

Fermat's sidste sætning: En oversigt.

Ian Kiming

14 Oktober, 1999

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

kimming@math.ku.dk

CONTENTS

| | |
|---|----|
| 1. Optakt: Et klassisk problem. | 2 |
| 1.1. Algebraisk-talteoretisk fortolkning. | 3 |
| 1.2. Højniveaufortolkning. | 4 |
| 2. Modulformer og Galoisrepræsentationer. | 5 |
| 2.1. Modulformer | 5 |
| 2.2. Hecke-operatorer og Galoisrepræsentationer. | 8 |
| 2.2.1. Antydning af konstruktion: | 10 |
| 2.3. Artin-formodningen | 11 |
| 2.4. Galoisrepræsentationer i positiv karakteristisk og Serre's formodning. | 13 |
| 2.4.1. Nogle modulære mod 3 repræsentationer: | 14 |
| 2.5. Ribet's sætning | 16 |
| 3. Elliptiske kurver og Taniyama-Shimura-formodningen. | 17 |
| 3.1. Elliptiske kurver. | 17 |
| 3.2. Elliptiske kurver og Galoisrepræsentationer. I | 18 |
| 3.3. Elliptiske kurver og Galoisrepræsentationer. II | 20 |
| 3.4. Wiles' sætning. | 22 |
| 4. Fermat's sidste sætning. | 23 |
| 4.1. Frey-kurver. | 23 |
| 4.2. Fermat's sidste sætning. | 24 |
| Appendix A. Valuationer. | 25 |
| A.1. Kompletion. | 26 |
| A.2. Udvidelser. | 26 |
| A.3. Forgrening og Frobenius-elementer. | 27 |
| A.4. Højere forgreningsgrupper. | 28 |
| Appendix B. Absolutte Galoisgrupper. | 29 |
| B.1. Dekompositionsgrupper | 29 |
| B.2. Galoisrepræsentationer. | 30 |
| B.3. Førere af Galoisrepræsentationer. | 32 |
| B.4. Bemærkninger. | 34 |
| References | 35 |

Dette manuskripts indhold beskrives godt af dets titel: En ikke overmåde teknisk, men heller ikke overfladisk oversigt over nogle af de essentielle punkter i A. Wiles' bevis for Fermat's sidste sætning. Manuskriptet indeholder et appendiks med en

oversigt over nogle nødvendige grundbegreber fra den algebraiske talteori. Læsere uden baggrund i algebraisk talteori kan som det første kort skimme dette appendiks igennem. De i appendikset omtalte grundbegreber vil blive benyttet frit i det følgende. Litteraturlisten indeholder referencer til såvel baggrundsmateriale som til avancerede arbejder.

Overalt i det følgende betegner p og ℓ primtal.

1. OPTAKT: ET KLASSISK PROBLEM.

Litteratur: [BS], [Neu], [Koc], [CF]

Lad os betragte en af de mest velkendte kurver i planen, nemlig enhedscirklen:

$$(*) \quad x^2 + y^2 = 1 .$$

Vi er alle fortrolige med strukturen af løsninger i *reelle* tal til (*): Løsningerne kan parametriseres ved:

$$(**) \quad (x, y) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right) ,$$

hvor t gennemløber $\mathbb{R} \cup \{\infty\}$, idet højresiden af (**) for $t = \infty$ fortolkes som $(1, 0)$. Lad os nu stille et andet – og måske tåbeligt – spørgsmål: Hvorledes ‘ser’ enhedscirklen ud over det endelige legeme med p elementer $\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}p$? Ved denne ‘enhedscirkel over \mathbb{F}_p ’ kan vi i første omgang næppe forstå andet end mængden af løsninger $(x, y) \in \mathbb{F}_p^2$ til (*). Som det første kunne vi spørge efter *antallet* af sådanne løsninger, lad os kalde det n_p . Kan vi angive en ‘formel’ for n_p som funktion af p ? Eftersom n_p kan beregnes som antallet af par (x, y) af hele tal med $0 \leq x, y \leq p - 1$ og $x^2 + y^2 \equiv 1 \pmod{p}$, er det let, (at få en computer til) at beregne eksempler på n_p :

$$n_2 = 2, \quad n_3 = 4, \quad n_5 = 4, \quad n_7 = 8, \quad n_{11} = 12, \quad n_{13} = 12, \quad n_{17} = 16, \quad n_{19} = 20,$$

$$n_{23} = 24, \quad n_{29} = 28, \dots, \quad n_{101} = 100, \dots, \quad n_{10037} = 10036, \dots$$

Studerer man disse eksempler et øjeblik, kan man opdage, at der tilsyneladende er en ‘formel’ for n_p . Lad os bevise, at den er korrekt. Man overbeviser sig let om, at (**) i det mindste for p *ulige* giver en fuldstændig parametrisering af løsningerne til (*) over \mathbb{F}_p , idet t nu gennemløber $\mathbb{F}_p \cup \{\infty\}$ med undtagelse af eventuelle værdier af t med $t^2 = -1$ i \mathbb{F}_p ; beviset herfor er analogt til det oprindelige bevis for (**) som parametrisering af de reelle løsninger til (*). For $p = 2$ er der problemer med fortolkningen af (**); vi ignorerer i første omgang dette, men vil nedenfor opdage den egentlige grund til særstillingen af tilfældet $p = 2$. Lad altså p være ulige. Ligningen $t^2 = -1$ vil have en løsning i \mathbb{F}_p , hvis og kun hvis \mathbb{F}_p^\times har et element af orden 4, altså – da \mathbb{F}_p^\times er cyklisk – hvis og kun hvis $|\mathbb{F}_p^\times| = p - 1$ er deleligt med 4; og *har* denne ligning en løsning, da har den netop 2. Med andre ord:

$$(***) \quad n_p = \begin{cases} p - 1 & , \text{ for } p \text{ ulige og } \equiv 1 \pmod{4} \\ p + 1 & , \text{ for } p \text{ ulige og } \equiv 3 \pmod{4} . \end{cases}$$

Lad nu N være et naturligt tal. Ved en *Dirichlet-karakter modulo N* forstås en homomorfi $(\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. Hvis $N = 4$, har vi $(\mathbb{Z}/N\mathbb{Z})^\times = \{\pm 1\}$, så der er netop 1 ikke-triviel Dirichlet-karakter modulo 4, nemlig $\chi: (\mathbb{Z}/4\mathbb{Z})^\times = \{\pm 1\} \rightarrow \mathbb{C}^\times$ givet ved $\chi(\pm 1) = \pm 1$. Hvis p er et ulige primtal, så er p 's restklasse modulo 4 et element i $(\mathbb{Z}/4\mathbb{Z})^\times$, og vi kan betragte χ 's værdi på denne restklasse; skriver vi $\chi(p)$ for denne værdi, og definerer vi $a_p := p - n_p$, da har vi så øjensynligt følgende omformulering af (***):

$$a_p = \chi(p), \text{ for } p \text{ ulige.}$$

1.1. Algebraisk-talteoretisk fortolkning. Den afgørende pointe i det foregående var, at ligningen $t^2 = -1$ for p ulige vist at have en løsning i \mathbb{F}_p , hvis og kun hvis $\chi(p) = 1$. Vi vil nu fortolke denne pointe algebraisk-talteoretisk. Lad os betragte det (over \mathbb{Q}) kvadratiske tallegeme $L := \mathbb{Q}(i)$, i.e. spaltningselementet for polynomiet $t^2 + 1$. Kald dette legemes ring af hele algebraiske tal for \mathfrak{D} (man kan vise, at $\mathfrak{D} = \mathbb{Z}[i]$).

Opfat nu primtal p som svarende til idealer i \mathbb{Z} (eller ækvivalent som svarende til ikke-arkimediske valuationer på \mathbb{Q}). Diskriminanten af L/\mathbb{Q} vises at være 4; følgelig er p uforgrenet i L , hvis og kun hvis p er ulige (appendiks).

Lad da p være ulige. Af sætning A.3.2 følger, at vi har følgende 2 muligheder for primfaktoriseringen af $p\mathfrak{D}$:

$$p\mathfrak{D} = \begin{cases} \mathfrak{P}_1\mathfrak{P}_2 & , \text{ med } \mathfrak{P}_1 \neq \mathfrak{P}_2 \text{ og } \mathfrak{D}/\mathfrak{P}_i \cong \mathbb{F}_p \\ \mathfrak{P} & , \text{ med } \mathfrak{D}/\mathfrak{P} \cong \mathbb{F}_{p^2}. \end{cases}$$

Disse 2 alternativer svarer øjensynligt til, at polynomiet $t^2 + 1$ har en rod i \mathbb{F}_p hhv. ikke har en rod i \mathbb{F}_p . Med χ som ovenfor, har vi følgelig:

$$(b) \quad p\mathfrak{D} = \begin{cases} \mathfrak{P}_1\mathfrak{P}_2 & , \text{ hvis } \chi(p) = 1 \\ \mathfrak{P} & , \text{ hvis } \chi(p) = -1. \end{cases}$$

Sammenhængen (b) er et eksempel på en '*dekompositionslov*' eller - i talteoretisk jargon - en '*reciprocitetslov*'; dens essentielle indhold er, at spaltningen af p i \mathfrak{D} - eller ækvivalent strukturen af fortsættelserne af den til p hørende valuation på \mathbb{Q} til L - 'kontrolleres' af en Dirichlet-karakter, nemlig χ . *Klasselegemeteorien* - en af de største landvindinger i det 20. århundredes matematik - er essentielt set en teori, der analogt til ovenstående etablerer dekompositionslove for vilkårlige cykliske (og dermed også for vilkårlige abelske) Galoisudvidelser af \mathbb{Q} via Dirichlet-karakterer; se næste afsnit for en præcis og mere moderne formulering. Klasselegemeteorien kan generaliseres til diskussion af vilkårlige abelske udvidelser af algebraiske tallegemer.

Spørgsmålet om eksistens af 'tilsvarende' dekompositionslove for vilkårlige ikke nødvendigtvis abelske udvidelser af algebraiske tallegemer kan af flere forskellige grunde betegnes som den algebraiske talteoris fundamentalproblem. En grund hertil er eksempelvis, at forståelse af strukturen af fortsættelserne af valuationer på algebraiske tallegemer til (endelige) udvidelser heraf tidligt viste sig at være nøglen til løsning af en lang række diophantiske problemer; for eksempel er det konkrete problem, som vi betragtede ovenfor, nøglen til forståelse af, hvilke naturlige tal,

der kan udtrykkes som sum af 2 kvadrater; således har man, at $p\mathcal{D} = \mathfrak{P}_1\mathfrak{P}_2 \Leftrightarrow p$ er sum af 2 kvadrater.

Det afgørende spørgsmål i denne forbindelse angår fortolkningen af udtrykket ‘tilsvarende’ ovenfor: Hvad skulle det overhovedet betyde, at opnå en ‘dekompositionslov’ for vilkårlige Galoisudvidelser af \mathbb{Q} ?; hvilken form kunne et svar overhovedet have? Nøglen til besvarelse af disse spørgsmål blev fundet i 1960’erne af R. P. Langlands, hvilket blev starten på diverse revolutionerende udviklinger omfattende blandt mange andre ting Taniyama-Shimura-formodningen og Wiles’ store arbejde. Lad os via det konkrete eksempel ovenfor se på kimen til disse udviklinger.

1.2. Højniveaufortolkning. Betragt igen det ovenstående konkrete eksempel. Galoisgruppen $G := \text{Gal}(L/\mathbb{Q})$ er cyklisk af orden 2; kald en frembringer for den c . Gruppen G er en kanonisk kvotient af \mathbb{Q} ’s absolutte Galoisgruppe: $\kappa: G_{\mathbb{Q}} \twoheadrightarrow G$. Lad igen p være et ulige primtal. Som i appendiks kan vi betragte en dekompositions- og inertigruppe over p : $I_p \trianglelefteq D_p \leq G_{\mathbb{Q}}$ og det tilhørende Frobeniuselement $\text{Fr}_p \in D_p/I_p$. Da p er uforgrenet i L , gælder $\kappa(I_p) = 1$, så det giver mening at tale om $\sigma_p := \kappa(\text{Fr}_p) \in G$; σ_p er da Frobeniuselement over p m.h.t. udvidelsen L/\mathbb{Q} , i.e. σ_p kan identificeres med den kanoniske frembringer for $\text{Gal}((\mathcal{O}_L/\mathfrak{P})/\mathbb{F}_p)$, hvor \mathfrak{P} er en primdivisor i $p\mathcal{D}$; denne frembringer er triviell, netop hvis $p\mathcal{D} = \mathfrak{P}_1\mathfrak{P}_2$ med $\mathfrak{P}_1 \neq \mathfrak{P}_2$, altså netop hvis $\chi(p) = 1$. Definerer vi en homomorfi $\varphi: G \rightarrow \mathbb{C}^{\times}$ ved $\varphi(c) = -1$, og betegner vi med ρ den sammensatte homomorfi:

$$(bb) \quad \rho: G_{\mathbb{Q}} \xrightarrow{\kappa} G \xrightarrow{\varphi} \mathbb{C}^{\times},$$

haves følgende omformulering af (b):

$$(bbb) \quad \rho(\text{Fr}_p) = \chi(p) .$$

Essensen af klasselegemeteori over \mathbb{Q} består i en generalisering af (bbb) til vilkårlige (endelige) cykliske udvidelser M/\mathbb{Q} : Givet en sådan og en indlejring af den cykliske gruppe $\text{Gal}(M/\mathbb{Q})$ i \mathbb{C}^{\times} , får vi en homomorfi $\rho: G_{\mathbb{Q}} \rightarrow \mathbb{C}^{\times}$ som ovenfor. Til M/\mathbb{Q} defineres et naturligt tal N kaldet føreren af M/\mathbb{Q} ; N har bl.a. den egenskab, at p er uforgrenet i M , hvis og kun hvis p ikke går op i N . For vores konkrete eksempel ovenfor er denne fælles fører $N = 4$.

Klasselegemeteoriens centrale udsagn består nu i konstruktion af en Dirichlet-karakter χ modulo N således, at (bbb) gælder for i M uforgrenede primtal p , med andre ord: For $p \nmid N$. Omvendt vises for given Dirichlet-karakter χ modulo N eksistensen af en homomorfi $\rho: G_{\mathbb{Q}} \rightarrow \mathbb{C}^{\times}$, der er uforgrenet over p for $p \nmid N$ således, at (bbb) gælder for $p \nmid N$.

Men hvorledes kunne man nu forestille sig en generalisering af relationen (bbb) til *ikke-abelske* Galoisudvidelser af \mathbb{Q} ? Et første, men afgørende konceptuelt skred består i et skift af fokus fra venstre- til højresiden af identiteten $\mathbb{C}^{\times} = \text{GL}_1(\mathbb{C})$ i forbindelse med (bb). Med andre ord: Vi opfatter ρ som en 1-dimensional kompleks *Galoisrepræsentation* $\rho: G_{\mathbb{Q}} \rightarrow \text{GL}_1(\mathbb{C})$. Som sådan har ρ en Artin-fører, som vi definerede i B.3; som nævnt i B.3 stemmer denne Artin-fører overens med den klasselegemeteoretiske fører; Artin-føreren af ρ er altså N . Følgelig kan vi - bringende

vores a_p fra 1 ovenfor ind i spillet igen - omskrive (bbb) til:

$$(h) \quad a_p = \text{Tr} \rho(\text{Fr}_p) = \chi(p) \quad , \text{ for } p \nmid N .$$

Den interessante fortolkning af (h) er følgende: Vi har givet en Galoisrepræsentation ρ , og interesserer os for sporene af $\rho(\text{Fr}_p)$ for m.h.t. ρ uforgrenede primtal p ; af Chebotarev's sætning B.2.1 kan man trække den konsekvens, at disse spor bestemmer repræsentationen ρ op til ækvivalens (i.e. op til konjugation med et element af $G_{\mathbb{Q}}$). Relationen (h) viser, at sporene af $\rho(\text{Fr}_p)$ er langt fra at være kaotisk fordelt, når p varierer: De 'kontrolleres' af et struktureret objekt, nemlig Dirichlet-karakteren χ . Den formodningsmæssige generalisering af (h), som blev udviklet af Langlands i 1960'erne, består i første omgang i at betragte højeredimensionale repræsentationer $\rho: G_{\mathbb{Q}} \rightarrow \text{GL}_n(\mathbb{C})$. Det oplagte spørgsmål er da, hvad man skulle forvente som generalisering af højresiden i (h), i.e. hvilke 'kontrolobjekter' kommer ind i spillet i stedet for χ , når $n > 1$?

