

Hvad er en modulær elliptisk  
kurve?

Hvilken rolle spiller de ved  
beviset af Fermat's sidste  
sætning?

Johan P. Hansen

28. oktober 1998

# Mål

- at beskrive den sammenknytning, der er mellem to vidt forskellige objekter:
  - modulære former (en bestemt slags komplekse funktioner)
  - elliptiske kurver

Sammenknytningen viser sig igennem en række, der dels er en Fourier-række for den komplekse funktion dels en række, der indeholder oplysninger om løsningerne til den elliptiske kurves ligning modulo  $p$  for alle primtal  $p$ .

- at redegøre for, hvordan det benyttes ved beviset af Fermat's sidste sætning

Eks.  $q$ -ekspansion,  $q = e^{2\pi iz}$

$$f(z) := q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = \sum_{i=1}^{\infty} a_i q^i$$

hvis led af grad til og med 71 er:

$$\begin{aligned} & \boxed{-3} q^{71} + 4 q^{70} + q^{69} - 4 q^{68} + \boxed{-7} q^{67} + 2 q^{66} + \\ & 4 q^{65} - 8 q^{64} + 4 q^{63} - 14 q^{62} + \boxed{12} q^{61} - 2 q^{60} + \\ & \boxed{5} q^{59} + q^{55} - 10 q^{54} + \boxed{-6} q^{53} + 8 q^{52} + 2 q^{51} + \\ & 8 q^{50} - 3 q^{49} + 4 q^{48} + \boxed{8} q^{47} + 2 q^{46} - 2 q^{45} + \\ & 2 q^{44} + \boxed{-6} q^{43} - 4 q^{42} + \boxed{-8} q^{41} - 4 q^{39} + \boxed{3} q^{37} - \\ & 4 q^{36} - 2 q^{35} + 4 q^{34} - q^{33} + 8 q^{32} + \boxed{7} q^{31} + \\ & 2 q^{30} + \boxed{0} q^{29} - 4 q^{28} + 5 q^{27} - 8 q^{26} - 4 q^{25} + \\ & \boxed{-1} q^{23} - 2 q^{22} + 2 q^{21} + 2 q^{20} + \boxed{0} q^{19} + 4 q^{18} + \\ & \boxed{-2} q^{17} - 4 q^{16} - q^{15} + 4 q^{14} + \boxed{4} q^{13} - 2 q^{12} + \\ & \boxed{1} q^{11} - 2 q^{10} - 2 q^9 + \boxed{-2} q^7 + 2 q^6 + \boxed{1} q^5 + \\ & 2 q^4 + \boxed{-1} q^3 + \boxed{-2} q^2 + q \end{aligned}$$

koefficienterne til  $q^p$ , hvor  $p$  er et primtal, er fremhævet  $\boxed{a_p}$

# En modulær elliptisk kurve

For alle primtal  $p$  bestemmer vi antallet  $|E(\mathbb{Z}/p\mathbb{Z})|$  af løsninger  $(x, y) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$  til ligningen:

$$E : y^2 + y = x^3 + x^2 + 10x + 20$$

Lad tallet  $b_p$  være

$$b_p := p - |E(\mathbb{Z}/p\mathbb{Z})|$$

## Tabel

$p$	2	3	5	7	11	13	17	19	23	29
$a_p$	-2	-1	1	-2	1	4	-2	0	-1	0
$b_p$	-2	-1	1	-2	1	4	-2	0	-1	0

$p$	31	37	41	43	47	53	59	61	67	71
$a_p$	7	3	-8	-6	8	-6	5	12	-7	-3
$b_p$	7	3	-8	-6	8	-6	5	12	-7	-3

# Oversigt

Lad  $f$  være en modulær form, der er en eigenform. Giver en gruppehomomorfi - billedet er et gitter i  $\mathbb{C}$ .

$$(\Gamma_0(N), \circ) \xrightarrow{\gamma \mapsto \int_{\tau_0}^{\gamma(\tau_0)} f(z) dz} (L, +) \leq (\mathbb{C}, +)$$

Knytter elliptisk kurve  $E$  til  $f$ :

$$\begin{array}{ccc}
 \mathbb{H} & \xrightarrow{\tau \mapsto \int_{\tau_0}^{\tau} f(z) dz} & \mathbb{C} \\
 \downarrow \text{(banen for } \tau) & & \downarrow \text{Eichler Shimura} \\
 \Gamma_0(N) \backslash \mathbb{H} & \xrightarrow{\bar{\tau} \mapsto \int_{\tau_0}^{\bar{\tau}} f(z) dz} & \mathbb{C}/L \\
 \downarrow \text{modulær} & & \downarrow \text{(p, p') Weierstrass} \\
 \text{parametrisering} & & E_1(\mathbb{C}) \\
 E(\mathbb{C}) & \xleftarrow{\text{isogeni}} & 
 \end{array}$$

