jeg her har begrænset mig til endelige grupper.)

Lidt notation

Lad mig starte med at minde om lidt gruppeteoretisk notation. Hvis G er en gruppe og $x, y \in G$ er $[x, y] := xyx^{-1}y^{-1}$. Læg især mærke til at der gælder:

$$[x, y] = 1 \iff xy = yx$$

altså at x og y kommuterer netop hvis $[x, y] = 1$.

Hvis $x_1, \ldots, x_n$ er elementer i G, er $\langle x_1, \ldots, x_n \rangle$ undergruppen frembragt af $x_1, \ldots, x_n$, det vil sige den mindste undergruppe i G, der indeholder $x_1, \ldots, x_n$.

For $x \in G$ er $|x|$ (*ordenen* af x) givet ved:

$$|x| := \min\{k \in \mathbb{N} | x^k = 1\}.$$

Husk at der for $n \in \mathbb{N}$ gælder $x^n = 1$ netop hvis n er delelig med $|x|$.

Quaterniongruppen Q_8 (ikke at forveksle med en vis tankstation!) kan nu beskrives som gruppen $\langle x, y \rangle$, hvor x og y er elementer som opfylder: $|x| = |y| = 4$, $x^2 = y^2$ og $xy = y^{-1}x$.

G's *centrum* $Z(G)$ er defineret ved:

$$Z(G) := \{x \in G | \forall y \in G : xy = yx\}.$$

Et element $x \in G$ kaldes *centralt*, hvis $x \in Z(G)$.

En gruppe hvis orden er en potens af primtallet p, kaldes en *p-gruppe*. Hvis $|G| = p_1^{a_1} \cdots p_r^{a_r}$, hvor $p_1, \ldots, p_r$ er forskellige primtal, findes for hvert $i = 1, \ldots, r$ en undergruppe P_i i G med $|P_i| = p_i^{a_i}$. Sådanne undergrupper kaldes *Sylowgrupper*.

Endelig bør jeg for god ordens skyld minde om hvad en nilpotent gruppe er, selv om jeg egentlig ikke får brug for det: En gruppe G kaldes *nilpotent*, hvis der findes normale undergrupper $G_1, \ldots, G_n$ i G, så

$$1 = G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G$$

og $G_{i+1}/G_i \subseteq Z(G/G_i)$ for $i = 1, \ldots, n-1$.
Der findes utallige måder at karakterisere nilpotente grupper på. Tillad mig at nævne følgende velkendte karakterisering uden bevis:

Sætning 1. *Lad G være en endelig gruppe. Følgende betingelser er da ækvivalente:*

(1) G er nilpotent.
(2) Alle Sylowgrupper i G er normale.
(3) G er isomorf med det direkte produkt af G's Sylowgrupper.

Pseudoabelske grupper

Det er klart, at en pseudoabelsk gruppe G automatisk opfylder (2) i sætning 1. Af (3) får man derfor at G har formen

$$G \cong P_1 \times \cdots \times P_n,$$

hvor $P_1, \ldots, P_n$ er de forskellige Sylowgrupper i G. Det er desuden klart at en undergruppe i G vil være enten abelsk eller pseudoabelsk, specielt gælder dette for Sylowgrupperne. Iøvrigt må mindst én af Sylowgrupperne være pseudoabelsk, da G ellers ville være abelsk. Dette reducerer analysen af pseudoabelske grupper til at betragte pseudoabelske p-grupper for primtal p. Før jeg går igang med at betragte pseudoabelske p-grupper, vil jeg nævne nogle lemmaer:

Lemma 1. *Lad A og B være normale undergrupper af en gruppe G, med $A \cap B = 1$. Hvis $a \in A$ og $b \in B$ er $ab = ba$.*

Bevis: Da A og B er normale, er $ba^{-1}b^{-1} \in A$ og $aba^{-1} \in B$, og dermed er

$$[a, b] = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in A \cap B = 1.$$

□

Lemma 2. *Hvis G er pseudoabelsk og elementet $z \in G$ har orden 2, da er $z \in Z(G)$.*