I disse noter vil vi udelukkende være beskæftigede med tilfældet $n = 2$, og endda kun med specielle typer af 2-dimensionale repræsentationer; til gengæld rækker det for vores formål ikke kun at betragte *komplekse* Galoisrepræsentationer: Vi får også brug for ℓ -adiske og mod ℓ Galoisrepræsentationer (jfr. B.2). *Taniyama-Shimura-formodningen*, som er emnet for afsnit 3 nedenfor, vil fremstå som et udsagn af samme formelle struktur som (h). Men inden da må vi først indføre de korrekte 'kontrolobjekter', i.e. substitutterne for χ i denne nye sammenhæng. Dette er emnet for næste afsnit.

2. MODULFORMER OG GALOISREPRÆSENTATIONER.

Litteratur: [Miy], [Shi]
 [Ser77], [DS], [DDT], [Del], [Ser87]
 * [Maz77], [Car]

2.1. **Modulformer.** Betragt den såkaldte 'øvre halvplan'

$$\mathfrak{H} := \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}.$$

Gruppen $\text{GL}_2^+(\mathbb{R})$ virker på \mathfrak{H} ved:

$$\alpha.z := \frac{az + b}{cz + d}, \quad \text{for } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2^+(\mathbb{R}), \quad z \in \mathfrak{H} .$$

Lad nu $N, k \in \mathbb{N}$, lad $\chi: (\mathbb{Z}/\mathbb{Z}N)^{\times} \rightarrow \mathbb{C}$ være en Dirichlet-karakter, og betragt gruppen

$$\Gamma_0(N) := \left\{ \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\} ;$$

bemærk, at $\Gamma_0(1) = \text{SL}_2(\mathbb{Z})$. Vi har en af (k, χ) afhængig højrevirkning $|_{k, \chi}$ af $\Gamma_0(N)$ på holomorfe funktioner f på \mathfrak{H} via:

$$(f |_{k, \chi} \alpha)(z) := \chi(d)^{-1} \cdot (cz + d)^{-k} \cdot f\left(\frac{az + b}{cz + d}\right), \quad \text{for } \alpha \in \Gamma_0(N) ;$$

bemærk, at da $\alpha \in \text{SL}_2(\mathbb{Z})$ og $c \equiv 0 \pmod{N}$, haves $ad \equiv 1 \pmod{N}$, hvorfor d er invertibel modulo N , så $\chi(d)$ er defineret. Vi definerer: En *modulform af vægt k og nebentypus χ på $\Gamma_0(N)$* er en holomorf funktion f på \mathfrak{H} med følgende egenskaber:

$$(i) \quad f|_{k,\chi} \alpha = f, \quad \forall \alpha \in \Gamma_0(N),$$

og

$$(ii) \quad \exists \nu > 0: f(\tau) = O(\text{Im}(\tau)^{-\nu}) \quad \text{for } \text{Im}(\tau) \rightarrow 0+ \quad \text{uniformt m.h.t } \text{Re}(\tau).$$

Hvis f tilfredstiller (ii) med et $\nu \in]0, k[$, siges f at være en *spidsform*. En sådan modul- eller spidsform siges også at være *af type (N, k, χ)* ; man referer til de enkelte data N , k og χ som f 's *niveau*, *vægt* hhv. *nebentypus*. Man betegner det komplekse vektorrum bestående af modulformer hhv. spidsformer af vægt k og nebentypus χ på $\Gamma_0(N)$ med $M_k(N, \chi)$ hhv. $S_k(N, \chi)$. Hvis $\chi = 1$, skrives i reglen blot $M_k(N)$ hhv. $S_k(N)$. Rummene $M_k(N, \chi)$ og $S_k(N, \chi)$ kan vises at være *endelig-dimensionale*; beviset kan opnås v.h.j.a. formernes fortolkning som differentialformer i algebraisk-geometrisk forstand (se nedenfor).

Lad nu $f \in M_k(N, \chi)$. Da $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$, giver betingelsen (i) ovenfor, at $f(z+1) = f(z)$; med dette vises vækstbetingelsen (ii) at medføre eksistensen af en *Fourier-udvikling* af f

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}, \quad \text{for } z \in \mathfrak{H},$$

hvor a_n er komplekse tal, der naturligvis kaldes f 's Fourier-koefficienter. Hvis endda $f \in S_k(N, \chi)$, vises $a_0 = 0$. Her følger et par klassiske eksempler på modul- og spidsformer:

Eksempel 1: Det uendelige produkt

$$\Delta(z) := e^{2\pi i z} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z})^{24}$$

vises at konvergere absolut og uniformt på kompakte delmængder af \mathfrak{H} , så $\Delta(z)$ er en holomorf funktion på \mathfrak{H} . Den kan vises at være en spidsform af type $(1, 12, 1)$.

Eksempel 2: Rummet $S_2(11)$ kan vises at være 1-dimensionalt og frembragt af:

$$(\Delta(z)\Delta(11z))^{1/2} = e^{2\pi i z} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z})^2 \cdot (1 - e^{2\pi i \cdot 11 n z})^2.$$

Eksempel 3: Lad ℓ være et ulige primtal, og lad χ være en Dirichlet-karakter modulo ℓ med $\chi(-1) = -1$. Den uendelige række:

$$E_{1,\chi}(z) := 1 - \frac{2\ell}{\sum_{1 \leq a \leq \ell-1} \chi(a)a} \cdot \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi(d) \right) \cdot e^{2\pi i n z},$$

hvor $\chi(d)$ for $\ell|d$ skal fortolkes som 0, kan vises at definere en modulform af vægt 1 og nebentypus χ på $\Gamma_0(\ell)$. Denne form er et specielt eksempel på såkaldte

Eisenstein-rækker. Et specielt og vigtigt eksempel på formerne $E_{1,\chi}$ fås således: Der findes en Dirichlet-karakter ψ modulo ℓ med $\psi(-1) = -1$, således, at:

$$\psi(a)a \equiv 1 \pmod{\ell} \quad \text{for } a \in \mathbb{Z} \text{ med } \ell \nmid a ,$$

hvor kongruensen skal forstås således: værdierne $\psi(a)$ ligger i det algebraiske tallegeme $\mathbb{Q}(e^{\frac{2\pi i}{\ell}})$; kongruensen skal forstås som kongruens mellem algebraisk hele tal i dette legeme med ℓ en primplads i legemet over \mathbb{Q} . Det interessante ved den tilhørende Eisenstein-række $E_{1,\psi}$ er, at vi har kongruensen:

$$E_{1,\psi} \equiv 1 \pmod{\ell} ,$$

hvilken kongruens skal forstås 'ledvist', i.e., at der for $E_{1,\psi}$'s Fourier-koefficienter a_n gælder:

$$a_0 \equiv 1 \pmod{\ell} \text{ og } a_n \equiv 0 \pmod{\ell} \text{ for } n > 0.$$

At modul- og spidsformer i virkeligheden snarere er algebraisk-geometriske objekter end analytiske, hænger sammen med følgende omstændigheder: Ækvivalensklasserne af punkter i \mathfrak{H} m.h.t. virkningen af $\Gamma_0(N)$ kan vises at have en naturlig struktur som en ikke-kompakt Riemann-flade, kaldet den *affine modulkurve* $Y_0(N)$; videre: $Y_0(N)$ kan ved tilføjelse af endeligt mange punkter (mere præcist: ækvivalensklasserne af punkterne i $\mathbb{Q} \cup \{\infty\}$ m.h.t. den naturlige virkning af $\Gamma_0(N)$) kompaktificeres til en kompakt Riemann-flade kaldet modulkurven $X_0(N)$. En berømt sætning af Riemann siger, at en kompakt Riemann-flade er en projektiv algebraisk kurve over \mathbb{C} . For $X_0(N)$ kan der vises den yderst vigtige og ikke-trivielle sætning, at den som projektiv algebraisk kurve kan defineres over \mathbb{Q} , i.e. at $X_0(N)$ i sidste ende kan beskrives ved polynomiumsligninger med rationale koefficienter. Dette er en af grundene til - som vi skal se nedenfor -, at $X_0(N)$ og modulformer har noget at gøre med Galoisrepræsentationer over \mathbb{Q} , som jo er vores egentlige studieobjekter.

Vi angiver den algebraisk-geometriske fortolkning af begrebet 'spidsform' for vægt 2 og trivial nebentypus, i.e. for elementer $f \in S_2(N)$: Lad $a = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$. Man beregner, at:

$$d(a.z) = d\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) = (\gamma z + \delta)^{-2} dz ,$$

og definitionen af elementer i $M_2(N)$ viser derfor, at differentiallet $f(z)dz$ på \mathfrak{H} er *invariant* ved substitutionen $z \mapsto a.z$ for $a \in \Gamma_0(N)$; følgelig kan $f(z)dz$ opfattes som et differential på den affine kurve $Y_0(N)$. Man viser nu, at de vækstbetingelser, der karakteriserer spidsformer, i det foreliggende tilfælde er ækvivalente med at forlange, at $f(z)dz$ kan fortsættes til et holomorft differential på den projektive kurve $X_0(N)$. Rummet $S_2(N)$ er altså isomorft med rummet af holomorfe differentialer på en projektiv algebraisk kurve, hvilket eksempelvis implicerer $S_2(N)$'s endeligheddimensionalitet: $\dim_{\mathbb{C}} S_2(N)$ er *genus* af Riemann-fladen $X_0(N)$. Denne genus kan bestemmes ved ren topologisk analyse af $X_0(N)$, og en formel kan angives (som funktion af N). Eksempelvis fås:

Sætning 2.1.1. For primtalsniveau $N = p$ haves:

$$\dim_{\mathbb{C}} S_2(p) = \begin{cases} 0 & , \text{ for } p = 2 \\ \frac{p-13}{12} & , \text{ for } p \equiv 1 \pmod{12} \\ \frac{p-5}{12} & , \text{ for } p \equiv 5 \pmod{12} \\ \frac{p-7}{12} & , \text{ for } p \equiv 7 \pmod{12} \\ \frac{p+1}{12} & , \text{ for } p \equiv 11 \pmod{12} . \end{cases}$$

Tilsvarende fortolkninger og formler haves for spidsformer af højere, lige vægte; for ulige vægte stiller sagen sig en smule mere kompliceret, for vægt 1 endda overordentligt meget mere kompliceret.

2.2. Hecke-operatorer og Galoisrepræsentationer. Betragt rummet af spidsformer $S_k(N, \chi)$. Vi vil nu indføre de såkaldte *Hecke-operatorer* på $S_k(N, \chi)$. Den bedste definition af disse operatorer går via algebraisk geometri, hvilket vi dog af pladshensyn ikke kan gennemføre. Vi vælger en konkret definition via Fourier-udviklinger, hvilken i øvrigt stemmer overens med Hecke's oprindelige definition. Det skal dog nævnes, at beviserne for diverse sætninger om Hecke-operatorer, som vil forekomme nedenfor, bedst føres udfra det algebraisk-geometriske synspunkt.

Lad $f \in S_k(N, \chi)$ med Fourier-udvikling:

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

og lad p være et primtal. Vi definerer den holomorfe funktion $T_p f$ på \mathfrak{H} ved:

$$(T_p f)(z) := \sum_{n=1}^{\infty} a_{pn} e^{2\pi i n z} + \chi(p) p^{k-1} \sum_{n=1}^{\infty} a_n e^{2\pi i p n z},$$

hvor $\chi(p)$ for $p|N$ skal fortolkes som 0. Det vises, at $T_p f$ igen er et element i $S_k(N, \chi)$, så vi kan opfatte T_p som en lineær operator på dette rum. Bemærk, at *definitionen af T_p er afhængig af (N, k, χ)* , hvilket ikke fremgår af notationen.

Antag nu, at $f \neq 0$ er en simultan egenform for samtlige Hecke-operatorer T_p , i.e. at vi har:

$$T_p f = \lambda_p f \quad \text{for alle primtal } p,$$

hvor λ_p 'erne er visse komplekse tal. Det kan vises, at vi så fald har $a_1 \neq 0$, så vi kan gerne antage, at f er *normaliseret* således, at:

$$a_1 = 1;$$

Vi betegner sådanne former simpelthen som *normaliserede egenformer*. Det følger nu af definitionen af $T_p f$, at egenværdien λ_p stemmer overens med Fourier-koefficienten a_p og, at vi har følgende i første omgang formelle identitet:

$$(\#) \quad \sum_{n=1}^{\infty} a_n n^{-s} = \prod_{p \text{ primtal}} (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1},$$

hvor 'formel' betyder $a_n = b_n$, hvis man formelt ganger produktet i højresiden ud og skriver det på formen $\sum_{n=1}^{\infty} b_n n^{-s}$; denne formelle identitet kan således oversættes til en (uendelig) liste af rekursionsformler for Fourier-koefficienterne a_n . (Det var i øvrigt studiet af sådanne rekursionformler i forbindelse med visse klassiske konstruktioner af modulformer fra kvadratiske former, der foranledigede Hecke til indførelse af Hecke-operatorerne). Men (#) er langt mere en blot en formel identitet: I den klassiske teori for modulformer vises det, at (#) konvergerer absolut for $s \in \mathbb{C}$ med $\text{Re}(s) > k$, hvor den definerer en funktion $L(f, s)$, holomorf i dette område; defineres videre $\Lambda(f, s) := (2\pi/\sqrt{N})^{-s} \Gamma(s) L(f, s)$, da har $\Lambda(f, s)$ holomorf fortsættelse til hele den komplekse plan $s \in \mathbb{C}$, hvor den tilfredsstiller en funktionalligning, der i mistænkelig grad minder om funktionalligninger for L-rækkerne knyttede til visse typer af Galoisrepræsentationer. Lad os nu se, at dette ikke er noget tilfælde.

Sætning 2.2.1. (se f.eks. [Shi]) *Antag, at $k \geq 2$, og lad $f \in S_k(N, \chi)$ være en normaliseret egenform med Fourier-udvikling*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

Da er tallene a_n alle algebraisk hele tal i en (af n uafhængig) endelig udvidelse af \mathbb{Q} .

Sætning 2.2.2. (Deligne [Del], se også [Car]) *Antag, at $k \geq 2$, og lad $f \in S_k(N, \chi)$ være en normaliseret egenform med Fourier-udvikling*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

Da findes der til hvert primtal ℓ en kontinuert, irreducibel ℓ -adisk Galois-repræsentation:

$$\rho_{f,\ell}: G_{\mathbb{Q}} \longrightarrow \text{GL}_2(\mathfrak{O}_{\lambda}),$$

hvor \mathfrak{O}_{λ} er ringen af hele tal i en endelig udvidelse af \mathbb{Q}_{ℓ} , og med følgende egenskaber:

(i) *For $p \nmid N\ell$ er $\rho_{f,\ell}$ uforgrenet over p ,*

(ii) *$\text{Tr} \rho_{f,\ell}(\text{Fr}_p) = a_p$ for $p \nmid N\ell$,*

og

(iii) *$\det \rho_{f,\ell}(\text{Fr}_p) = \chi(p) p^{k-1}$ for $p \nmid N\ell$.*

Det kan vises, at $\rho_{f,\ell}$ har fører N (B.3).

Ved en første konfrontation med Sætning 2.2.2 kan denne forekomme overordentligt mystisk: Hvordan i alverden kommer man fra formen f til repræsentationen $\rho_{f,\ell}$? Denne mystificering er berettiget for såvidt, som den faktiske konstruktion er både kompliceret og afhængig af avanceret matematik. Den afgørende pointe er imidlertid den algebraisk-geometriske fortolkning af begrebet ‘spidsform’, som vi antydede ovenfor. I det følgende underafsnit giver vi - for tilfældet $k = 2$ - en antydning af, hvordan $\rho_{f,\ell}$ konstrueres.