# Elliptiske kurver

En elliptisk kurve  $E$  har en Weierstrass ligning:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in k$$

med  $\Delta \neq 0$

$$b_2 = a_1^2 + 4a_2$$

$$b_4 = 2a_4 + a_1a_3$$

$$b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

$$j = \frac{(b_2^2 - 24b_4)^3}{\Delta}$$

- Med fordel kan man tilføje et punkt  $O$  i uendelig.  $\overline{E} = E \cup \{O\}$
- Linier gennem  $O$  er de lodrette linier
- Korde-sekant gruppestrukturen: 3 kollineære punkter har sum  $O$ .

# Afbildninger, isomorfier og isogenier

Lovlige koordinatskift  $u, r, s, t \in k$  og  $u \neq 0$

$$\begin{aligned}x &= u^2x' + r \\y &= u^3y' + su^2x' + t\end{aligned}$$

- betydningen af legemet  $k$
- isomorfibegrebet
- $j$  - invarianten, bestemmer isomorfiklassen over algebraisk lukkede legemer
- $\Delta$  EJ invariant under lovligt koordinatskift
- global minimal model
- isogeni - afbildning der er en gruppehomomorfi

## Eksempler

$$y^2 + y = x^3 + x^2 + 10x + 20$$

er en elliptisk kurve, idet  $\Delta = -11^5$ .

Ved lovligt koordinatskift

$$X = x - \frac{1}{3}$$

$$Y = 2y + 1$$

så bliver ligningen

$$Y^2 = 4X^3 + \frac{2^2 \cdot 31}{3}x - \frac{17 \cdot 107}{3^3}$$

## Frey kurverne

Lad  $\alpha, \beta, \gamma$  være hypotetiske heltalsløsninger til Fermat ligningen

$$x^l + y^l = z^l.$$

Frey anviste (og Wiles viste), at den elliptiske kurve med ligningen

$$y^2 = x(x - \alpha^l)(x - \gamma^l),$$

med

$$\Delta = 16\alpha^{2l}\beta^{2l}\gamma^{2l}$$

ikke kunne eksistere. Ved lovligt koordinatskift

$$x = 4X$$

$$y = 8Y + 4X$$

så bliver ligningen

$$Y^2 + XY = X^3 + \frac{1}{4}(1 - \alpha^l - \gamma^l)X^2 + \frac{1}{16}\alpha^l\gamma^lX$$

(global minimal Weierstrass form)

## Weierstrass teori

Lad  $L$  være et gitter i den komplekse plan  $\mathbb{C}$ , dvs heltals linearkombinationer af 2 komplekse tal  $\omega_1, \omega_2$ . Det fundamentale parallelogram er

$$\Pi = \{a_1\omega_1 + a_2\omega_2 \mid 0 \leq a_i \leq 1\}.$$

En meromorf funktion  $f : \mathbb{C} \rightarrow \mathbb{C} \cup \infty$  kaldes *elliptisk*, hvis den er periodisk med hensyn til  $L$ , dvs.

$$f(z + l) = f(z) \quad l \in L$$

Det er klart, at en elliptisk funktion for det første er bestemt ved sine værdier på det fundamentale parallelogram og for det andet er dets værdier på modsatte punkter af randen af  $\Pi$  ens, altså at

$$f(a_1\omega_1 + \omega_2) = f(a_1\omega_1)$$

og at

$$f(\omega_1 + a_2\omega_2) = f(a_2\omega_2)$$

En elliptisk funktion er altså en funktion på det fundamentale parallelogram  $\Pi$  med modsatte sider identificerede. Topologisk er det en *torus*, algebraisk er det  $\mathbb{C}/L$ .