Bevis: Antag at $z \in G$ har orden 2, og lad $x \in G$ være vilkårlig. Da G er pseudoabelsk er undergruppen $\langle z \rangle = \{1, z\}$ normal, specielt er $xzx^{-1} \in \{1, z\}$. Da $xzx^{-1} \neq 1$ (ellers ville $z = 1$ i modstrid med $|z| = 2$), må $xzx^{-1} = z$, det vil sige $xz = zx$. Altså vil z tilhøre $Z(G)$. □

Det følgende tekniske lemma er snarere talteoretisk end gruppeteoretisk:

Lemma 3. *Lad p være et primtal. Lad $k, q, r, s \in \mathbb{N}$ og antag at $k \equiv 1 \pmod{p^r}$, at p^s er den største p-potens, der går op i q, samt at $p^s > 2$. Så er*

$$\sum_{i=0}^{q-1} k^i \equiv q \pmod{p^{r+1}}.$$

Bevis: Da $k \equiv 1 \pmod{p^r}$ findes $a \in \mathbb{N}_0$ så $k = 1 + ap^r$. Nu er:

$$\begin{aligned}
\sum_{i=0}^{q-1} k^i &= \sum_{i=0}^{q-1} (1+ap^r)^i = \sum_{i=0}^{q-1} \sum_{j=0}^{i} \binom{i}{j} (ap^r)^j \\
&\equiv \sum_{i=0}^{q-1} (1+iap^r) \pmod{p^{r+1}} \\
&= q + ap^r \sum_{i=0}^{q-1} i \\
&= q + ap^r \frac{q(q-1)}{2}.
\end{aligned}$$

Da $p^s > 2$, vil $\frac{q(q-1)}{2}$ være delelig med p, og dermed må $q + ap^r \frac{q(q-1)}{2} \equiv q \pmod{p^{r+1}}$, hvilket viser det ønskede. □

Hvis p er et primtal og x og y er gruppeelementer der frembringer en pseudoabelsk p-gruppe vil jeg kalde x, y for et *p-par*. Bemærk at $xy \neq yx$ (idet gruppen $\langle x, y \rangle$ ellers ville være abelsk). Bemærk også at enhver pseudoabelsk gruppe vil indeholde et p-par for et primtal p (idet man blot vælger to ikke-kommuterende elementer i en pseudoabelsk Sylowgruppe). Her er et par lemmaer, der viser hvordan p-par opfører sig:

Lemma 4. *Lad x, y være et p-par. Da findes $k \in \mathbb{N}$, k delelig med p, så $[x, y] = y^k$.*

Bevis: Da $\langle x \rangle$ og $\langle y \rangle$ er normale undergrupper i $\langle x, y \rangle$, vil

$$[x, y] = x(yx^{-1}y^{-1}) = (xyx^{-1})y^{-1} \in \langle x \rangle \cap \langle y \rangle \subseteq \langle y \rangle,$$

specielt er $[x, y] = y^k$ for et $k \in \mathbb{N}$. Hvis k ikke var delelig med p, ville $\langle y^k \rangle = \langle y \rangle$ og dermed ville $y \in \langle y^k \rangle \subseteq \langle x \rangle \cap \langle y \rangle \subseteq \langle x \rangle$, specielt skulle y kommutere med x, hvilket er en modstrid. □

Ligningen $[x, y] = y^k$ i lemma 4 kan omskrives til $xyx^{-1} = y^{k+1}$, og det ses let (f.eks. ved induktion efter q) at x og y også opfylder:

$$xy^q x^{-1} = y^{q(k+1)} \quad \text{og at} \quad x^q y x^{-q} = y^{(k+1)^q},$$

for alle $q \in \mathbb{N}$.

Lemma 5. *Lad x, y være et p-par. Da gælder:* $[x^p, y] = 1 \iff [x, y^p] = 1$.