2.2.1. *Antydning af konstruktion:* En *abelsk varietet* er en komplet gruppevarietet A , i.e. A er en komplet algebraisk varietet defineret over et eller andet grundlegeme K og forsynet med en ‘gruppetstruktur’: Hvis L/K er en legemsudvidelse, har mængden $A(L)$ af L -rationale punkter på A struktur af en gruppe, og tilordningen $L \mapsto A(L)$ er ‘funktoriel’. Det vises, at A er projektiv, og at gruppe-loven er abelsk (kommutativ), i.e. gruppen $A(L)$ er abelsk for hvert L .

Lad nu A være en abelsk varietet af dimension d defineret over \mathbb{Q} ; med andre ord: A kan beskrives ved polynomiumsligninger med rationale koefficienter. Betragt $A(\bar{\mathbb{Q}})$, dvs. a priori mængden af løsninger i algebraiske tal til de nævnte polynomiumsligninger; da A er en abelsk varietet, har $A(\bar{\mathbb{Q}})$ struktur af en abelsk gruppe. Lad ℓ være et primtal. For $m \in \mathbb{Z}$ definerer vi mængden $A[\ell^m]$ af ℓ^m -torsionspunkter for A som delmængden af punkter $P \in A(\bar{\mathbb{Q}})$ for hvilke

$$\ell^m \cdot P = 0 ,$$

hvor 0 betegner neutralelementet i $A(\bar{\mathbb{Q}})$ og $\ell^m \cdot$ betyder potensering med ℓ^m m.h.t. gruppestrukturen i $A(\bar{\mathbb{Q}})$. Øjensynligt er $A[\ell^m]$ en undergruppe af $A(\bar{\mathbb{Q}})$ og har en naturlig struktur som $\mathbb{Z}/\mathbb{Z}m$ -modul. Vi definerer videre mængden $A[\ell^\infty]$ af ℓ^∞ -torsionspunkter for A med en naturlig struktur som \mathbb{Z}_ℓ -modul ved:

$$A[\ell^\infty] := \varprojlim_m A[\ell^m] \otimes \mathbb{Z}_\ell .$$

For $A[\ell^\infty]$ som \mathbb{Z}_ℓ -modul har man følgende fundamentale sætning:

Sætning 2.2.3. $A[\ell^\infty] \cong (\mathbb{Z}_\ell)^{2d}$ som \mathbb{Z}_ℓ -modul.

Men vi har yderligere struktur på $A[\ell^\infty]$: Galoisgruppen $G_{\mathbb{Q}}$ virker på naturlig måde på $A(\bar{\mathbb{Q}})$: Hvis vi har en løsning (x_0, x_1, \dots) i algebraiske tal til de polynomiumsligninger, der definerer A , og har vi et $g \in G_{\mathbb{Q}}$, da vil øjensynligt $(g.x_0, g.x_1, \dots)$ igen være en løsning i algebraiske tal til de nævnte polynomiumsligninger, eftersom disse har *rationale* koefficienter. Man viser nu, at denne virkning respekterer gruppestrukturen i $A(\bar{\mathbb{Q}})$, specielt bringer den $A[\ell^\infty]$ ind i sig selv. Vi har altså en virkning af $G_{\mathbb{Q}}$ på $A[\ell^\infty]$. Sætning 2.2.3 siger nu, at denne virkning giver os en homomorfi:

$$\rho_{A,\ell}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_{2d}(\mathbb{Z}_\ell) ,$$

som vises at være kontinuert. $\rho_{A,\ell}$ er altså en ℓ -adisk Galoisrepræsentation; den kaldes passende for den ℓ -adiske repræsentation hørende til A .

Betragt nu modulkurven $X_0(N)$. Det er som nævnt en projektiv algebraisk varietet defineret over \mathbb{Q} . Som sådan har den en tilknyttet *Jacobi-varietet*, kaldet

$J_0(N)$, som er en abelsk varietet defineret over \mathbb{Q} . Som ovenfor kan vi betragte $J_0(N)[\ell^\infty]$ og får herfra repræsentationer af $G_{\mathbb{Q}}$. Betragtes nu Hecke-operatorerne hørende til rummet $S_2(N)$, kan det vises, at disse har en naturlig fortolkning (via ‘funktorialitet’) som endomorfier af $J_0(N)$; dette hænger sammen med den ovenfor omtalte fortolkning af elementerne i $S_2(N)$ som holomorfe differentialer på $X_0(N)$. Denne fortolkning af Hecke-operatorerne muliggør en bestemt type af spaltning af $J_0(N)[\ell^\infty]$, hvor de enkelte ‘stykker’ svarer til normaliserede egenformer $f \in S_2(N)$; denne spaltning udmøntes i sidste ende i en spaltning af Galoisrepræsentationen hørende til $J_0(N)[\ell^\infty]$ svarende igen til normaliserede egenformer $f \in S_2(N)$. Galoisrepræsentationen $\rho_{f,\ell}$ fra Sætning 2.2.2 konstrueres via denne proces. Det virkeligt hårde arbejde består så i at vise, at den således konstruerede repræsentation $\rho_{f,\ell}$ har egenskaberne angivet i Sætning 2.2.2.

Konstruktionen af $\rho_{f,\ell}$ i det tilfælde, hvor vægten k er større end 2, er noget mere abstrakt, da man ikke længere blot kan arbejde med $J_0(N)$: Der skal nogle noget mere abstrakte objekter ind i spillet (såkaldte ℓ -adiske kohomologigrupper). Set fra en højere synsvinkel er konstruktionen for vægte >2 dog analog til konstruktionen for $k = 2$.

2.3. Artin-formodningen. Det er ikke svært at gætte på en mulig version af Sætning 2.2.2 i tilfældet $k = 1$. Vanskeligheden består deri, at de ovenfor omtalte metoder til konstruktion af $\rho_{f,\ell}$ for vægte $k \geq 2$ bryder totalt sammen for vægt $k = 1$. Ikke desto mindre gælder der følgende bemærkelsesværdige sætning, hvis bevis vi ikke kan komme ind på; det skal dog nævnes, at beviset bl.a. *benytter* Sætning 2.2.2.

Sætning 2.3.1. (*Deligne-Serre [DS]*) *Lad $f \in S_1(N, \chi)$ være en normaliseret egenform med Fourier-udvikling*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

Da findes der en kontinuert, irreducibel Galoisrepræsentation

$$\rho_f: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{C}),$$

med følgende egenskaber:

(i) *For $p \nmid N$ er ρ_f uforgrenet over p ,*

(ii) *$\mathrm{Tr} \rho_f(\mathrm{Fr}_p) = a_p$ for $p \nmid N$,*

og

(iii) *$\det \rho_f(\mathrm{Fr}_p) = \chi(p)$ for $p \nmid N$.*

Men får vi ikke ℓ -adiske repræsentationer knyttet til f ? Jo, via en simpel konstruktion: Repræsentationen ρ_f har endeligt billede, og kan derfor realiseres over et algebraisk tallegeme K , i.e. vi kan opfatte ρ_f som en homomorfi:

$$\text{\#\#\#} \quad \rho_f: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(K),$$

der naturligvis har samme endelige billede som ρ_f . Er nu ℓ et primtal, kan repræsentationen $(\#\#)$ som bekendt gøres ‘ ℓ -adisk heltallig’, dvs. er ækvivalent med en repræsentation

$$\rho_{f,\ell}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathfrak{O}_{\lambda}),$$

med \mathfrak{O}_{λ} ringen af hele tal i en endelig udvidelse af \mathbb{Q}_{ℓ} . Repræsentationen $\rho_{f,\ell}$ har naturligvis billede isomorft med $\mathrm{Im}\rho_f$.

Vi har nu kørt tilstrækkeligt meget skyts i stilling til at kunne vende tilbage til diskussionen sidst i afsnit 1.2. Det spørgsmål, som man ønsker besvaret, er følgende: Vi har gennem sætningerne 2.2.2 og 2.3.1 via normaliserede egenformer fået konstrueret Galoisrepræsentationer; hvis vi vedtager at kalde disse konstruerede repræsentationer for *modulære* (de opstår fra *modul*-former), hvilke Galoisrepræsentationer er så modulære? Vi vil nu kort gå ind på dette spørgsmål i forbindelse med repræsentationerne fra sætning 2.3.1. Inden vi kan formulere den berømte *Artin-formodning* i denne forbindelse, skal vi have noteret os en lille, men vigtig egenskab ved repræsentationerne i sætningerne 2.2.2 og 2.3.1: Kompleks konjugering af algebraiske tal er øjensynligt en legemsautomorfi af $\bar{\mathbb{Q}}$, der fikserer \mathbb{Q} punktvis. Følgelig kan vi opfatte kompleks konjugering som et element $c \in G_{\mathbb{Q}}$; dette element har orden 2. Er nu ρ en repræsentation fra Sætning 2.2.2 eller 2.3.1, kan vi følgelig betragte $\rho(c)$; da $c^2 = 1$, haves $(\det \rho(c))^2 = 1$, altså

$$\det \rho(c) = \pm 1.$$

Definition: Repræsentationen ρ kaldes *ulige*, hvis $\det \rho(c) = -1$.

Sætning 2.3.2. *Samtlige repræsentationer, der forekommer i sætningerne 2.2.2 og 2.3.1 er ulige.*

Den følgende formodning ville være en delvis generalisering af klasselegemeteorien til studiet af 2-dimensionale, komplekse Galoisrepræsentationer, jfr. diskussionen sidst i afsnit 1.2.

Formodning: *Lad $\rho: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{C})$ være en irreducibel, ulige Galoisrepræsentation. Da er ρ modulær af vægt 1, i.e. der findes $((N, \chi)$ og) en normaliseret egenform $f \in S_1(N, \chi)$ således, at $\rho \cong \rho_f$, hvor ρ_f er repræsentationen fra Sætning 2.3.1.*

En stærkere version af denne formodning opnås ved at forlange, at (N, χ) kan vælges således, at N er Artin-føreren af ρ (appendiks B.3) og således, at χ via klasselegemeteorien svarer til $\det \rho: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_1(\mathbb{C})$, men det kan vises, at denne stærkere version følger af den svagere.

Det er blevet standard at kalde denne formodning for ‘Artin-formodningen’ (for irreducible, 2-dimensionale, komplekse, ulige Galoisrepræsentationer over \mathbb{Q}), idet den kan vises at være ækvivalent med en del af den i appendiks B.3 omtalte klassiske Artin-formodning.

Der følger nu en kort beskrivelse af, hvad der i øjeblikket er kendt om denne formodning.

Lad altså $\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{C})$ være en irreducibel, ulige repræsentation. Betragt den naturlige homomorfi $\mathrm{GL}_2(\mathbb{C}) \rightarrow \mathrm{PGL}_2(\mathbb{C})$, og lad os diskutere gruppen

$$G := \mathrm{Im} \left(G_{\mathbb{Q}} \xrightarrow{\rho} \mathrm{GL}_2(\mathbb{C}) \rightarrow \mathrm{PGL}_2(\mathbb{C}) \right) ;$$

da G således er en endelig undergruppe af $\mathrm{PGL}_2(\mathbb{C})$, har vi som bekendt a priori følgende muligheder for isomorfiklassen af G :

$$G \cong \begin{cases} C_n, & \text{den cykliske gruppe af orden } n \\ D_n, & \text{diedergruppen af orden } 2n \\ A_4, & \text{den alternerende gruppe på 4 symboler} \\ S_4, & \text{den symmetriske gruppe på 4 symboler} \\ A_5, & \text{den alternerende gruppe på 5 symboler} \end{cases},$$

men tilfældet $G \cong C_n$ er udelukket, da ρ i så fald ville være reducibel.

Formodningen ovenfor er bevist generelt i tilfældene, hvor G er isomorf med D_n , A_4 eller S_4 : I tilfældet $G \cong D_n$ kan påstanden i sidste ende (svært) føres tilbage til klasselegemeteorien, mens der i tilfældene A_4 og S_4 kræves en nyere fundamental (svær) teori, den såkaldte teori for cyklisk Base Change; beviserne i A_4 - og S_4 -tilfældene skyldes Langlands hhv. Tunnell, se [Lan] og [Tun]. Disse metoder virker ikke i tilfældet $G \cong A_5$, der derfor længe forekom at være en fuldstændigt uindtagelig bastion. Men et bevis for formodningen i A_5 -tilfældet (under visse tekniske indskrænkninger på ρ) er for nyligt (sommer 1999) blevet annonceret; dette sidstnævnte bevis bygger stadig på Wiles' fundamentalt nye og banebrydende ideer i disse problemkredse, men involverer også en længere række nye og højst komplicerede resultater, bl.a. angående såkaldt niveaureduktion.

2.4. Galoisrepræsentationer i positiv karakteristik og Serre's formodning.

Lad $\rho_{\ell}: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathfrak{O}_{\lambda})$ være enten en repræsentation fra Sætning 2.2.2 eller den ℓ -adiske repræsentation konstrueret fra en repræsentation ρ_f fra Sætning 2.3.1 som skitseret umiddelbart efter Sætning 2.3.1. Lad \mathfrak{M} være maksimalidealet i \mathfrak{O}_{λ} ; vi har altså, at $F := \mathfrak{O}_{\lambda}/\mathfrak{M}$ er en endelig udvidelse af \mathbb{F}_{ℓ} . Via den kanoniske homomorfi $\mathrm{GL}_2(\mathfrak{O}_{\lambda}) \rightarrow \mathrm{GL}_2(F)$ giver ρ_{ℓ} anledning til en mod ℓ repræsentation $\bar{\rho}_{\ell}$:

$$(\dagger) \quad \bar{\rho}_{\ell}: G_{\mathbb{Q}} \xrightarrow{\rho_{\ell}} \mathrm{GL}_2(\mathfrak{O}_{\lambda}) \rightarrow \mathrm{GL}_2(F),$$

som er ulige i samme forstand som i foregående afsnit. Betegner vi f 's Fourierkoefficienter med $a_n(f)$, og f 's niveau med N , er repræsentationen $\bar{\rho}_{\ell}$ øjensynligt uforgrenet over p , for $p \nmid N\ell$, og har følgende egenskab:

$$(\ddagger) \quad \mathrm{Tr} \bar{\rho}_{\ell}(\mathrm{Fr}_p) = (a_p(f) \bmod \mathfrak{l}) \quad , \text{ for } p \nmid N\ell ,$$

hvor \mathfrak{l} er et primideal over ℓ i et algebraisk tallegemes ring af hele algebraiske tal \mathfrak{O} , der er tilstrækkelig stor til at indeholde samtlige tal $a_n(f)$, og så $\mathfrak{O}/\mathfrak{l} \supseteq F$ (eksisterer ifølge Sætning 2.2.1).

Lad nu F/\mathbb{F}_{ℓ} være en endelig udvidelse, og lad

$$(\ddagger\ddagger) \quad \bar{\rho}_{\ell}: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(F)$$

være en vilkårlig, absolut irreducibel, ulige repræsentation.

Definition: Vi siger, at $\bar{\rho}_\ell$ er (mod ℓ) modulær, hvis der findes en normaliseret egenform f af en eller anden type (N, k, χ) og med Fourierkoefficienter $a_n(f)$ således, at $\bar{\rho}_\ell$ er uforgrenet over p , for $p \nmid N\ell$, og således, at (\dagger) gælder.

I 1987 formulerede J.-P. Serre i [Ser87] følgende bemærkelsesværdige og - på det pågældende tidspunkt - temmeligt dristige formodning:

Serre's formodning: Lad $\bar{\rho}_\ell$ være en absolut irreducibel, ulige repræsentation som i $(\dagger\dagger)$. Da er $\bar{\rho}_\ell$ (mod ℓ) modulær.

Grunden til, at vi i forbindelse med (\dagger) , definitionen ovenfor og Serre's formodning og i modsætning til Sætningerne 2.2.2 og 2.3.1 fokuserer i mindre grad på det $\bar{\rho}_\ell$ er følgende: I sætningerne 2.2.2 og 2.3.1, der jo omhandler karakteristik 0 repræsentationer, hænger det $\rho_{f,\ell}$ hhv. det ρ_f øjensynligt sammen med vægten k of f . Faktisk kan det vises, at data-triplet (N, k, χ) hørende til f er entydigt bestemt alene ved repræsentationerne $\rho_{f,\ell}$ hhv. ved ρ_f . Dette står i skarp kontrast til situationen i karakteristik ℓ : Er $\bar{\rho}_\ell$ som i $(\dagger\dagger)$ modulær, kan det vises, at der altid findes uendeligt mange mulige valg af såvel k som N ; vi vil se et eksempel på et sådant fænomen nedenfor. Ønsker man ikke desto mindre at betone et muligt valg af k og/eller N , siges $\bar{\rho}_\ell$ naturligvis at være mod ℓ modulær af vægt k hhv. af niveau N .