## Weierstrass $\wp$ funktioner

$$\wp(z) := \frac{1}{z^2} + \sum_{l \in L, l \neq 0} \left( \frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

$$\wp'(z) := -2 \sum_{l \in L} \frac{1}{(z-l)^3}$$

er elliptiske funktioner, der tilfredsstiller:

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3,$$

$$g_2 = 60 \sum_{l \in L, l \neq 0} \frac{1}{l^4}$$

$$g_3 = 140 \sum_{l \in L, l \neq 0} \frac{1}{l^6}$$

Vi har altså en afbildning:

$$(p, p') : \mathbb{C}/L \rightarrow \overline{E(\mathbb{C})}$$

hvor  $E$  er den elliptiske kurve med ligningen

$$y^2 = 4x^3 - g_2x - g_3$$

Den elliptiske kurve  $\overline{E(\mathbb{C})}$  bliver identificeret med  $\mathbb{C}/L$ , som er en torus.

Inversionsproblemet er nu om det altid er tilfældet.

Altså om der til enhver elliptisk kurve  $E$  findes et gitter  $L$  i  $\mathbb{C}$ , så

$$\mathbb{C}/L \sim \overline{E(\mathbb{C})}$$

via Weierstrass  $\wp$  funktioner som netop beskrevet.

Svaret er JA!

## Elliptiske kurver over $\mathbb{Z}/p\mathbb{Z}$

Ligningen til en elliptiske kurve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

kan vi i det tilfælde, at  $a_i \in \mathbb{Z}$  løse modulo  $p$  for et givet primtal  $p$

Vi søger altså restklasser

$$x, y = 0, 1, \dots, p - 1$$

så

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$$

altså så

$$p \mid y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$$

Lad

$$|E(\mathbb{Z}/p\mathbb{Z})|$$

være antallet af løsninger.

$$b_p := p - |E(\mathbb{Z}/p\mathbb{Z})|$$

Betragt den elliptiske kurve med ligningen

$$y^2 + y = x^3 + x^2 + 10x + 20$$

For  $p = 2$  er der fire løsninger, nemlig

$$(0, 0), (0, 1), (1, 0), (1, 1)$$

hvorfor  $b_2 = 2 - 4 = -2$ .

For  $p = 3$  er der også fire løsninger, nemlig

$$(1, 0), (1, 2), (2, 0), (2, 2)$$

og  $b_3 = 3 - 4 = -1$ .

Værdierne for  $b_p$  for  $p \leq 71$  er angivet i tabellen.

## Cusp former af niveau $N$

En holomorf funktion:

$$f : \mathbb{H} \rightarrow \mathbb{C}$$

fra den øvre komplekse halvplan

$$\mathbb{H} := \{z = x + iy \mid y > 0\} \subset \mathbb{C}$$

$$\Gamma_0(N) = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right), \quad ad - bc = 1, \quad N|c$$

Så skal  $f$  opfylde funktionalligningen:

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^2 f(z)$$

for alle  $\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma_0(N)$

Endelig skal  $q$ -ekspansionen have lutter positive led:

$$f(z) = \sum_{n=1}^{\infty} c_n q^n, \quad q = e^{2\pi iz}$$

$q$ -ekspansion

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$$

hvorfor  $f(x + iy)$  er periodisk i  $x$ :

$$f(z + 1) = f(z)$$

Fourierrække udvikling for fast  $y$ :

$$\sum_{n=-\infty}^{\infty} a_n(y) e^{2\pi i n x} = \sum_{n=-\infty}^{\infty} c_n e^{2\pi i n z}$$

$$c_n = \int_{-\frac{1}{2}}^{\frac{1}{2}} f(x + iy) e^{-2\pi i n z} dx$$

bliver uafhængig af  $y$ .

$$f(z) = \sum_{n=-\infty}^{\infty} c_n q^n, \quad q = e^{2\pi i z}$$

Funktion  $f$  defineret ved det uendelige produkt er en cusp form af niveau 11:

$$f(z) := q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2, \quad q = e^{2\pi iz}$$

Mere generelt ( $p$  primtal,  $p \equiv -1 \pmod{12}$ ) er  $f$  en cusp form af niveau  $p$ :

$$f(z) := q^{\frac{p+1}{12}} \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{pn})^2, \quad q = e^{2\pi iz}$$

Cusp-formerne af niveau  $N$  et vektorrum  $S(N)$ , hvis dimension er kendt for alle  $N$ .