Bevis: Af symmetri-grunde er det nok at vise den ene implikation. Antag at $[x, y^p] = 1$. Ifølge lemma 4 er

$$1 = [x, y^p] = xy^p x^{-1} y^{-p} = y^{p(k+1)} y^{-p} = y^{pk},$$

for et tal k som er deleligt med p. For at dette kan lade sig gøre må $|y|$ gå op i pk. Nu er

$$[x^p, y] = x^p y x^{-p} y^{-1} = y^{(k+1)^p} y^{-1} = y^{(k+1)^p - 1}.$$

Der gælder:

$$(k+1)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} k^i \equiv \binom{p}{1} k = pk \equiv 0 \pmod{|y|},$$

idet det benyttes at k^i er delelig med $|y|$, når $i > 1$. Heraf ses det at $[x^p, y] = 1$. □

Som alle der har beskæftiget sig med gruppeteori ved, udgør primtallet 2 meget ofte et specialtilfælde. (Tænk for eksempel på sætningen: Enhver gruppe af ulige orden er opløselig!) Som det ses af den følgende sætning, gælder dette også her. Bemærk iøvrigt at specialtilfældet her kommer fra specialtilfældet $p^s = 2$ i det talteoretiske lemma (lemma 3).

Sætning 2. *Lad p være et primtal, og antag at x, y er et p-par. Da er $p = 2$ og $\langle x, y\rangle \cong Q_8$.*

Bevis: Vælg $q \in \mathbb{N}_0$ maksimal så $[x^{p^q}, y] \neq 1$ og sæt $\tilde{x} = x^{p^q}$. Nu er $\tilde{x}, y$ et p-par og $[\tilde{x}^p, y] = 1$.
Vælg $m, n \in \mathbb{N}$ minimale, så $\tilde{x}^{p^m}, y^{p^n} \in \langle \tilde{x}\rangle \cap \langle y\rangle$. Der må nødvendigvis gælde at

$$\langle \tilde{x}^{p^m}\rangle = \langle y^{p^n}\rangle = \langle \tilde{x}\rangle \cap \langle y\rangle = \langle x\rangle \cap \langle y\rangle.$$

(Overvej.) Specielt findes et tal $c \in \mathbb{N}$, som ikke er deleligt med p, så $\tilde{x}^{p^m} = y^{cp^n}$. Det kan antages at $c = 1$ idet man blot erstatter y med y^c (det er klart at y og y^c frembringer de samme grupper), således at $\tilde{x}^{p^m} = y^{p^n}$.
Sæt $\tilde{y} = \tilde{x}^{-p^{|m-n|}} y$. Det er klart at $\langle \tilde{x}, \tilde{y}\rangle = \langle \tilde{x}, y\rangle$.
Påstand: $m = n$. Antag nemlig at $m > n$ (tilfældet $m < n$ udelukkes tilsvarende). Da $[\tilde{x}^p, y] = 1$ er også $[\tilde{x}^{-p^{m-n}}, y] = 1$. Derfor er

$$\tilde{y}^{p^n} = (\tilde{x}^{-p^{m-n}} y)^{p^n} = \tilde{x}^{-p^m} y^{p^n} = y^{-p^n} y^{p^n} = 1.$$

Antag at $z \in \langle \tilde{x}\rangle \cap \langle \tilde{y}\rangle$. Så findes $a, b \in \mathbb{N}$, så

$$z = \tilde{x}^a = \tilde{y}^b = (\tilde{x}^{-p^{m-n}} y)^b = \tilde{x}^{-bp^{m-n}} y^b.$$

Heraf ses det at $y^b = \tilde{x}^{a+bp^{m-n}} \in \langle \tilde{x}\rangle \cap \langle y\rangle$, hvorfor der må gælde at p^n går op i b. Altså må $z = \tilde{y}^b = 1$. Dette viser at $\langle \tilde{x}\rangle \cap \langle \tilde{y}\rangle = 1$, og af lemma 1 sluttes at $\tilde{x}$ og $\tilde{y}$ kommuterer, men så må gruppen $\langle \tilde{x}, y\rangle = \langle \tilde{x}, \tilde{y}\rangle$ jo være abelsk, hvilket er en modstrid. Dermed må $m = n$ (og $\tilde{y} = \tilde{x}^{-1} y$).
Ifølge lemma 4 anvendt på p-parret $\tilde{x}, y$ findes $k \in \mathbb{N}$, så $\tilde{x} y \tilde{x}^{-1} = y^k$, hvor $k - 1$ er delelig med p. Lad p^r være den største p-potens, der går op i $k - 1$. Da $[\tilde{x}^p, y] = 1$, er ifølge lemma 5 også $[\tilde{x}, y^p] = 1$ og derfor er $y^p = \tilde{x} y^p \tilde{x}^{-1} = y^{pk}$. Dette medfører at $p \equiv pk \pmod{|y|}$, altså at $p(k-1)$ er delelig med $|y|$. Da $k - 1$ ikke er delelig med $|y|$ (i så fald ville $\tilde{x}$ jo kommutere med y), må $|y| = p^{r+1}$.
Påstand: $p^m = 2$. Antag at $p^m > 2$. Ifølge lemma 3 (med $q = p^m$ og $s = m$) er så