Serre's forfinede formodning - også formuleret i [Ser87] - er den ovenstående formodning plus en præcis angivelse af et muligt valg af data (N, k, χ) , der i en vis forstand er optimalt (minimalt). Vi for ikke brug for at formulere denne forfinede formodning i fuld generalitet, men vil dog senere se et specielt eksempel på, hvad dens indhold er.

I det følgende underafsnit vil vi se eksempler på mod 3 repræsentationer, der beviseligt er modulære.

2.4.1. *Nogle modulære mod 3 repræsentationer:* Lad i dette underafsnit $\bar{\rho}$ være en absolut irreducibel, ulige mod 3 Galoisrepræsentation:

$$\bar{\rho}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_3).$$

Lad os nu bemærke, at gruppen $\mathrm{PGL}_2(\mathbb{F}_3)$ som bekendt er isomorf med den symmetriske gruppe S_4 på 4 symboler. Gruppen $\mathrm{GL}_2(\mathbb{F}_3)$ har følgelig S_4 som kvotient. Mere præcist kan vi vise, at $\mathrm{GL}_2(\mathbb{F}_3)$ er isomorf med en såkaldt overdækningsgruppe \tilde{S}_4 af S_4 : Gruppen \tilde{S}_4 er som abstrakt gruppe givet ved frembringere a_1, a_2, a_3, z med definerende relationer:

$$(\clubsuit) \quad a_1^2 = a_2^2 = a_3^2 = z^2 = (a_1 a_2)^3 = (a_2 a_3)^3 = 1, \quad (a_1 a_3)^2 = z.$$

Elementet z er centralt i \tilde{S}_4 , og kvotienten $\tilde{S}_4 / \langle z \rangle$ er isomorf med S_4 ; vi har altså $|\tilde{S}_4| = 48$.

Man checker nu, at hvis vi betragter følgende matricer i $\mathrm{GL}_2(\mathbb{F}_3)$:

$$\alpha_1 := \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \quad \alpha_2 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \alpha_3 := \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad \zeta := \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

da tilfredstiller disse elementer $\alpha_1, \alpha_2, \alpha_3, \zeta$ relationerne (\clubsuit); vi har følgelig en surjektiv homomorfi $\tilde{S}_4 \rightarrow \mathrm{GL}_2(\mathbb{F}_3)$; eftersom $|\tilde{S}_4| = 48 = |\mathrm{GL}_2(\mathbb{F}_3)|$, følger

$$\mathrm{GL}_2(\mathbb{F}_3) \cong \tilde{S}_4 .$$

Betragt nu følgende matricer i $\mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \subseteq \mathrm{GL}_2(\mathbb{C})$ ($\mathbb{Z}[\sqrt{-2}]$ er ringen af hele algebraiske tal i det algebraiske tallegeme $\mathbb{Q}(\sqrt{-2})$):

$$A_1 := \begin{pmatrix} -\sqrt{-2} & -1 + \sqrt{-2} \\ -1 - \sqrt{-2} & \sqrt{-2} \end{pmatrix}, \quad A_2 := \begin{pmatrix} 1 & -1 - \sqrt{-2} \\ 0 & -1 \end{pmatrix},$$

$$A_3 := \begin{pmatrix} -2 & 1 + \sqrt{-2} \\ -1 + \sqrt{-2} & 2 \end{pmatrix}, \quad Z := \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix};$$

man checker, at disse matricer tilfredsstiller relationerne (\clubsuit); følgelig har vi en homomorfi

$$\sigma: \mathrm{GL}_2(\mathbb{F}_3) \longrightarrow \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \subseteq \mathrm{GL}_2(\mathbb{C}),$$

der kan ses at være injektiv. Sættningen

$$\rho := \sigma \circ \bar{\rho}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{C})$$

ses at være irreducibel, ulige, og med billede isomorft med $\mathrm{Im} \bar{\rho} \subseteq \mathrm{GL}_2(\mathbb{F}_3)$; da denne gruppe er isomorf med \tilde{S}_4 og således opløselig, er ρ *ikke* af A_5 -type. Det følger derfor af [resultaterne](#) omtalt sidst i afsnit 2.3, at ρ er modulær, i.e. knyttet til en normaliseret egenform af vægt 1 via Sætning 2.3.1. Man efterviser let, at ρ er et 'løft' af $\bar{\rho}$ i følgende forstand: Er \mathfrak{P} et primideal over 3 i $\mathbb{Z}[\sqrt{-2}]$, haves $\mathbb{Z}[\sqrt{-2}]/\mathfrak{P} \cong \mathbb{F}_3$; repræsentationen $\bar{\rho}$ er isomorf med mod \mathfrak{P} reduktionen af ρ , i.e. med

$$(\rho \bmod \mathfrak{P}): G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \longrightarrow \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]/\mathfrak{P}) \cong \mathrm{GL}_2(\mathbb{F}_3) .$$

Følgelig er $\bar{\rho} \bmod 3$ modulær af vægt 1. Vi får senere brug for at vide, at $\bar{\rho}$ også er mod 3 modulær af vægt 2, og antyder nu beviset for denne kendsgerning:

Da som nævnt ρ er modulær af vægt 1, er ρ Galoisrepræsentationen knyttet til en normaliseret egenform af vægt 1

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

via sætning 2.3.1. Betragt nu den specielle Eisenstein-række $E_{1,\psi}$ fra [eksempel 3](#) ovenfor i tilfældet $\ell = 3$: Konkret haves i dette tilfælde:

$$(\clubsuit\clubsuit) \quad E_{1,\psi}(z) = 1 + 6 \sum_{n=1}^{\infty} \left(\sum_{d|n} \psi(d) \right) e^{2\pi i n z} ,$$

hvor $\psi(x)$ er 0, 1, -1 for $x \equiv 0, 1, -1 \pmod{3}$, hhv. Da $E_{1,\psi}$ er en modulform af vægt 1, og da f er en spidsform af vægt 1, er $g(z) := E_{1,\psi}(z)f(z)$ en spidsform af vægt 2. Nu er g *ikke* en egenform, men det følger af [eksempel 3](#) eller direkte af ($\clubsuit\clubsuit$), at hvis

$$g(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z} ,$$

da gives

$$(\clubsuit\clubsuit\clubsuit) \quad b_n \equiv a_n \pmod{l}, \forall n,$$

hvor l er et primideal over 3 i en tilstrækkelig stor udvidelse af \mathbb{Q} . Af $(\clubsuit\clubsuit\clubsuit)$ og et 'løftningslemma' af Deligne og Serre (se [DS]) følger eksistensen af en normaliseret egenform

$$\tilde{g}(z) = \sum_{n=1}^{\infty} \tilde{b}_n e^{2\pi i n z}$$

af vægt 2 således, at

$$\tilde{b}_n (\equiv b_n) \equiv a_n \pmod{l}, \forall n;$$

ifølge definition er altså $\tilde{\rho}$ mod 3 modulær af vægt 2. Vi har altså følgende sætning:

Sætning 2.4.1. *Lad*

$$\tilde{\rho}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$$

være en absolut irreducibel, ulige Galoisrepræsentation. Da er $\tilde{\rho}$ mod 3 modulær af vægt 2.

2.5. Ribet's sætning. Lad i dette afsnit ℓ være ulige, og lad

$$\tilde{\rho}_{\ell}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_{\ell})$$

være en kontinuert (i.e.: $\mathrm{Im}\rho$ endelig), irreducibel, ulige Galoisrepræsentation, som antages at være mod ℓ modulær af vægt 2 og triviel nebentypus. Der findes altså en normaliseret egenform f af vægt 2 således, at $\tilde{\rho}_{\ell}$ er representationen konstrueret via sætning 2.2.2 og processen beskrevet i begyndelsen af afsnit 2.4. Lad N være f 's niveau. Som vi tidligere nævnte, er N ikke entydigt bestemt: Der kunne (og vil) findes en anden normaliseret egenform \tilde{f} af type $(M, 2, 1)$ og med $M \neq N$ således, at $\tilde{\rho}_{\ell}$ også er repræsentationen knyttet til \tilde{f} via den nævnte proces. Men vi kunne spørge efter det *minimale mulige* niveau, når vægten fastholdes. Som vi også tidligere nævnte, opstillede Serre i [Ser87] en præcis formodning om, hvad dette minimale niveau er. Vi vil i dette afsnit citere en for anvendelserne i forbindelse med Fermat's sidste sætning afgørende sætning af Ribet, der under visse omstændigheder beviser Serre's forudsigelse angående det minimale niveau; mere præcist giver Ribet's sætning tistrækkelige betingelser for at kunne 'fjerne' en primdivisor fra niveauet N :

Sætning 2.5.1. (Ribet, [Rib]). *Lad ℓ være ulige og antag, at $\tilde{\rho}_{\ell}$ er modulær af vægt 2, triviel nebentypus, og niveau N . Lad p være en primdivisor i N , og antag, at $p^2 \nmid N$. Antag yderligere, at enten*

(i) $\tilde{\rho}_{\ell}$ er uforgrenet over p ,

eller

(ii) $p = \ell$, og $\tilde{\rho}_{\ell}$ er flad over p .

Da er $\tilde{\rho}_{\ell}$ modulær af vægt 2, triviel nebentypus og niveau N/p .

Betingelsen i (ii) er en betingelse på restriktionen

$$(\bar{\rho}_\ell)_{D_p}, \quad D_p \subseteq G_{\mathbb{Q}} \text{ dekompositionsgruppe over } p,$$

af geometrisk natur. Den korrekte, tekniske definition på begrebet ‘flad over p ’ er at denne restriktion skal kunne udvides til et endeligt, fladt gruppeskema over \mathbb{Z}_p ; vi vil ikke gå ind på at forklare indholdet af denne definition, men vil dog nedenfor i forbindelse med mod ℓ Galoisrepræsentationer knyttede til elliptiske kurver over \mathbb{Q} se en anden og - for disse tilfælde - ækvivalent definition.

3. ELLIPTISKE KURVER OG TANIYAMA-SHIMURA-FORMODNINGEN.

Litteratur: [Sil86], [Har], [Ser87], [CSS], [DDT], [Shi]

* [Sil94], [CS]

3.1. Elliptiske kurver. En *elliptisk kurve over et legeme K* er en abelsk varietet af dimension 1 defineret over K . Vi vil i det følgende kun betragte tilfældene $K = \mathbb{Q}$ og $K = \mathbb{Q}_p$. En elliptisk kurve E over K kan vises at være givet ved en såkaldt *Weierstraß-ligning*:

$$(\diamond) \quad y^2 z + \alpha_1 x y z + \alpha_3 y z^2 = x^3 + \alpha_2 x^2 z + \alpha_4 x z^2 + \alpha_6 z^3,$$

hvor $\alpha_1, \alpha_3, \alpha_2, \alpha_4, \alpha_6 \in K$, i.e., E er isomorf med den projektive kurve i $\mathbb{P}^2(K)$ givet ved (\diamond) ; denne kurve har netop 1 punkt med $z = 0$, nemlig punktet $O := [0, 1, 0]$. Normalt vil man blot give E ved ligningen

$$y^2 + \alpha_1 x y + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6,$$

hvor det så er underforstået, at der skal tilføjes punktet O ‘i ∞ ’.

Weierstraß-ligningen (\diamond) er ikke entydigt bestemt ved E : Ved et variabelskift af typen

$$x' := u^2 x + r, \quad y' := u^3 y + u^2 s x + t,$$

hvor $r, s, t, u \in K$, $u \neq 0$, fås en ny Weierstraß-ligning, der dog definerer en kurve isomorf med E . Ikke desto mindre er det af interesse at knytte diverse tal til ligningen (\diamond) ; vi får især brug for den såkaldte *diskriminant* Δ , der defineres således: Sæt:

$$b_2 := \alpha_1^2 + 4\alpha_2, \quad b_4 := 2\alpha_4 + \alpha_1\alpha_3, \quad b_6 := \alpha_3^2 + 4\alpha_6,$$

$$b_8 := \alpha_1^2\alpha_6 + 4\alpha_2\alpha_6 - \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3^2 - \alpha_4^2;$$

da er:

$$\Delta := -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.$$

For en Weierstraß-ligning af den simple type

$$y^2 = x^3 + ax^2 + bx + c$$

er Δ simpelthen 16 gange diskriminanten af polynomiet på højresiden.

Er der omvendt givet en Weierstraß-ligning (\diamond) , vises det, at denne definerer en ikke-singular, projektiv kurve af genus 1 over K , og dermed en elliptisk kurve over K , hvis og kun hvis vi for ligningens diskriminant har $\Delta \neq 0$.

Antag nu, at E er defineret over \mathbb{Q}_p , og givet ved en ligning (\diamond) med $\alpha_i \in \mathbb{Q}_p$. Ved et passende **variabelskift** kan vi opnå, at $\alpha_i \in \mathbb{Z}_p$. I så fald har vi øjensynligt for den tilhørende diskriminant Δ , at

$$\nu_p(\Delta) \geq 0 ,$$

hvor ν_p som i appendiks A er den 'additive valuation' hørende til \mathbb{Q}_p , i.e. konkret:

$$\nu_p(\Delta) = s , \text{ hvis } \Delta = p^s u \text{ med } u \text{ en enhed i } \mathbb{Z}_p .$$

Vi kan derfor definere en *minimal Weierstraß-ligning* for E som en Weierstraß-ligning, der minimaliserer størrelsen $\nu_p(\Delta)$. Er Δ diskriminanten for en minimal Weierstraß-ligning, kan vi altså også definere størrelsen

$$(\spadesuit) \quad \Delta_{\min}(E) := p^{\nu_p(\Delta)} .$$

Antag så, at E er defineret over \mathbb{Q} . For hvert primtal p kan vi - via indlejringen $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ - opfatte E som en elliptisk kurve E/\mathbb{Q}_p over \mathbb{Q}_p , og har hertil knyttet størrelsen $\Delta_{\min}(E/\mathbb{Q}_p)$ givet ved (\spadesuit); det kan vises, at denne størrelse er 1 for alle pånær endeligt mange p ; derfor giver følgende definition - som vi nedenfor vil se formålet med - mening:

Definition: E 's *minimale diskriminant* $\Delta_{\min}(E)$ defineres ved:

$$\Delta_{\min}(E) := \prod_{p \text{ primtal}} \Delta_{\min}(E/\mathbb{Q}_p) .$$

3.2. Elliptiske kurver og Galoisrepræsentationer. I. Lad E være en elliptisk kurve defineret over \mathbb{Q} . Da E er en abelsk varietet af dimension 1 defineret over \mathbb{Q} , har vi - som skildret i afsnit 2.2.1 - for hvert primtal ℓ en kontinuert ℓ -adisk Galoisrepræsentation:

$$\rho_{E,\ell}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_{\ell}) .$$

Bringes den algebraiske geometri mere dybtgående ind i spillet, kan repræsentationen $\rho_{E,\ell}$ vises at have følgende egenskaber: Den er irreducibel, uforgrenet over alle pånær endeligt mange primtal p , og **ulige**; den har en fører (se B.3), der kan vises at være uafhængig af ℓ den forstand, at den er konstant lig et vist naturligt tal N_E , når blot ℓ er tilstrækkelig stor (afhængigt af E); mere præcist stemmer N_E op til en potens af ℓ overens med føreren af $\rho_{E,\ell}$. Vi definerer E 's fører som dette *naturlige tal* N_E . Repræsentationen $\rho_{E,\ell}$ er uforgrenet over p , netop hvis $p \nmid N_E \ell$.

