

# Om kongruenstal.

Ian Kiming.

<http://www.math.ku.dk/~kiming/>

## CONTENTS

1. Indledning.	1
2. Omformulering.	2
3. L-rækker, spidsformer og modularitet.	4
4. Birch- og Swinnerton-Dyer formodningen og Waldspurger's sætning.	6
5. Eksempel.	9

## 1. 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  $\alpha, \beta, \gamma$ , hvis kvadrater er på hinanden følgende tal i en aritmetisk progression med modulus  $d$ ; med andre ord: Der spørges efter rationale tal  $\alpha, \beta, \gamma$  således, at:

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

Hvis  $(*)$  har en løsning i rationale tal  $\alpha, \beta, \gamma$ , 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 *karaktarisere* 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  $(\alpha, \beta, \gamma)$  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 i afsnit 3).

**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 kvadrattfrit. Af pladshensyn vil vi i denne artikel yderligere antage, at  $d$  er ulige; tilfældet, hvor  $d$  er lige kan behandles helt analogt. Altså:

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

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

**Sætning 1.1.** *Definer:*

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

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

*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 ud fra 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 løsbarehed 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 løsbarehed 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.

## 2. OMFORMULERING.

**Lemma 2.1.** *Ligningen (\*) 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:

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

og vi vil betegne den specielle elliptiske kurve, der forekommer i 2.1, med  $E_d$ , altså:

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

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  $x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - a - x_1 - x_2$ ,  $y_3 = -\left(\frac{y_1 - y_2}{x_1 - x_2}\right)x_3 - \left(\frac{y_2x_1 - y_1x_2}{x_1 - x_2}\right)$  (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  $\ell$ . Den såkaldte Nagell-Lutz sætning specialiseret til kurven  $E_\ell$  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 2.2.** ( $d$  er et kongruenstal)  $\Leftrightarrow r(E_d) > 0$ .

**Bevis:** Ifølge Lemma 2.1 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  $r(E_d) > 0$ .

## 3. L-RÆKKER, SPIDSFORMER OG MODULARITET.

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  $(a_2(E), a_3(E), a_5(E), a_7(E), a_{11}(E), \dots)$  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:

$$(\#) \quad \zeta(s) := \sum_{n=1}^{\infty} n^{-s} = \prod_p (1 - p^{-s})^{-1} ,$$

med sin udvidede version:

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

hvor  $\Gamma$  er den sædvanlige gamma-funktion. Som bekendt konvergerer (#) absolut for  $s \in \mathbb{C}$ ,  $\operatorname{Re}(s) > 1$ , 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:

$$(\#\#) \quad L(E, s) := \prod_p (1 - a_p(E) \cdot p^{-s} + p^{1-2s})^{-1} ,$$

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  $|a_p(E)| < 2\sqrt{p}$ , kan man slutte, at (#) konvergerer absolut for  $s \in \mathbb{C}$ ,  $\operatorname{Re}(s) > 2$  og definerer en holomorf funktion af  $s$  i dette område. I dette område kan vi så gange paranteserne i (#) ud, og finder under benyttelse af den geometriske række

$$(1 - q)^{-1} = 1 + q + q^2 + \dots$$

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

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 tilfredsstillen 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'  $\{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$  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)  $\exists \nu \in ]0, 2[$ :  $f(\tau) = O(\text{Im}(\tau)^{-\nu})$  for  $\text{Im}(\tau) \rightarrow 0+$ , uniformt m.h.t.  $\text{Re}(\tau)$ . 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  $\text{Re}(s) > 2$ , har holomorf fortsættelse til hele  $s \in \mathbb{C}$ , og tilfredsstillen her funktionalligningen:

$$\text{###} \quad \Lambda(f, s) = -\Lambda(\hat{f}, 2 - s),$$

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  $\text{Re}(s) > 2$ . Af ### følger da med lidt ekstra arbejde, hvor man viser, at der i dette tilfælde gælder  $\hat{f} = \pm f$ :

**Sætning 3.1.** *Lad  $E$  være en modulær elliptisk kurve over  $\mathbb{Q}$ . Da kan  $\Lambda(E, s)$  fortsættes holomorft til hele  $s \in \mathbb{C}$ , og tilfredsstillen her funktionalligningen:*

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

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 holomorfe funktion at gøre? *Noget* af mystikken forsvinder, hvis man ved, at en spidsform i virkeligheden er et betydeligt mere abstrakt (repræsentationsteoretisk, algebraisk-geometrisk) objekt. Intuitivt kunne man sige, at den holomorfe funktion  $f$  ovenfor blot er en af  $\infty$  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.