Specielt er

$$\dim S(p) = n + 1 \quad \text{hvis} \quad p = 12n + 11$$

## Hecke operatorer

$S(N)$  er udstyret med lineære afbildninger:

$$T(n) : S(N) \rightarrow S(N), \quad n \geq 1$$

Hvis  $p$  er et primtal, der ikke går op i  $N$ :

$$T(p^r)T(p) = T(p^{r+1}) + pT(p^{r-1})$$

$$T(p) : \sum_{n=1}^{\infty} c_n q^n \mapsto \sum_{n=1}^{\infty} c_{pn} q^n + p \sum_{n=1}^{\infty} c_n q^{pn}$$

Hvis  $p$  er et primtal, der går op i  $N$ :

$$T(p^r) = T(p)^r$$

$$T(p) : \sum_{n=1}^{\infty} c_n q^n \mapsto \sum_{n=1}^{\infty} c_{pn} q^n$$

Hvis  $m$  og  $n$  er indbyrdes primiske:

$$T(m)T(n) = T(mn)$$

# Eigenform

En eigenform er en fælles egenvektor for alle  $T(n)$ . Lad

$$f(z) = \sum_{n=1}^{\infty} c_n q^n$$

være en eigenform, normaliseret så  $c_1 = 1$ . Egenværdien for  $T(n)$  er  $c_n$

Vi får ved at bruge udtrykkene for  $T(n)$ .

- Hvis  $p$  er et primtal, der ikke går op i  $N$ :

$$c_{p^r} c_p = c_{p^{r+1}} + p c_{p^{r-1}}$$

- Hvis  $p$  er et primtal, der går op i  $N$ :

$$c_{p^r} = (c_p)^r$$

- Hvis  $m, n$  er indbyrdes primiske:

$$c_m c_n = c_{mn}$$

# Invariant differential

Differentialet

$$f(z)dz, \quad f \in S(N)$$

er invariant under  $\Gamma_0(N)$ :

$$f(\gamma(z))d(\gamma(z)) = f\left(\frac{az+b}{cz+d}\right) \frac{(bz+d)a - c(az+d)}{(cz+d)^2} dz = f(z)dz$$

Det bevirker (Cauchy's integralsætning), at

$$\Theta(\gamma) := \int_{\tau_0}^{\gamma(\tau_0)} f(z)dz$$

er uafhængigt af valg af  $\tau_0 \in \mathbb{H}$  og at

$$\Theta : \Gamma_0(N) \rightarrow \mathbb{C}$$

er en gruppehomomorfi. Billedet er et gitter  $L \subset \mathbb{C}$

## Elliptisk kurve knyttet til modulær form

Betragt for et  $\tau_0 \in \mathbb{H}$  afbildningen

$$F : \mathbb{H} \rightarrow \mathbb{C}$$
$$\tau \mapsto \int_{\tau_0}^{\tau} f(z) dz$$

Så er

$$(F(\gamma(z))) = F(z) + \Theta(\gamma)$$

$F$  giver altså anledning til en afbildning fra banerne

$$\Gamma_0(N) \backslash \mathbb{H}$$

til

$$\mathbb{C}/L$$

og dermed til en elliptisk kurve  $E$ , som så kaldes modulær.

Her sker der (mindst) to mirakler

- Konstruktionen kan gennemføres over  $\mathbb{Q}$
- Koefficienterne i  $q$ -ekspansionen til eigenformen  $f$  er  $p - |E(\mathbb{Z}/p\mathbb{Z})|$  for alle pånær endelig mange  $p$ .
- Igennem den modulære parametrisering

$$\Gamma_0(N)\backslash\mathbb{H} \rightarrow E$$

arver  $E$  symmetrierne fra  $\Gamma_0(N)\backslash\mathbb{H}$ . Det er

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N)$$

der har orden

$$N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

## Taniyama-Shimura-Weil's formodning

Enhver elliptisk kurve over  $\mathbb{Q}$  er isogen med en elliptisk kurve, der fremkommer ved Eichler-Shimura konstruktionen ud fra en eigenform  $f$ .

Det er det Wiles har vist for en stor klasse af elliptiske kurver (omfattende Frey kurverne).

Fra anden side var det vist (Frey-Serre-Ribet), at Frey kurverne ikke kunne konstrueres på denne måde. Dermed findes den hypotetiske løsning til Fermat ligningen ikke, og Fermat's sidste sætning er bevist.

# Projekt

Udgangspunkt den modulære form på side 2.

Er det en eigenform?

Bestem gitteret  $L$  hørende til formen. Her kan anvendes, at  $\Gamma_0(11)$  er frembragt af

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 1 \\ -33 & -4 \end{pmatrix}, \begin{pmatrix} 9 & 1 \\ -55 & -6 \end{pmatrix}$$

Bestem dernæst Weierstrass ligningen for den elliptiske kurve hørende til  $L$

Bestem  $j$ -invarianterne for den fundne Weierstrass ligning og ligningen på side 3.