Videre kan det vises, at vi for m.h.t. $\rho_{E,\ell}$ uforgrenede primtal p - altså for $p \nmid N_E \ell$ - har:

$$\det \rho_{E,\ell}(\mathrm{Fr}_p) = p ,$$

og

$$a_p := \mathrm{Tr} \rho_{E,\ell}(\mathrm{Fr}_p) = p + 1 - \#E(\mathbb{F}_p) ;$$

her betyder $\#E(\mathbb{F}_p)$ 'antallet af punkter på E over \mathbb{F}_p ', hvilket konkret er følgende: Vælg en minimal **Weierstraß-ligning** for E over \mathbb{Q}_p med $\alpha_i \in \mathbb{Z}_p$; det giver da mening at reducere denne ligning modulo p , i.e. at reducere hver af koefficienterne

α_i modulo p ; vi får en Weierstraß-ligning over legemet \mathbb{F}_p ; det kan vises, at denne for $p \nmid N_E \ell$ definerer en elliptisk kurve over \mathbb{F}_p ; $\#E(\mathbb{F}_p)$ er antallet af \mathbb{F}_p -rationale punkter på denne kurve, i.e. antallet af løsninger - projektivt talt - over \mathbb{F}_p til denne Weierstraß-ligning.

Vi kan nu i sammenhæng med repræsentationen $\rho_{E,\ell}$ vende tilbage til den problemkreds, der optog os i afsnit 1, mere specielt til de vage spørgsmål, som vi stillede sidst i afsnit 1.2: Vi havde der at gøre med en 1-dimensional kompleks Galois-repræsentation ρ og fortolkede klasselgemeteorien som et udsagn om, at sporene $\text{Tr}\rho(\text{Fr}_p)$ 'kontrolleres' af et struktureret objekt, nemlig en Dirichlet-karakter, jfr. relationen (h); i afsnit 2.3 havde vi at gøre med 2-dimensionale, irreducible, komplekse, ulige Galoisrepræsentationer ρ og fik udtalt formodningen, at sporene i disse tilfælde kontrolleres af spidsformer af vægt 1. Det spørgsmål, der nu stilles er naturligvis spørgsmålet efter et 'kontrolobjekt' i forbindelse med den ℓ -adiske repræsentation $\rho_{E,\ell}$ hørende til E . Sammenholder man de egenskaber for $\rho_{E,\ell}$, som vi opsummerede ovenfor, med sætning 2.2.2, er det ikke svært at gætte på følgende formodning, som er en mulig formulering af den berømte *Taniyama-Shimura-formodning*:

Taniyama-Shimura-formodningen: Lad E være en elliptisk kurve defineret over \mathbb{Q} . Da findes der et primtal ℓ og en normaliseret egenform f af vægt 2 således, at

$$\rho_{E,\ell} \cong \rho_{f,\ell} ,$$

hvor $\rho_{f,\ell}$ er Galoisrepræsentationen hørende til f fra sætning 2.2.2.

I denne forbindelse synes følgende definitioner relevante:

Definition: Lad $\rho_\ell: G_{\mathbb{Q}} \rightarrow \text{GL}_2(K)$ med K en endelig udvidelse af \mathbb{Q}_ℓ være en kontinuert, irreducibel, ulige ℓ -adisk Galoisrepræsentation. Vi siger, at ρ_ℓ er *modulær af vægt 2*, hvis der findes en normaliseret egenform f af type $(N, 2, 1)$ således, at

$$\rho_\ell \cong \rho_{f,\ell} .$$

Ønskes f 's niveau N betonet, siger vi, at ρ_ℓ er modulær (af vægt 2 og) niveau N .

Definition: Den elliptiske kurve E over \mathbb{Q} siges at være *modulær*, hvis repræsentationen $\rho_{E,\ell}$ er modulær af vægt 2 for et eller andet ℓ .

Taniyama-Shimura-formodningen siger således simpelthen, at enhver elliptisk kurve over \mathbb{Q} er modulær. Det kan være nyttigt at notere sig følgende sætning, der ikke er svært at bevise:

Sætning 3.2.1. *Lad E være en elliptisk kurve over \mathbb{Q} med fører N_E . Da er følgende betingelser ækvivalente:*

- (i) E er modulær.
- (ii) For ethvert primtal ℓ er $\rho_{E,\ell}$ modulær af vægt 2.
- (iii) For ethvert primtal ℓ er $\rho_{E,\ell}$ modulær af vægt 2 og niveau N_E .

Der findes andre (naturligvis med ovenstående ækvivalente) formuleringer af Taniyama-Shimura-formodningen, som er af mere algebraisk-geometrisk natur, men vi går ikke ind på disse.

Det for talteorien helt revolutionerende i Wiles' og Taylor's store arbejde ([Wil], [TW]) er *ikke* så meget beviset for den set ud fra en nøgtern synsvinkel relativt uvigtige Fermat's sidste sætning, men derimod, at disse arbejder giver et bevis for Taniyama-Shimura-formodningen under visse indskrænkende, men relativt milde tekniske betingelser på E , som vi går nærmere ind på nedenfor. For ganske nyligt (sommer 1999) er et bevis for Taniyama-Shimura-formodningen uden nogen indskrænkninger blevet annonceret af Breuil, Conrad, Diamond og Taylor [BCDT]; den fundamentale grundsten for dette bevis er stadig Wiles' gennembrud [Wil], og det går - startende med dette gennembrud - igennem adskillige etaper, hvor betingelserne på E gradvist svækkes. En af etaperne er eksempelvis arbejdet [CDT].

Det vigtige for talteorien er, at Taniyama-Shimura-formodningen og Wiles' nye fundamentale ideer giver et bidrag til at komme videre med de meget generelle spørgsmål, som vi antydede i slutningen af afsnit 1.2: Hele spillet går ud på - som generalisering af klasselegemeteorien - at finde 'reciprocitetslove' for meget generelle klasser af enten komplekse eller ℓ -adiske Galoisrepræsentationer (især for sådanne, der er af algebraisk-geometrisk oprindelse). Den generelle filosofi udviklet oprindeligt af Langlands i 1960'erne er, at sådanne reciprocitetslove bør tage form af en bestemt type af associering mellem Galoisrepræsentationer og såkaldte automorfe former: Eksempler på, hvad der menes denne 'associering' får vi fra afsnit 1.2: Dirichlet-karakterer er 'automorfe former på GL_1 ', fra afsnit 2.3 i forbindelse med Artin-formodningen, og fra ovenstående definition af modulære ℓ -adiske Galoisrepræsentationer: Modulformer er 'automorfe former på GL_2 '.

Langlands' ideer er idag blevet udmøntet i et præcist og ganske overvældende formodningssystem i hvilket eksempelvis Artin-formodningen og Taniyama-Shimura-formodningen blot er små specialtilfælde.

3.3. Elliptiske kurver og Galoisrepræsentationer. II. Lad igen E være en elliptisk kurve defineret over \mathbb{Q} , og lad os atter for primtal ℓ betragte de ℓ -adiske repræsentationer

$$\rho_{E,\ell}: G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_{\ell})$$

knyttet til E . Via den kanoniske homomorfi $\mathbb{Z}_{\ell} \rightarrow \mathbb{F}_{\ell}$ giver repræsentationerne $\rho_{E,\ell}$ anledning til mod ℓ repræsentationer knyttet til E :

$$\bar{\rho}_{E,\ell}: G_{\mathbb{Q}} \xrightarrow{\rho_{E,\ell}} GL_2(\mathbb{Z}_{\ell}) \longrightarrow GL_2(\mathbb{F}_{\ell}) .$$

Lad p være et primtal, og betragt som i 3.2 en over \mathbb{Q}_p minimal Weierstraß-ligning

$$y^2z + \alpha_1xyz + \alpha_3yz^2 = x^3 + \alpha_2x^2z + \alpha_4xz^2 + \alpha_6z^3, \quad \alpha_i \in \mathbb{Z}_p .$$

Vi skal nu interessere os lidt mere dybtgående for denne lignings opførsel under reduktion modulo p . Vi betragter altså den reducerede ligning:

$$(\mathfrak{X}) \quad y^2z + \bar{\alpha}_1xyz + \bar{\alpha}_3yz^2 = x^3 + \bar{\alpha}_2x^2z + \bar{\alpha}_4xz^2 + \bar{\alpha}_6z^3 ,$$

hvor $\bar{\alpha}_i \in \mathbb{F}_p$ er reduktionen af $\alpha_i \in \mathbb{Z}_p$ modulo p . Vi opfatter (\mathfrak{X}) som definerende en projektiv kurve C_p over \mathbb{F}_p . For C_p haves følgende 3 muligheder:

- (i) C_p er uden singulariteter (og definerer derfor en elliptisk kurve over \mathbb{F}_p),
- (ii) C_p har en singularitet, som er et dobbeltpunkt,
- (iii) C_p har en singularitet, som er en spids.

Definition: Svarende til tilfældene (i), (ii) og (iii) for C_p siges E at have *god*, *multiplikativ hhv. additiv reduktion* over p .

E kaldes *semistabil* over p , hvis E har god eller multiplikativ reduktion over p . E kaldes *semistabil*, hvis den er semistabil over p for ethvert primtal p .

Er E givet konkret ved en Weierstraß-ligning, findes der en algoritme, der for givet p bestemmer en minimal Weierstraß-ligning over \mathbb{Q}_p og dermed også fører til en bestemmelse af E 's reduktionstype over p .

Det afgørende for os er nu, at E 's reduktionstype over et givet p siger noget om egenskaberne for restriktionerne til en dekompositionsgruppe over p af Galoisrepræsentationerne $\rho_{E,\ell}$ og $\bar{\rho}_{E,\ell}$. Mere præcist viser den dyberegående aritmetisk-geometriske teori for elliptiske kurver følgende sætning.

Sætning 3.3.1. *Lad E være en elliptisk kurve over \mathbb{Q} med fører*

$$N_E = \prod_{p \text{ primtal}} p^{\gamma_p} ,$$

minimal diskriminant $\Delta_{\min}(E)$, og tilhørende Galoisrepræsentationer $\rho_{E,\ell}$ og $\bar{\rho}_{E,\ell}$ for primtal ℓ . Da gælder følgende.

$$(a) \gamma_p = \begin{cases} 0 & , \text{ hvis og kun hvis } E \text{ har god reduktion over } p \\ 1 & , \text{ hvis og kun hvis } E \text{ har multiplikativ reduktion over } p \end{cases}$$

(b) *Antag, at E har multiplikativ reduktion over p . For $\ell \neq p$ er da $\bar{\rho}_{E,\ell}$ ufor-grenet over p , hvis og kun hvis $\ell | \nu_p(\Delta_{\min}(E))$ (med ν_p som ovenfor den additive p -adiske valuation på \mathbb{Q} , i.e. $\nu_p(a) =$ eksponenten af p i primfaktoriseringen af a).*

(c) *Antag, at E har multiplikativ reduktion over p . Da er $(\bar{\rho}_{E,p})$ flad over p , hvis og kun hvis $p | \nu_p(\Delta_{\min}(E))$.*

Som vi nævnte ovenfor er repræsentationen $\rho_{E,\ell}$ altid irreducibel. Dette gælder imidlertid ikke altid for $\bar{\rho}_{E,\ell}$. Hvad angår dette spørgsmål har man følgende 'big theorem', der skyldes Mazur; vi får i det følgende kun brug for udsagnet (c).

Sætning 3.3.2. *(Mazur, [Maz78], [Maz77]). Lad E være en elliptisk kurve over \mathbb{Q} . Da gælder følgende.*

- (a) *Hvis $\ell > 163$, er $\bar{\rho}_{E,\ell}$ absolut irreducibel.*
- (b) *Hvis E er semistabil og $\ell > 7$, er $\bar{\rho}_{E,\ell}$ absolut irreducibel.*
- (c) *Hvis E er semistabil, $\bar{\rho}_{E,2}$ er triviel, og $\ell > 3$, da er $\bar{\rho}_{E,\ell}$ absolut irreducibel.*

3.4. **Wiles' sætning.** Vi kan nu formulere Wiles' store sætning angående Taniyama-Shimura-formodningen.

Sætning 3.4.1. (*Wiles, Taylor-Wiles, [Wil], [TW]*) *Lad E være en semistabil elliptisk kurve over \mathbb{Q} . Da er E modulær.*

Vi giver nu en meget kortfattet beskrivelse af (superstrukturen af) strategien for beviset for denne sætning: Lad E være en **semistabil** elliptisk kurve over \mathbb{Q} og betragt Galoisrepræsentationen

$$\bar{\rho}_{E,3}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_3) .$$

Nu er denne repræsentation *ikke* nødvendigvis (absolut) irreducibel, men beviset for 3.4.1 reduceres i [Wil] ved hjælp af et bestemt trick til tilfældet, hvor den er det. Vi antager altså, at $\bar{\rho}_{E,3}$ er absolut irreducibel. Som vi tidligere har bemærket, er denne repræsentation **ulige**. Af sætning 2.4.1 følger derfor:

$$\bar{\rho}_{E,3} \text{ er modulær af vægt } 2.$$

Der findes altså en normaliseret egenform f af vægt 2 (og triviell nebentypus) således, at

$$(\text{Y}) \quad \bar{\rho}_{E,3} \cong \bar{\rho}_{f,3} ,$$

hvor $\bar{\rho}_{f,3}$ er den modulære mod 3 repræsentation opnået ved mod 3 reduktion af den 3-adiske modulære repræsentation

$$\rho_{f,3}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathfrak{O}) ,$$

\mathfrak{O} ringen af hele tal i en endelig udvidelse af \mathbb{Q}_3 . Det næste skridt er nu fra (Y) at slutte, at $\rho_{E,3}$ er **modulær**, hvilket ifølge definition giver E 's modularitet. Modulariteten af $\rho_{E,3}$ opnås via etableringen af et princip ('Mazur's princip') - og dette er den virkelig afgørende og hårde kerne i Wiles' arbejde -, der groft udtrykt siger følgende:

Betragt en absolut irreducibel, ulige mod ℓ Galoisrepræsentation

$$\bar{\rho}_{\ell}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_{\ell}) ,$$

med ℓ et ulige primtal. Vi betragter ℓ -adiske 'løft' af $\bar{\rho}_{\ell}$, dvs. repræsentationer

$$\rho_{\ell}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathfrak{O}) ,$$

\mathfrak{O} ringen af hele tal i en endelig udvidelse af \mathbb{Q}_{ℓ} , der reducerer til $\bar{\rho}_{\ell}$ via den kanoniske homomorfi $\mathfrak{O} \rightarrow (\text{restklasselegeme})$. 'Mazur's princip' er da et princip, der groft sagt siger: 'Hvis $\bar{\rho}_{\ell}$ har 1 modulært ℓ -adisk løft af vægt 2, da er ethvert ℓ -adisk løft (med cyklotomisk determinant) modulært af vægt 2'. Det er et udsagn af denne type, som Wiles (komplementeret af Taylor-Wiles i [TW]) under visse tekniske betingelser på $\bar{\rho}_{\ell}$ beviser i [Wil].

Anvendelsen på $\bar{\rho}_{E,3}$ ovenfor er nu klar: Denne mod 3 repræsentation har ifølge (Y) et modulært 3-adisk løft, nemlig $\rho_{f,3}$. Anvendes 'Mazur's princip' på $\bar{\rho}_{E,3}$, fås derfor modulariteten af $\rho_{E,3}$ og dermed af E . Det er i forbindelse med anvendelsen på $\bar{\rho}_{E,3}$ af den version af Mazur's princip, som Wiles beviser i [Wil],

at semistabilitets-forudsætningen på E kommer ind i spillet: Denne bruges til at sikre, at $\bar{\rho}_{E,3}$ opfylder de ovenfor omtalte tekniske betingelser.

4. FERMAT'S SIDSTE SÆTNING.

Litteratur: [CSS], [DDT], [Ser87], [Sil86]

* [Dia96], [Wil], [TW], [Dia97], [Fre86], [Fre89]

4.1. **Frey-kurver.** Frey's geniale ide i [Fre86] og [Fre89] var, at ternære Diofantiske ligninger af den formelle form

$$(\S) \quad A + B = C$$

kan analyseres ved at studere aritmetikken af en vis elliptisk kurve knyttet til (§): Lad A, B, C være parvist primiske hele tal med (§), og betragt Weierstraß-ligningen

$$(\S\S) \quad y^2 = x(x - A)(x + B) .$$

Man beregner, at diskriminanten af (§§) er:

$$\Delta = 16(ABC)^2 ,$$

så hvis $ABC \neq 0$, definerer (§§) en elliptisk kurve $E_{A,B,C}$ over \mathbb{Q} .