T.-S.-formodningen er blevet bevist i fuld almenhed af C. Breuil, B. Conrad, F. Diamond og R. Taylor. Beviset forløber over adskillige etaper, hvoraf Wiles' store sætning udgør den første. Relativt kort tid efter Wiles' resultat var man (F. Diamond og K. Kramer) dog i stand til at bevise følgende udsagn: *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 3.2.** *Kurven  $E_d$  er modulær.*

At bruge Wiles' store sætning til at bevise sætning 3.2 er i virkeligheden et massivt teoretisk overkill; grunden er, at kurverne  $E_d$  tilhører en speciel klasse af elliptiske kurver, hvis teori er simple 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.h.j.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 3.2. 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.

#### 4. BIRCH- OG SWINNERTON-DYER FORMODNINGEN OG WALDSPURGER'S 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 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 4.1.** (*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 koherent formodningsnetværk (Beilinson-formodningerne), der forbinder algebraisk-aritmetiske egenskaber ved bestemte typer af talteoretiske objekter (såkaldte '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 2.2 og sætning 4.1 kan vi da konkludere:

**Lemma 4.1.**  $L(E_d, 1) \neq 0 \Rightarrow (d \text{ er ikke kongruenstal})$ .

*Hvis B.-Sw.-D.-formodningen gælder, kan denne implikation vendes om.*

Et bevis for [Tunnell's sætning](#) fås derfor, hvis man viser:

$$(b) \quad L(E_d, 1) \neq 0 \Leftrightarrow c_d \neq 0 .$$

Vi skitserer nu, hvordan man kan reducere beviset for (b) 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  $(E_d)_d$  ulige, kvadrattfri; disse værdier er  $L(f_d, 1)$ , hvor  $(f_d)_d$  ulige, kvadrattfri 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  $\left(\frac{d}{\ell}\right)$  er det sædvanlige Legendre-symbol, altså (eksempelvis) for primtal  $\ell$ ,  $(d, \ell) = 1$ :  $\left(\frac{d}{\ell}\right) = 1$ , 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 (bbb) 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  $\{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$  med:

(i)  $\exists \nu \in ]0, 3/2[$ :  $g(\tau) = O(\text{Im}(\tau)^{-\nu})$  for  $\text{Im}(\tau) \rightarrow 0+$ , uniformt m.h.t.  $\text{Re}(\tau)$ ; (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:

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

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 (bb) - således, at:

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

formen  $g$  er ikke entydigt bestemt ved kravet (bbb), men (bbb) er opfyldt, hvis  $g$  for ethvert ulige primtal  $p$  er egenform for en vis operator (kaldet en Hecke-operator)  $T_{p^2}$  med tilhørende egenverdier  $a_p(f_1)$ , 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-dimensionaleitet 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  $p$ , 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 (bbb) gælder, er således reduceret til en endelig mængde lineær algebra. Man kan på denne måde verificere, at vi har (bbb), hvis  $g$  betegner følgende form:

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

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  $\text{Im}(\tau) > 0$ .

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  $L(f_1, 1) = 0,655514\dots \neq 0$ . For vores form  $g$  givet ved [\(h\)](#) haves  $b_1(g) = 1 \neq 0$ . Da  $g$  tilfredsstiller [\(bbb\)](#), fås således

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

så [\(b\)](#) 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:

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

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

## 5. EKSEMPEL.

Betragt tallet 751 (primtal). Vi har, at  $751 \equiv 7 \pmod{8}$ , i.e. 751 giver rest 7 ved division med 8. Hvis man bemærker, at kvadratet på et ulige, helt tal er  $\equiv 1 \pmod{8}$ , 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 [3.1](#); benyttes denne, finder man, at  $\sigma(E_{751}) = -1$ ; af sætning [3.1](#) følger da  $L(E_{751}, 1) = 0$ ). Nu er det således, at man for en modulær elliptisk kurve  $E$  v.h.j.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  $L'(E_{751}, 1) = 10,89225888\dots$ . 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 4.1 ovenfor) er da  $r(E_{751}) = 1$ . Ifølge lemma 2.2 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  $\alpha, \beta, \gamma$  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  $\alpha, \beta, \gamma$ ? Nu, man konstaterer, at:

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

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  $d = 1063$ .