$$\sum_{i=0}^{p^m - 1} k^i \equiv p^m \pmod{|y|}.$$

Heraf ses det at

$$\tilde{y}^{p^m} = (\tilde{x}^{-1}y)^{p^m} = \tilde{x}^{-p^m}y^{1+k+k^2+\cdots+k^{p^m-1}} = y^{-p^m}y^{p^m} = 1,$$

idet ligningen $y\tilde{x}^{-1} = \tilde{x}^{-1}y^k$ benyttes til at „ flytte y'erne mod højre" .
Ethvert element i gruppen $H := \langle \tilde{x}, y\rangle = \langle \tilde{x}, \tilde{y}\rangle$ kan skrives på formen $\tilde{x}^a y^b$ (idet y'erne kan „flyttes mod højre" som ovenfor). Da $\langle \tilde{y}^{p^m}\rangle = \langle \tilde{x}\rangle \cap \langle y\rangle$, må H indeholde præcis $|\tilde{x}|\, p^m$ elementer. Eftersom ethvert element i H ligeledes kan skrives på formen $\tilde{x}^a\tilde{y}^b$, hvor $0 \le a < |\tilde{x}|$ og $0 \le b < |\tilde{y}| \le p^m$, må $\langle \tilde{x}\rangle \cap \langle \tilde{y}\rangle = 1$, idet der ellers ikke ville kunne forekomme $|\tilde{x}|\, p^m$ forskellige elementer. Ifølge lemma 1 må $\tilde{x}$ og $\tilde{y}$ nu kommutere, hvilket er en modstrid. Altså er $p^m = 2$.
Vi konkluderer nu at $p = 2$ og $m = n = 1$, specielt at $\langle \tilde{x}^2\rangle = \langle y^2\rangle = \langle \tilde{x}\rangle \cap \langle y\rangle = \langle x\rangle \cap \langle y\rangle$. Da sætningens antagelse er symmetrisk i x og y, må ligeledes $\langle x^2\rangle = \langle x\rangle \cap \langle y\rangle$. (Altså må faktisk $x = \tilde{x}$ og $x^2 = y^2$.)
Det kan antages at $k = 2^r + 1$, idet $k - 1$ er delelig med 2^r, men ikke med 2^{r+1}, og k kun er defineret modulo $|y| = 2^{r+1}$.
Påstand: $|x| = |y| = 4$. Sæt $z = y^{2^{r-1}-1}x$, så er

$$z^2 = y^{2^{r-1}-1}xy^{2^{r-1}-1}x = y^{(2^{r-1}-1)(1+k)}x^2 = y^{(2^{r-1}-1)(2+2^r)+2} = y^{2^{2r-1}}.$$

Hvis $r \ge 2$ er $2r - 1 \ge r + 1$ og dermed er $z^2 = 1$. I så fald er z central ifølge lemma 2, specielt vil y kommutere med z og dermed med x, hvilket er en modstrid. Dette viser at $r = 1$, altså at $|y| = 2^{r+1} = 4$. Tilsvarende må også $|x| = 4$.
Ialt er det vist at $|x| = |y| = 4$, at $x^2 = y^2$, samt at $xy = y^k x = y^3 x = y^{-1}x$, altså at $\langle x, y\rangle \cong Q_8$. □

Ved hjælp af sætningen er det nu endelig muligt at bestemme samtlige pseudoabelske grupper:

Korollar 1. *Hvis G er en pseudoabelsk gruppe, da er: $G \cong Q_8 \times (C_2)^n \times A$, hvor C_2 er den cykliske gruppe af orden 2, n er et ikke-negativt heltal og A er en abelsk gruppe af ulige orden.*

Bevis: Lad G være pseudoabelsk. Ifølge sætning 1 er $G \cong P_1 \times P_2 \times \cdots \times P_r$, hvor $P_1, \ldots, P_r$ er Sylowgrupperne i G. Disse er alle abelske eller pseudoabelske og mindst én er pseudoabelsk. Ifølge sætning 2 er det kun 2-Sylowgruppen, der kan være pseudoabelsk. Antag at $S := P_1$ er 2-Sylowgruppen, og sæt $A = P_2 \times \cdots \times P_r$. Så er $G \cong S \times A$, og A er en abelsk gruppe af ulige orden.
Lad x, y være et 2-par i S. Ifølge sætning 2 er $\langle x, y\rangle \cong Q_8$, det vil sige $|x| = |y| = 4$, $x^2 = y^2$ og $xyx^{-1} = y^3$. Lad $z \in S$ være vilkårligt.
Påstand: $z = g\tilde{z}$, hvor $g \in \langle x, y\rangle$ og $|\tilde{z}| \le 2$. Der deles op i fire tilfælde: z kan kommutere med x eller ikke, og z kan kommutere med y eller ikke. Hvis f.eks. z kommuterer med y men ikke med x, vil x, z være et 2-par. Ifølge sætning 2 er så $|z| = 4$, $z^2 = x^2 = y^2$ og $xzx^{-1} = z^3$. Nu er

$$x(yz)x^{-1} = (xyx^{-1})(xzx^{-1}) = y^3z^3 = yz,$$

dvs. x kommuterer med yz. Bemærk at y kommuterer med yz netop hvis y kommuterer med z. I dette tilfælde sættes $g = y^{-1}$ og $\tilde{z} = yz$. De øvrige tilfælde er

tilsvarende. Dette viser at ethvert $z \in S$ kan skrives som et produkt $z = g\tilde{z}$, hvor g tilhører $\langle x, y\rangle$ og $\tilde{z}$ kommuterer med både x og y.
Antag nu at $\tilde{z} \in S$ kommuterer med både x og y samt at $|\tilde{z}| > 2$. Det kan antages at $|\tilde{z}| = 4$, idet $\tilde{z}$ ellers erstattes med en passende potens af $\tilde{z}$. Betragt undergruppen $H := \langle y\tilde{z}\rangle$. Da S er pseudoabelsk, er H normal. Specielt må

$$y^3\tilde{z} = xyx^{-1}\tilde{z} = x(y\tilde{z})x^{-1} \in H = \{1, y\tilde{z}, y^2\tilde{z}^2, y^3\tilde{z}^3\}.$$

Det ses let at dette giver en modstrid i hvert af de fire tilfælde, f.eks. vil $y^3\tilde{z} = 1$ medføre at $y = \tilde{z}$, hvilket er en modstrid, da x kommuterer med $\tilde{z}$ men ikke med y. Vi konkluderer at ethvert element i S er på formen $g\tilde{z}$, hvor $g \in \langle x, y\rangle$ og $\tilde{z}$ har orden højst 2 (og er centralt ifølge lemma 2). Dette kan kun lade sig gøre, hvis $S \cong \langle x, y\rangle \times (C_2)^n$ for et tal $n \in \mathbb{N}_0$ (overvej), hvilket viser det ønskede. □

Jeg burde nu strengt taget vise at alle grupperne i korollaret er pseudoabelske, men det vil jeg overlade til læseren. Jeg vil slutte af med at bemærke (uden bevis), at der gælder noget tilsvarende for vilkårlige (altså også uendelige) grupper, nemlig følgende:

Sætning 3. *Lad G være en ikke-abelsk gruppe hvori enhver undergruppe er normal. Da er $G \cong Q_8 \times A$, hvor A er en abelsk gruppe, og ethvert element $a \in A$ opfylder at $|a| < \infty$ og at $|a|$ ikke er delelig med 4.*