Antages det yderligere, at $A \equiv -1 \pmod{4}$ og $B \equiv 0 \pmod{16}$, kan det vises, at $E_{A,B,C}$ har følgende globalt minimale Weierstraß-ligning ('globalt' betyder, at den er minimal over \mathbb{Q}_p for ethvert p):

$$y^2z + xyz = x^3 + \frac{B - A - 1}{4}x^2z - \frac{AB}{16}xz^2 ,$$

hvoraf beregnes, at

$$\Delta_{\min}(E_{A,B,C}) = 2^{-8}(ABC)^2 ,$$

og under brug af hvilken man kan bevise, at $E_{A,B,C}$ er *semistabil* medfører

$$N_{E_{A,B,C}} = \prod_{\substack{p \text{ primtal} \\ p|ABC}} p .$$

Af Wiles' sætning 3.4.1 følger derfor, at $E_{A,B,C}$ er *modulær*.

Vi får desuden brug for at vide, at repræsentationen $\bar{\rho}_{E_{A,B,C},2}$ er trivial: Dette følger af, at denne repræsentation er defineret (se afsnit 2.2.1) via virkningen af $G_{\mathbb{Q}}$ på de 4 punkter P på $E_{A,B,C}$ med algebraiske koordinater, som tilfredsstiller $2 \cdot P = 0$ m.h.t. gruppestrukturen på $E(\bar{\mathbb{Q}})$, og fordi man ved, at disse 4 punkter for en elliptisk kurve af den specielle form (§§) er 'punktet i ∞ ' samt de 3 punkter med affine koordinater $(0, 0)$, $(0, A)$ og $(0, -B)$. Da de 4 punkter således har *rationale* koordinater, er virkningen af $G_{\mathbb{Q}}$ på dem trivial, hvoraf det ønskede.

Vi opsummerer i følgende sætning:

Sætning 4.1.1. *Lad A, B, C være parvist primiske hele tal med*

$$A + B = C , \quad ABC \neq 0 , \quad A \equiv -1 \pmod{4} , \quad B \equiv 0 \pmod{16} ,$$

og betragt den elliptiske kurve $E_{A,B,C}$ over \mathbb{Q} givet ved ligningen

$$y^2 = x(x - A)(x + B) .$$

Da er $E_{A,B,C}$ semistabil og følgelig ifølge Wiles' sætning 3.4.1 modulær. Vi har

$$\Delta_{\min}(E_{A,B,C}) = 2^{-8}(ABC)^2, \quad N_{E_{A,B,C}} = \prod_{\substack{p \text{ primtal} \\ p|ABC}} p,$$

og repræsentationen $\bar{\rho}_{E_{A,B,C},2}$ er triviel.

4.2. Fermat's sidste sætning. Lad ℓ være et ulige primtal og antag, at a, b, c er hele tal med

$$a^\ell + b^\ell = c^\ell.$$

Fermat's sidste sætning er da udsagnet, at vi i så fald må have $abc = 0$. Vi antager derfor, at $abc \neq 0$, og søger at opnå en modstrid. Allerede fra Fermat selv ved vi da, at vi må have $\ell > 3$. Øjensynligt kan vi gerne antage, at a, b, c er parvist primiske, og via eventuelt fortegnsskift og/eller permutation af a, b, c yderligere, at $a \equiv -1 \pmod{4}$ og, at b er lige. Da $\ell > 3$, fås derfor $b^\ell \equiv 0 \pmod{16}$. Hvis vi derfor betragter Frey-kurven $E_{A,B,C}$ fra foregående afsnit i tilfældet:

$$A = a^\ell, \quad B = b^\ell, \quad C = c^\ell,$$

er forudsætningerne i sætning 4.1.1 opfyldte: Sæt

$$E := E_{a^\ell, b^\ell, c^\ell};$$

da er E semistabil, modulær, har minimal diskriminant

$$(\$) \quad \Delta_{\min}(E) = 2^{-8}(abc)^{2\ell},$$

og fører

$$(\$ \$) \quad N_E = \prod_{\substack{p \text{ primtal} \\ p|abc}} p.$$

Vi ønsker at studere mod ℓ Galoisrepræsentationen

$$\bar{\rho}_{E,\ell}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell),$$

som er mod ℓ reduktionen af den ℓ -adiske repræsentation

$$\rho_{E,\ell}: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell),$$

der er modulær af vægt 2, fordi E er modulær (se sætning 3.2.1). Der findes altså en normaliseret egenform f af vægt 2 og triviel nebentypus således, at

$$\rho_{E,\ell} \cong \rho_{f,\ell}.$$

Ifølge sætning 3.2.1, kan vi antage, at f har niveau N_E , der ifølge (§§) er kvadratfrit. Det følger, at $\bar{\rho}_{E,\ell}$ er (mod ℓ) modulær af type $(N_E, 2, 1)$. Lad nu p være en ulige primdivisor i N_E . Vi påstår på grundlag af Ribet's sætning 2.5.1, at $\bar{\rho}_{E,\ell}$ er modulær af type $((N_E)/p, 2, 1)$: Da $p|N_E$, er p en primdivisor i abc , så p går op i $\Delta_{\min}(E)$. Af (§) følger, at eksponenten af p i primfaktoriseringen af $\Delta_{\min}(E)$ er delelig med ℓ :

$$\nu_p(\Delta_{\min}(E)) = \nu_p((abc)^{2\ell}) = 2\ell \cdot \nu_p(abc) \equiv 0 \pmod{\ell}.$$

Af sætning 3.3.1 følger derfor:

$$\bar{\rho}_{E,\ell} \text{ er uforgrenet over } p, \text{ hvis } p \neq \ell,$$

og

$$\bar{\rho}_{E,\ell} \text{ er flad over } p, \text{ hvis } p = \ell.$$

Med disse oplysninger kan vi da af Ribet's sætning 2.5.1 - idet N_E er kvadratfrit - slutte, at $\bar{\rho}_{E,\ell}$ er modulær af vægt 2, triviel nebentypus og niveau $(N_E)/p$. Da vi kan gentage argumentet for en eventuel ulige primdivisor i $(N_E)/p$ følger:

$$\bar{\rho}_{E,\ell} \text{ er modulær af vægt 2, triviel nebentypus og niveau 2 ;}$$

der findes følgelig en normaliseret egenform $g \in S_2(2)$, der giver anledning til $\bar{\rho}_{E,\ell}$ via sætning 2.2.2 og reduktion modulo ℓ ; da en normaliseret egenform ikke er 0, slutter vi følgelig

$$\dim_{\mathbb{C}} S_2(2) \neq 0 ,$$

hvilket imidlertid strider mod sætning 2.1.1. Q.E.D.

Appendiks. Et par grundbegreber fra algebraisk talteori.

Dette appendiks er et højst koncentreret kompendium over nogle essentielle begreber og resultater fra den algebraiske talteori til brug for læsere uden baggrund i denne teori.

Lad i det følgende K være et algebraisk tallegeme, i.e. en endelig udvidelse af de rational tal \mathbb{Q} .

APPENDIX A. VALUATIONER.

En (ikke-triviel) *valuation* v på et legeme F er en ikke-konstant homomorfi $v: F^\times \rightarrow \mathbb{R}_+^\times$ med

$$v(x + y) \leq v(x) + v(y) \quad \text{for } x + y \neq 0.$$

Man udvider definitionen af v til hele F ved at sætte $v(0) := 0$. Man får da fra v en metrik d_v på F ved at sætte $d_v(x, y) := v(x - y)$; metrikken d_v giver F struktur af et topologisk legeme; 2 valuationer kaldes *ækvivalente*, hvis de inducerede topologier på F stemmer overens.

Lad nu $F = K$. Ved en *primplads* i K forstås en ækvivalensklasse af valuationer på K . De begreber/strukturer, der i det følgende indføres for valuationer, stemmer enten overens, eller er naturligt isomorfe for ækvivalente valuationer, hvorfor man ikke finder anledning til at skelne skarpt mellem en valuation og den ækvivalensklasse, den er medlem af. Lad altså v være en primplads.

Man kalder v *arkimedesisk*, hvis følgen $v(n)$, $n \in \mathbb{N}$, konvergerer mod ∞ ; i modsat fald *ikke-arkimedesisk*. Man skriver ofte $v \mid \infty$ hhv. $v \nmid \infty$ som kort notation skelnende mellem disse 2 tilfælde. For v ikke-arkimedesisk vises:

$$v(a + b) \leq \max\{v(a), v(b)\},$$

med lighed hvis $v(a) \neq v(b)$.

De arkimediske primpladser i K er følgende: $v(x) = |\varphi(x)|$, hvor φ er en legemsindlejring af K i \mathbb{C} , og $|\cdot|$ den sædvanlige absolutte værdi. De ikke-arkimediske primpladser i K opstår alle på følgende vis: Lad \mathfrak{O}_K være ringen af hele algebraiske tal i K , i.e. ringen af elementer x i K , der er rødder i et eller andet (i.e. af x afhængigt) normeret polynomium med heltallige koefficienter. Lad \mathfrak{p} være et primideal i \mathfrak{O}_K , lad $\alpha \in K^\times$, vælg $\beta \in \mathfrak{O}_K - \{0\}$, så $\alpha\beta \in \mathfrak{O}_K$, lad

$$\nu_{\mathfrak{p}}(\alpha) := \max_{n \in \mathbb{N}} \{\alpha\beta \in \mathfrak{p}^n\} - \max_{n \in \mathbb{N}} \{\beta \in \mathfrak{p}^n\},$$

og sæt

$$(\dagger) \quad v_{\mathfrak{p}}(\alpha) := a^{-\nu_{\mathfrak{p}}(\alpha)}, \quad v_{\mathfrak{p}}(0) := 0,$$

hvor a er et vilkårligt reelt tal > 1 ; $v_{\mathfrak{p}}$ afhænger ikke af valget af β , og definerer en ikke-arkimedisk valuation på K . Forskellige valg af a resulterer i ækvivalente valuationer. Sædvanligvis vil man 'normalisere' valget af a ved at sætte $a = |\mathfrak{O}_K/\mathfrak{p}|$; i så fald kaldes $v_{\mathfrak{p}}$ defineret ved (\dagger) for den *normaliserede p-adiske valuation på K*. Vi forudsætter i det følgende, at vores ikke-arkimediske valuationer er normaliserede i denne forstand.

A.1. Kompletion. Lad v være en primplads i K . Via metrikken d_v kan vi konstruere *kompletionen* K_v af K m.h.t. v : Det er samme type konstruktion som konstruktionen af \mathbb{R} fra \mathbb{Q} : Givet d_v har man begreberne 'Cauchy-følge' og 'nulfølge' m.h.t. d_v , og vi definerer:

$$K_v = \{\text{Cauchy-følger}\} / \{\text{nul-følger}\}.$$

K_v bliver da født med en naturlig legemsstruktur, man har en legemsindlejring $K \hookrightarrow K_v$, og v kan fortsættes til en valuation på K_v ; K_v bliver et lokalkompakt, fuldstændigt topologisk legeme m.h.t. d_v . Hvis v er arkimedisk, er K_v velkendt: Vi får $K_v = \mathbb{R}$ eller \mathbb{C} , eftersom $\varphi(K)$ (se ovenfor) er indeholdt i \mathbb{R} eller \mathbb{C} .

Lad nu v være ikke-arkimedisk. Mængden

$$\mathfrak{O}_v := \{v \in K_v \mid v(x) \leq 1\}$$

vises at udgøre en underring i K_v (kaldet ringen af hele v -adiske tal). Denne ring er en *lokal* (kommutativ) ring, i.e. den har netop et maksimalideal; dette er

$$\mathfrak{p}_v := \{v \in K_v \mid v(x) < 1\}.$$

Legemet $k_v := \mathfrak{O}_v/\mathfrak{p}_v$ vises at være et *endeligt* legeme kaldet *v's restklasselegeme*.

A.2. Udvidelser. Lad L/K være en endelig, normal udvidelse af grad n og Galoisgruppe G . Lad v være en (normaliseret) ikke-arkimedisk valuation i K . Hvis w er en valuation på L , så siges w at være en udvidelse af v , såfremt restriktionen af w til K er ækvivalent med v . I så fald er også w ikke-arkimedisk. Man viser følgende: v har mindst 1 og højst n udvidelser til en normaliseret ikke-arkimedisk valuation på L ; lad $w = w_1, \dots, w_s$ være disse. Man har da for $\alpha \in L$:

$$\prod_{i=1}^s w_i(\alpha) = v(N_{L/K}(\alpha)),$$

hvor $N_{L/K}(\cdot)$ er normafbildningen $\alpha \mapsto \prod_{g \in G} g.\alpha$ af L ind i K . Nu virker Galois-gruppen G på mængden $\{w_1, \dots, w_s\}$ via fastsættelsen:

$$(g.w_i)(\alpha) := w_i(g^{-1}.\alpha);$$

man viser, at denne virkning er *transitiv*.

Man definerer *dekompositionsgruppen* D_w for w som stabilisatoren i G m.h.t. denne virkning:

$$D_w := \{g \in G \mid g.w = w\}.$$

Grupperne D_{w_1}, \dots, D_{w_s} er indbyrdes konjugerede i G : Hvis $w_j = g.w_i$, haves $D_{w_j} = gD_{w_i}g^{-1}$.

Da w er en udvidelse af v , har man på naturlig måde K_v indlejret som dellegeme af L_w . Nu har vi en naturlig virkning af D_w på mængden af Cauchy-følger m.h.t. w i L (hvis $g \in G$, og (α_m) er en Cauchy-følge m.h.t. w , da er $(g.\alpha_m)$ en Cauchy-følge m.h.t. $g.w$). Ved denne virkning går nul-følger over i nul-følger, så vi får en virkning på L_w ; denne stabiliserer K_v punktvis. Man viser: L_w/K_v er en normal udvidelse, og den beskrevne virkning af D_w giver en *isomorfi*:

$$D_w \xrightarrow{\sim} \text{Gal}(L_w/K_v).$$

Man kan anstille fuldstændigt tilsvarende overvejelser, hvis v er en arkimedisk valuation; i dette tilfælde vil analogierne til ovenstående dog kun bestå af trivialiteter, som vi ikke vil få yderligere brug for.

A.3. Forgrening og Frobenius-elementer. Behold situation og notation som i **A.2**. For hvert i er $\mathfrak{p}_v \mathfrak{D}_{w_i}$ et ideal i \mathfrak{D}_{w_i} og følgerlig en potens af \mathfrak{p}_{w_i} :

$$\mathfrak{p}_v \mathfrak{D}_{w_i} = \mathfrak{p}_{w_i}^{e_i};$$

størrelsen e_i kaldes w_i 's *forgreningsindex* (over v); w_i kaldes *uforgrenet*, hvis $e_i = 1$, i modsat fald *forgrenet*. Nu vises $e_1 = \dots = e_s$; det har da mening at kalde v *uforgrenet i L*, hvis $e := e_1 = 1$; i modsat fald siges v at være *forgrenet i L*. Man har følgende fundamentale sætning:

Sætning A.3.1. *Mængden af i L forgrenede primpladser i K er endelig.*

Mere præcist kan man definere et ideal $\mathfrak{D}(L/K)$ - kaldet *diskriminanten for L/K* - i ringen \mathfrak{D} af hele algebraiske tal i K med den egenskab, at primpladsen i K hørende til et primideal \mathfrak{p} i \mathfrak{D} forgrenes i L , hvis og kun hvis \mathfrak{p} går op i $\mathfrak{D}(L/K)$.

Man definerer w 's *inertigruppe* I_w som følgende undergruppe af D_w :

$$I_w := \{g \in D_w \mid w(g.\alpha - \alpha) < 1, \forall \alpha \in \mathfrak{D}_w\},$$

og viser:

$$I_w = 1 \Leftrightarrow w \text{ er uforgrenet};$$

mere præcist er $\#I_w = e$.

Lad nu F være fikspunktslegemet for I_w i L_w ; w inducerer en valuation w^{unr} på F ('unr' for 'unramified'); w^{unr} er en fortsættelse af v til F , og F er fuldstændig m.h.t. w^{unr} ; vi kan altså skrive $F = F_{w^{\text{unr}}}$ og har størrelserne $\mathfrak{D}_{w^{\text{unr}}}$ og $\mathfrak{p}_{w^{\text{unr}}}$

knyttet hertil. F_w^{unr} er den maksimale uforgrenede udvidelse af K_v i L_w , og man har med $k_w := \mathfrak{D}_w/\mathfrak{p}_w$ en kanonisk homomorfi

$$\text{Gal}(F_w^{\text{unr}}/K_v) \cong D_w/I_w \longrightarrow \text{Gal}(k_w/k_v),$$

der vises at være en isomorfi. Da k_w er en endelig udvidelse af det endelige legeme k_v , kender vi strukturen af Galoisgruppen $\text{Gal}(k_w/k_v)$: Den er cyklisk af orden $\dim_{k_v} k_w$ med den kanoniske frembringer (Frobenius-automorfien) $x \mapsto x^q$, hvor $q := \#k_v$; et løft til D_w af denne kanoniske frembringer kaldes et (aritmisk) *Frobenius-element hørende til w* , og vi betegner et sådant med Fr_w ; $\text{Fr}_w \in D_w$ er altså *kun defineret modulo I_w* ; som element i D_w/I_w karakteriseres det ved egenskaben:

$$\text{Fr}_w(\alpha) \equiv \alpha^q \pmod{\mathfrak{p}_w}, \quad \forall \alpha \in \mathfrak{D}_w.$$

Som vi nævnte ovenfor har enhver anden primplads w_i af L over v formen $w_i = g.w$ for et $g \in G := \text{Gal}(L/K)$; man verificerer, at $\text{Fr}_{g.w} = g\text{Fr}_w g^{-1}$ (som elementer i $D_{g.w}/I_{g.w}$). Er man derfor kun interesseret i egenskaber ved Frobenius-elementerne, der er invariante under konjugation (som eksempelvis sporene af deres billeder under en lineær repræsentation), så tillader man sig i reglen at benytte Fr_v som betegnelse for ethvert af disse; Fr_v er altså kun bestemt op til konjugation med elementer i G , og kaldes '*Frobenius-element over v* '.

Endelig vil vi nævne følgende down-to-earth fortolkning af de størrelser, der forekommer ovenfor. Lad som ovenfor w_1, \dots, w_s være fortsættelserne af v til L med tilhørende forgreningsindices $e_1 = \dots = e_s =: e$. Størrelsen $f_i := \dim_{k_v} k_{w_i}$ kaldes w_i 's restklassegrad; det følger af det ovenstående, at vi har $f_1 = \dots = f_s =: f$. Man viser, at størrelserne s, e, f også kan aflæses på følgende måde: Valuationen v svarer til et primideal \mathfrak{p} i \mathfrak{D}_K ; ringen \mathfrak{D}_L af hele algebraiske tal i L har entydig faktorisering af idealer som produkt af primidealer; vi kan følgelig betragte primfaktoriseringen af $\mathfrak{p}\mathfrak{D}_L$; denne faktorisering har form:

$$\mathfrak{p}\mathfrak{D}_L = \mathfrak{P}_1^e \dots \mathfrak{P}_s^e,$$

hvor $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ er indbyrdes forskellige primidealer i \mathfrak{D}_L med $\mathfrak{D}_L/\mathfrak{P}_i = f_i = f$, og man har følgende sætning:

Sætning A.3.2. $sef = n = [L : K]$.

A.4. Højere forgreningsgrupper. Samme situation som i 1.2. Sæt $\mathfrak{D} := \mathfrak{D}_w$, $I := I_w$ og $\nu := \nu_{\mathfrak{p}_w}$ således, at vi ifølge definitioner har $w(\alpha) = |\mathfrak{D}/\mathfrak{p}_w|^{-\nu(\alpha)}$ for $\alpha \in L$. Ifølge definitionen på I haves da:

$$\begin{aligned} g \in I &\Leftrightarrow w(g.\alpha - \alpha) < 1, \quad \forall \alpha \in \mathfrak{D} \Leftrightarrow \nu(g.\alpha - \alpha) > 0, \quad \forall \alpha \in \mathfrak{D} \\ &\Leftrightarrow \nu(g.\alpha - \alpha) \geq 1, \quad \forall \alpha \in \mathfrak{D}. \end{aligned}$$

For $u \in \mathbb{Z}$, $u \geq -1$, defineres den *højere forgreningsgruppe I_u* ved:

$$(*) \quad g \in I_u \Leftrightarrow \nu(g.\alpha - \alpha) \geq u + 1, \quad \forall \alpha \in \mathfrak{D}.$$

Således er $D_w = I_{-1}$ og $I = I_0$. Det vises, at grupperne I_u er *normale* undergrupper i D_w ; man har $I_0 \geq I_1 \geq \dots$, og $I_u = 1$ for u tilstrækkelig stor. Gruppen I_1 kan vises at være en p -gruppe, hvis p betegner karakteristikken af k_v , hvorimod kvotienten I_0/I_1 er cyklisk af orden primisk med p .

Definitionen (*) giver mening for ethvert $u \in \mathbb{R}$; vi kan således definere en funktion $\varphi : \mathbb{R}_{\geq -1} \rightarrow \mathbb{R}$ ved:

$$\varphi(u) = \int_0^u \frac{dt}{[I_0 : I_t]},$$

hvor $[I_0 : I_t]$ for $t \leq 0$ skal fortolkes som $[I_t : I_0]^{-1}$. Funktionen φ vises at være en stykkevis lineær, kontinuert, voksende og konkav afbildning af $[-1, \infty[$ på sig selv. Kald den inverse funktion til φ for ψ og definer for $s \geq -1$: $I^s := I_{\psi(s)}$. Grupperne I^s kaldes *forgreningsgrupper med øvre nummerering*, og formålet med deres indføring er følgende sætning, hvis betydning vi vil se i næste afsnit:

Sætning A.4.1. *Lad L'/K være en Galoisudvidelse indeholdt i L , og lad w' være va-uationen på L' , som w er en fortsættelse af. Lad $N := \text{Gal}(L_w/L'_{w'})$ således, at $N \trianglelefteq D_w$. Da gælder*

$$I_{w'}^s = (I_w^s N)/N .$$

APPENDIX B. ABSOLUTTE GALOISGRUPPER.

Lad M/K være en vilkårlig Galoisudvidelse af legemer, i.e., M er algebraisk over K , og gruppen $\text{Gal}(M/K)$ bestående af legems-automorfier af M , der fikserer K elementvist, fikserer *kun* elementer i K . Lad $K(j)$, $j \in J$, være mængden af endelige Galoisudvidelser af K indeholdt i M . Hvis $K(i) \subseteq K(j)$, har vi fra Galoisteorien en surjektiv homomorf $\pi_{ji} : \text{Gal}(K(j)/K) \rightarrow \text{Gal}(K(i)/K)$, hvilket giver systemet af endelige grupper $\text{Gal}(K(j)/K)$, $j \in J$, struktur af et projektivt system. Vi kan derfor betragte systemets projektive limes:

$$G := \varprojlim_{j \in J} \text{Gal}(K(j)/K) ;$$

man viser, at vi har en naturlig isomorfi:

$$\text{Gal}(M/K) \cong G .$$

Vi kan forsyne hver af grupperne $\text{Gal}(K(j)/K)$ med den diskrete topologi; homomorfierne π_{ji} er da kontinuerte, og 'abstrakt nonsens' giver derfor en topologi på $\text{Gal}(M/K) \cong G$ p.gr.a. G 's konstruktion som projektiv limes: Et system af åbne omegne af 1 er mængden $\text{Gal}(M/K(j))$, $j \in J$. $\text{Gal}(M/K)$ er et eksempel på en *pro-endelig* topologisk gruppe; sådanne kan karakteriseres ved at være kompakte og totalt usammenhængende.

Vi skal benytte denne konstruktion i tilfælde, hvor K er et algebraisk tallegeme, kompletteringen af et sådant m.h.t. en valuation, eller er et endeligt legeme, og hvor $M = \bar{K}$ er en algebraisk afslutning af K . I disse tilfælde skriver vi

$$G_K := \text{Gal}(\bar{K}/K) .$$

B.1. Dekompositionsgrupper. Betragt specielt tilfældet $K = \mathbb{Q}$, $M = \bar{\mathbb{Q}}$, med $K(j)/\mathbb{Q}$, $j \in J$, systemet af endelige Galoisudvidelser af \mathbb{Q} . Lad p være et primtal. Lad $w(p, j)$, $j \in J$, være et system af valuationer på legemerne $K(j)$ med følgende egenskaber: (i) $w(p, j)$ er en valuation på $K(j)$, der fortsætter valuationen hørende til p på \mathbb{Q} ; (ii) Hvis $K(i) \subseteq K(j)$, da er $w(p, j)$ en fortsættelse af $w(p, i)$.

Et sådant system $w(p, j)$ eksisterer, men er på ingen måde entydigt bestemt; faktisk er mængden af mulige systemer overtælleligt.

Givet systemet $w(p, j)$, $j \in J$, kan vi lade $K(p, j)$ betegne kompletionen af $K(j)$ m.h.t. $w(p, j)$, og lade $D(p, j)$ hhv. $I(p, j)^u$, $u \geq -1$, være de tilhørende dekompositionsgrupper hhv. højere inertigrupper med øvre nummerering; vi har altså $I(p, j)^{-1} = D(p, j)$. Vi vil nu se formålet med introduktionen af den øvre nummerering på de højere inertigrupper: Sætning A.4.1 medfører, at systemet $I(p, j)^u$, $j \in J$, for ethvert givet $u \geq -1$, på naturlig måde udgør et projektivt system: Hvis $K(i) \leq K(j)$, da er $I(p, i)^u$ kvotient af $I(p, j)^u$ via den kanoniske homomorfi fra Galoisteorien. Det giver således mening at definere:

$$I_p^u := \varprojlim_{j \in J} I(p, j)^u,$$

og specielt

$$D_p := I_p^{-1} = \varprojlim_{j \in J} D(p, j).$$

Af konstruktion af tidligere nævnte resultater følger:

- (i) $D_p \leq G_{\mathbb{Q}}$, $I_p^u \leq D_p$, $\forall u \geq -1$,
- (ii) $I_p^v \geq I_p^u$, for $v \leq u$, $I_p^u = \bigcap_{v < u} I_p^v$, og $\bigcap_u I_p^u = 1$.

Grupperne D_p , I_p^u afhænger naturligvis af valget af systemet $w(p, j)$. Resultaterne i A.2 viser imidlertid, at forskellige valg af systemet $w(p, j)$ resulterer i konjugation med elementer i $G_{\mathbb{Q}}$ af de tilknyttede grupper D_p . Vi kalder D_p hhv. I_p^u , $u \geq 0$, for (en) *dekompositionsgruppe over p i $G_{\mathbb{Q}}$* hhv. (højere) *inertigrupper over p i $G_{\mathbb{Q}}$* . Vi sætter $I_p := I_p^0$. Der gælder følgende sætning, som ikke helt følger af tidligere nævnte resultater:

Sætning B.1.1. (i) $D_p \cong G_{\mathbb{Q}_p}$,
(ii) $D_p/I_p \cong G_{\mathbb{F}_p}$.

Disse isomorfier er kanoniske i den forstand, at deres konstruktion som injektive homomorfier følger direkte af de tilsvarende konstruktioner i A.3 ovenfor samt konstruktionen af grupperne I_p^u ; kun surjektiviteten af disse homomorfier kræver yderligere overvejelser.

Gruppen $G_{\mathbb{F}_p}$ har en kanonisk *topologisk* frembringer: Frobenius-automorfien σ , der virker på \mathbb{F} ved $\sigma(\alpha) = \alpha^p$; 'topologisk frembringer' betyder naturligvis, at $\langle \sigma \rangle$ er *tæt* i $G_{\mathbb{F}_p}$. Et løft af σ til D_p via isomorfien i (ii) i sætningen ovenfor kaldes (et) *Frobenius-element over p i $G_{\mathbb{Q}}$* , og vi betegner et sådant med Fr_p . Således er $\text{Fr}_p \in D_p \leq G_{\mathbb{Q}}$ efter valg af system $w(p, j)$ og dermed D_p kun entydigt bestemt modulo I_p ; forskellige valg af systemer $w(p, j)$ resulterer i konjugation af de tilknyttede elementer Fr_p .

B.2. Galoisrepræsentationer. Lad n være et naturligt tal. Ved en *n -dimensional Galoisrepræsentation* (af $G_{\mathbb{Q}}$) vil vi forstå en semisimpel, kontinuert homomorfi $\rho: G_{\mathbb{Q}} \rightarrow \text{GL}_n(F)$, hvor F er enten (i) \mathbb{C} med den diskrete topologi, (ii) en endelig udvidelse af \mathbb{Q}_{ℓ} , (ℓ primtal) med sin naturlige topologi, eller (iii) et endeligt legeme (lad os sige af karakteristisk ℓ) med den diskrete topologi. Svarende

til disse 3 tilfælde kalder man ρ en *kompleks*, en *l -adisk*, hhv. en *mod l Galoisrepræsentation*. Billedet $\rho(G_{\mathbb{Q}})$ er *endeligt* i tilfældene (i) og (iii), men ikke nødvendigvis i tilfældet (ii). Hvis ρ er givet, vil vi som fast betegnelse benytte ℓ som betegnelse for det primtal, der er givet med ρ , hvis ρ er af typen (ii) eller (iii).

Lad nu $\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(F)$ være en Galoisrepræsentation, lad p være et primtal, lad D_p være (en) dekompositionsgruppe over p , og lad $I_p \trianglelefteq D_p$ være den tilhørende inertigruppe. Vi siger, at ρ er *uforgrenet over p* , hvis $\rho(I_p) = 1$; i modsat fald siges ρ naturligvis at være *forgrenet over p* ; man siger også, at p er et *forgreningspunkt* for ρ . Da jo ρ 's kerne er en normal undergruppe i $G_{\mathbb{Q}}$, følger det, at selvom gruppen $I_p \leq G_{\mathbb{Q}}$ ikke er entydigt bestemt, så er egenskaben 'uforgrenet over p ' uafhængig af valget af D_p , I_p . Hvis ρ er af type (i) eller (iii), så følger det af sætning A.3.1, at ρ kun er forgrenet over p for endeligt mange p . Hvis ρ er af type (ii) følger dette ikke nødvendigvis, men man finder i øjeblikket i talteorien ikke anledning til at betragte l -adiske repræsentationer med uendeligt mange forgreningspunkter; vi vil overalt forudsætte, at *l -adiske Galoisrepræsentationer kun har endeligt mange forgreningspunkter*; man kan således tage denne egenskab som en del af definitionen af en l -adisk repræsentation.

Hvis ρ er uforgrenet, giver ρ via restriktion til D_p anledning til en homomorfi $D_p/I_p \rightarrow \mathrm{GL}_n(F)$, hvorfor det giver mening at tale om $\rho(\mathrm{Fr}_p)$; dette element i $\mathrm{GL}_n(F)$ afhænger naturligvis af valget af D_p , men det følger af bemærkningerne i B.1, at det *karakteristiske polynomium* af $\rho(\mathrm{Fr}_p)$ - og dermed specielt $\mathrm{Tr}\rho(\mathrm{Fr}_p)$ - er *uafhængigt* af dette valg. Mere generelt kan vi gøre os følgende overvejelser: Vi kan opfatte ρ som en homomorfi $G_{\mathbb{Q}} \rightarrow \mathrm{Aut}(V)$, hvor V er et n -dimensionalt vektorrum over F . Betegner vi med ρ_p restriktionen af ρ til D_p , da giver ρ_p - eftersom $I_p \trianglelefteq D_p$ - en homomorfi $D_p/I_p \rightarrow \mathrm{Aut}(V^{I_p})$, hvor V^{I_p} betegner *fikspunkterne* for $\rho(I_p)$ i V ; betegner vi denne homomorfi med $\rho_p^{I_p}$, kan vi således tale om $\rho_p^{I_p}(\mathrm{Fr}_p)$, og vi har, at det karakteristiske polynomium og dermed specielt sporet af af dette element i $\mathrm{Aut}(V^{I_p})$ er uafhængigt af valget af D_p .

Vi har nu følgende fundamentale sætninger.

Sætning B.2.1. (*Chebotarev's sætning.*) *Lad L/\mathbb{Q} være en endelig Galoisudvidelse med Galoisgruppe G . Lad $C \subseteq G$ være en konjugationsklasse i G . For $x \in \mathbb{R}$, $x \geq 2$, har vi da for antallet $\pi_{L/\mathbb{Q},C}(x)$ af primtal $p \leq x$, der er uforgrenede i L/\mathbb{Q} , og for hvilke $\mathrm{Fr}_p \in C$:*

$$\pi_{L/\mathbb{Q},C}(x) = \frac{|C|}{|G|} \cdot \int_2^x \frac{dt}{\log t} + o\left(\frac{x}{\log x}\right).$$

Chebotarev's sætning er en generalisering af den velkendte primtalssætning. Beviset er i det væsentlige analytisk talteori, men benytter sig dog af et grundlæggende udsagn fra klasselegemeteorien. Restleddet kan præciseres, og under antagelse af den såkaldte generaliserede Riemann-hypotese forbedres betydeligt. Følgende sætning er et korollar til Chebotarev's sætning.

Sætning B.2.2. *Lad L/\mathbb{Q} være en (ikke nødvendigvis endelig) Galoisudvidelse med Galoisgruppe G , der er uforgrenet udenfor en endelig mængde af primtal*

S . Betegn for $p \in S$ med $[\text{Fr}_p]$ konjugationsklassen af Fr_p i G . Da er $\bigcup_{p \notin S} [\text{Fr}_p]$ tæt i G .

Denne sætning medfører sammen med generelle egenskaber for semisimple repræsentationer følgende sætning, der giver en første antydning af begrundelsen for vores fokusering på Frobenius-elementer i forbindelse med Galoisrepræsentationer.

Sætning B.2.3. Lad $\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_n(F)$ være en Galoisrepræsentation uforgrenet udenfor den endelige mængde S af primtal.

Hvis ρ er kompleks eller ℓ -adisk, er ρ bestemt op til konjugation ved sporene $\text{Tr}\rho(\text{Fr}_p)$, $p \notin S$.

Hvis ρ er en mod ℓ repræsentation, er ρ bestemt op til konjugation ved de karakteristiske polynomier af $\rho(\text{Fr}_p)$, $p \notin S$. Er $\ell > n$, er ρ bestemt op til konjugation ved sporene $\text{Tr}\rho(\text{Fr}_p)$, $p \notin S$.

B.3. Førere af Galoisrepræsentationer. Samme betegnelser og notationer som i B.2. Lad altså igen $\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_n(F)$ være en Galoisrepræsentation. Opfat som i B.2 ρ som en homomorfi $G_{\mathbb{Q}} \rightarrow \text{Aut}(V)$, hvor V er et n -dimensionalt vektorrum over F . Lad p være et primtal, der forudsættes $\neq \ell$, hvis ρ er en mod ℓ eller ℓ -adisk repræsentation. Vi definerer:

$$(\#) \quad m_p(\rho) = \dim_F(V/V^{\rho(I_p)}) + \int_0^{\infty} \dim_F(V/V^{\rho(I_p^u)}) du .$$

Man viser først, at $m_p(\rho) < \infty$; hvis ρ er en kompleks eller mod ℓ repræsentation, følger dette af endeligheden af $\rho(G_{\mathbb{Q}})$. Hvis ρ er ℓ -adisk, følger endeligheden af $m_p(\rho)$ af en påvisning af, at $\rho(P_p)$ er endelig, hvor $P_p := \bigcup_{u>0} I_p^u$; dette medføres af $p \neq \ell$, efter at man har bevist, at P_p er en *pro- p -gruppe*, i.e. en projektiv limes af endelige p -grupper.

Der gælder følgende ikke-trivielle sætning:

Sætning B.3.1. $m_p(\rho) \in \mathbb{N}_0$.

Vi bemærker, at definitionen af $m_p(\rho)$ umiddelbart giver:

$$m_p(\rho) = 0 \Leftrightarrow \rho \text{ er uforgrenet over } p.$$

Følgelig kan vi definere et naturligt tal $N(\rho)$ kaldet *føreren af ρ* (eng.: *conductor*) ved:

$$N(\rho) := \prod_p p^{m_p(\rho)} ,$$

hvor produktet er over alle primtal p , hvis ρ er kompleks, mens det er over alle $p \neq \ell$, hvis ρ er en mod ℓ eller ℓ -adisk repræsentation.

Hvis ρ er en kompleks repræsentation, kaldes $N(\rho)$ også *Artin-føreren* af ρ . Begrebet 'Artin-fører' er generalisering af et klassisk begreb fra klasselegemeteorien: Antag, at ρ er 1-dimensional: $\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_1(\mathbb{C}) = \mathbb{C}^{\times}$; da er $\rho(G_{\mathbb{Q}})$ *cyklisk*, i.e. fikslegemet for $\text{Ker}(\rho) \leq G_{\mathbb{Q}}$ er en endelig Galoisudvidelse af \mathbb{Q} med cyklisk Galoisgruppe; i klasselegemeteorien knytter man til en sådan et naturligt tal kaldet

føreren af den givne udvidelse; denne fører stemmer overens med Artin-føreren af ρ .

Selvom vi i artiklens hoveddel ikke beskæftiger os synderligt med L-rækker af Galoisrepræsentationer, vil vi dog for fuldstændighedens skyld kort anføre deres definition for komplekse repræsentationer, da det kan siges at være 'L-funktions-yoga', der historisk set førte Langlands frem til sine storslåede visioner om sammenhænge mellem Galoisrepræsentationer og automorfe former, hvorved den udvikling, der i sidste ende førte frem til beviset for Taniyama-Shimura-formodningen, blev igangsat.

Lad altså $\rho: G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_n(\mathbb{C})$ være en kompleks repræsentation, og V som ovenfor. Man definerer for en kompleks parameter s :

$$(b) \quad L(\rho, s) = A(\rho)^{s/2} \gamma(s) \prod_p \frac{1}{\det(1 - p^{-s} \rho(\mathrm{Fr}_p) | V^{I_p})},$$

hvor $|$ betyder 'virkende på', $A(\rho)$ er et vist naturligt tal, der afhænger bl. a. af $N(\rho)$, $\gamma(s)$ er en vis funktion, der kan udtrykkes via den klassiske Gamma-funktion $\Gamma(s)$, og hvor produktet er over alle primtal p . Denne definition er i første omgang rent formel, men vi kan dog straks notere os, at den generaliserer en yderst velkendt, klassisk funktion: Antag, at ρ er den trivielle repræsentation $G_{\mathbb{Q}} \rightarrow \mathrm{GL}_1(\mathbb{C})$, i.e. $\rho(g) = 1, \forall g \in G_{\mathbb{Q}}$. I dette tilfælde er $N(\rho) = 1, A(\rho) = 1, \gamma(s) = \pi^{-s/2} \Gamma(s/2)$, og følgelig $L(\rho, s) = \pi^{-s/2} \Gamma(s/2) \zeta(s)$, hvor $\zeta(s)$ er Riemann's zeta-funktion; som bekendt gælder der altså i dette tilfælde, at $L(\rho, s)$ definerer en holomorf funktion af s for $\mathrm{Re}(s) > 1$, og kan fortsættes meromorft til hele den komplekse plan, hvor den har simple poler i 0 og 1, og tilfredsstiller funktionalligningen:

$$L(\rho, 1 - s) = L(\rho, s).$$

Generelt har man følgende berømte sætning af Artin:

Sætning B.3.2. *$L(\rho, s)$ definerer en holomorf funktion af s for $\mathrm{Re}(s) > 1$, som kan fortsættes meromorft til hele den komplekse plan, hvor den tilfredsstiller funktionalligningen*

$$L(\rho, 1 - s) = W(\rho) L(\hat{\rho}, s).$$

Her er $\hat{\rho}$ den til ρ kontragrediente repræsentation, og $W(\rho)$ er et vist komplekst tal med absolutværdi 1 (det såkaldte Artin'ske 'rodtal' knyttet til ρ).

Artin's berømte formodning udsiger, at hvis enten $n > 1$ og ρ er irreducibel, eller hvis $n = 1$ og ρ er ikke-triviel, da kan $L(\rho, s)$ fortsættes holomorft til hele den komplekse plan (med ovenstående funktionalligning). For $n = 1$ kan denne formodning bevises ved hjælp af klasselegemeteorien. For $n = 2$ vides der nu ganske meget, hvilket bl.a. (men *ikke* kun) skyldes de nyeste udviklinger, som Wiles' fundamentale arbejde har givet anledning til. For $n > 1$ er formodningen stort set stadig åben, idet man kun kender beviser i en række (ret beset temmeligt) specielle tilfælde.

B.4. Bemærkninger. Samtlige af de ovenstående begreber, resultater og formodninger har generaliseringer til situationen, hvor man betragter repræsentationer af G_K , hvor K er et vilkårligt algebraisk tallegeme.

Man kan også definere L -rækker knyttede til *visse* typer af l -adiske repræsentationer (eller rettere: til visse systemer af sådanne), og for disse udtale formodninger, der generaliserer Artin's formodning ovenfor. Vi undgår af give de relevante definitioner, da de forudsætter indførelse af yderligere begreber, især fra algebraisk geometri. Det skal dog nævnes, at disse 'generaliserede Artin-formodninger' i sammenhæng med de systemer af l -adiske repræsentationer, der opstår på naturlig måde fra elliptiske kurver defineret over \mathbb{Q} , kan vises at være ækvivalente med (en version af) den berømte Taniyama-Shimura-formodning, der står centralt i Wiles' arbejde. Vi vil dog ikke beskæftige os nærmere med *denne* formulering af Taniyama-Shimura-formodningen, især fordi denne formulering ikke har vist sig at være en frugtbar ansats for *beviser* for Taniyama-Shimura.

Artin's formodning (i den ovenfor benyttede analytiske version) er af betydning for moderne talteori, fordi den (overraskende) viste sig i tilfældet $n = 2$ at være *ækvivalent* til en generalisering af klasselegemeteorien til 2-dimensionale komplekse repræsentationer af $G_{\mathbb{Q}}$; denne synsvinkel har - i modsætning til foregående bemærkning - vist sig at være frugtbar, idet den har spillet en rolle for *beviser* for en del af disse generaliseringer, hvoraf én udgør udgangspunktet for Wiles' bevis for en del af Taniyama-Shimura-formodningen.

Litteratur.

Der følger her et kort og på ingen måde fuldstændigt udvalg af litteratur; listen indeholder litteratur til brug ved studium af baggrundsstof, selve beviset for Taniyama-Shimura/Fermat, samt mere avancerede emner.

Algebraisk talteori, klasselegemeteorien: [BS], [Neu], [Ser68], [Koc], [CF]

Gruppekohomologi, Galoiskohomologi: [CF], [Mil], [Hab]

Grupperrepræsentationer: [CR]

Algebraisk/aritmetisk geometri: [Har], [CS]

Elliptiske kurver: [Sil86], [Sil94]

Modulformer: [Miy], [Shi]

Aritmetik af modulkurver: [CSS], [Maz77]

Modulformer og Galoisrepræsentationer: [Del], [Ser77], [DS], [Ser87], [Rib], [Car]

Artinske L -funktioner, Artin's formodninger: [Mar], [Neu], [Ser77], [DS], [Lan], [Tun]

Base change teori: [Lan], [Tun]

Serre's formodninger: [Ser87], [Rib], [Edi]

Taniyama-Shimura \implies Fermat: [Fre86], [Fre89], [Ser87], [Rib]

Taniyama-Shimura og generaliseringer: [DDT], [CSS], [Wil], [TW], [Dia97], [Dia96], [CDT], [BCDT]

REFERENCES

- [BS] Z.I. Borevich, I.R. Shafarevich: Number theory. Academic Press, 1966.
- [BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor: On the modularity of elliptic curves over \mathbb{Q} . To appear.
- [Car] H. Carayol: Sur les représentations l -adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)* **19** (1986), 409–468.
- [CF] J.W.S. Cassels, A. Fröhlich: Algebraic number theory. Academic Press, 1967.
- [CDT] B. Conrad, F. Diamond, R. Taylor: Modularity of certain potentially Barsotti-Tate Galois representations. *J. Amer. Math. Soc.* **12** (1999), 521–567.
- [CS] G. Cornell, J.H. Silverman (eds.): Arithmetic geometry. Springer, 1986.
- [CSS] G. Cornell, J.H. Silverman, G. Stevens (eds.): Modular forms and Fermat's last theorem. Springer, 1998.
- [CR] C.W. Curtis, I. Reiner: Representation theory of finite groups and associative algebras. Wiley, 1962.
- [DDT] H. Darmon, F. Diamond, R. Taylor: Fermat's last theorem. Current developments in mathematics 1995, International Press, 1995.
- [Del] P. Deligne: Formes modulaires et représentations l -adiques. *Sém. Bourbaki 1968/69* **355** (1969), 139–172.
- [DS] P. Deligne, J.-P. Serre: Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)* **7** (1975), 507–530.
- [Dia96] F. Diamond: On deformation rings and Hecke rings. *Ann. of Math (2)* **144** (1996), 137–166.
- [Dia97] F. Diamond: The Taylor-Wiles construction and multiplicity one. *Invent. math.* **128** (1997), 379–391.
- [Edi] B. Edixhoven: The weight in Serre's conjectures on modular forms. *Invent. math.* **109** (1992), 563–594.
- [Fre86] G. Frey: Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Saraviensis, ser. Math.* **1** (1986), 1–40.
- [Fre89] G. Frey: Links between solutions of $A=B=C$ and elliptic curves. In: Number Theory, Ulm 1987, *Lecture Notes in Mathematics* **1380**, Springer, 1989.
- [Hab] K. Haberland: Galois cohomology of algebraic number fields. VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.
- [Har] R. Hartshorne: Algebraic geometry. *Graduate texts in Mathematics* **52**, Springer, 1977.
- [Koc] H. Koch: Algebraic number theory. Springer, 1997.
- [Lan] R.P. Langlands: Base change for $GL(2)$. *Annals of Math. Studies* **96**, Princeton Univ. Press, 1980.
- [Mar] J. Martinet: Character theory and Artin L -functions. I: A. Fröhlich (ed.): Algebraic Number Fields, L -functions and Galois properties. Academic Press, 1977.
- [Maz77] B. Mazur: Modular curves and the Eisenstein ideal. *Publ. Math. IHES* **47** (1977), 33–186.
- [Maz78] B. Mazur: Rational isogenies of prime degree. *Invent. Math.* **44** (1978), 129–162.
- [Mil] J. S. Milne: Arithmetic duality theorems. *Perspectives in Mathematics* **1**, Academic Press, 1986.
- [Miy] T. Miyake: Modular forms. Springer, 1989.
- [Neu] J. Neukirch: Algebraic number theory. Springer, 1999.
- [Rib] K.A. Ribet: On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Invent. math.* **100** (1990), 431–476.
- [Ser68] J.-P. Serre: Corps locaux. *Hermann, Paris*, 1968.
- [Ser77] J.-P. Serre: Modular forms of weight one and Galois representations. I: A. Fröhlich (ed.): Algebraic Number Fields, L -functions and Galois properties. Academic Press, 1977.
- [Ser87] J.-P. Serre: Sur les représentations de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.* **54** (1987), 179–230.
- [Shi] G. Shimura: Introduction to the arithmetic theory of automorphic functions. Princeton University Press, 1971.
- [Sil86] J.H. Silverman: The arithmetic of elliptic curves. *Graduate texts in Mathematics* **106**, Springer, 1986.
- [Sil94] J.H. Silverman: Advanced topics in the arithmetic of elliptic curves. *Graduate texts in Mathematics* **151**, Springer, 1994.

- [TW] R. Taylor, A. Wiles: Ring theoretic properties of certain Hecke algebras. *Ann. Math.* **141** (1995), 553–572.
- [Tun] J. Tunnell: Artin's conjecture for representations of octahedral type. *Bull. AMS* **5** (1981), 173–175.
- [Wil] A. Wiles: Modular elliptic curves and Fermat's Last Theorem. *Ann. Math.* **141** (1995), 443–551.