Sir Andrew John Wiles,
Abelprisvinner 2016

MODULARITETSTEOREMET

Modularitetsteoremet sier at enhver elliptisk kurve definert over de rasjonale tallene er modulær. I dette notatet skal vi se på bakgrunnen for teoremet og beskrive de to hovedbegrepene som inngår, elliptiske kurver og modulære former.

La $\mathbb{H}$ være øvre halvplan av det komplekse planet, dvs. alle komplekse tall med positiv imaginærdel. En **modulær form** av vekt $2k$ for et positivt heltall k er en holomorf funksjon f på $\mathbb{H}$, som er slik at for alle heltallige 2×2-matriser $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ så er

$$f(\alpha z) = (cz + d)^{2k} f(z)$$

og hvor f også er holomorf i det uendelig fjerne punktet, dvs. når $z \to i\infty$.

Virkningen av 2×2-matrisen α på $z \in \mathbb{H}$ er gitt ved Möbiustransformasjonen

$$z \mapsto \frac{az + b}{cz + d}$$

Ved å substituere $\alpha = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ ser vi at

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

dvs. at funksjonen er translasjons-invariant. Siden

$$e^{2\pi i(z+1)} = e^{2\pi iz + 2\pi i} = e^{2\pi iz}$$

kan vi dermed uttrykke f som en funksjon av $q = e^{2\pi iz}$. Betingelsen at f er holomorf i $z = i\infty$ er ekvivalent med at funksjonen er holomorf i $q = 0$, så vi kan skrive

$$f(z) = \sum_{n \geq 0} a_n \, q^n, \quad q = e^{2\pi iz}$$

En berømt modulær form er den såkalte **diskriminantfunksjonen**,

$$\Delta(z) = q \prod_{r=1}^{\infty} (1 - q^r)^{24}, \quad q = e^{2\pi iz}$$

Ved å bruke denne kan vi lage et annet eksempel på en modulær fom

$$f(z) = \sqrt[12]{\Delta(z)\Delta(11z)}$$

Fourier-utviklingen til f som en funksjon i q er gitt ved

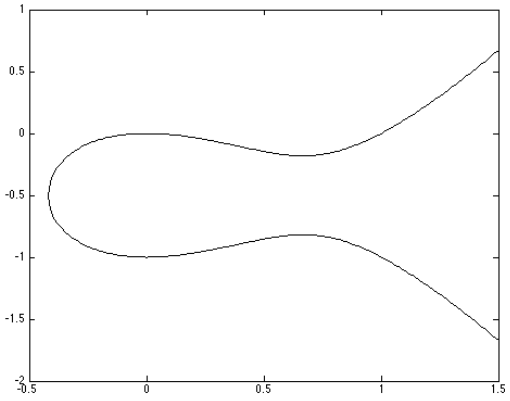
$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 \\ - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + \dots$$

Vi skal komme tilbake til denne rekken, først skal vi introdusere det andre sentrale begrepet, elliptiske kurver.

Elliptiske kurver er en klasse plane kurver definert ved polynomer av tredje grad. Likningen

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

er et eksempel på en **elliptisk kurve**.



Grafen til den elliptiske kurven

$$E = \{(x, y) \in \mathbb{R}^2 \mid y^2 + y = x^3 - x^2\}$$

Sir Andrew John Wiles, Abelprisvinner 2016

Vi er interessert i antall heltallsløsninger av likningen modulo et primtall p, dvs. vi ser etter løsninger blant restene $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ når vi deler med p. La for eksempel $p = 11$. Da vil $(x, y) = (10, 4)$ være en løsning av likningen $y^2 + y = x^3 - x^2$ fordi begge sider av likningen gir samme rest når vi deler med 11;

$$4^2 + 4 = 20 \equiv 9 \pmod{11}$$

og

$$10^3 - 10^2 = 900 \equiv 9 \pmod{11}$$

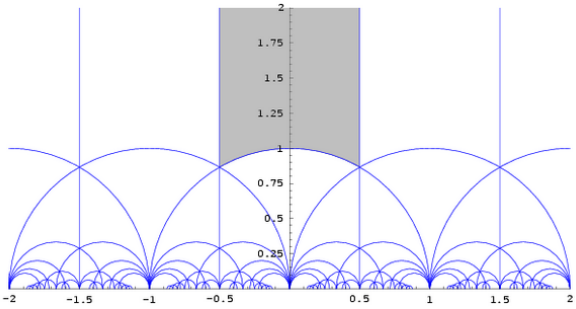
Generelt lar vi $\#E_p$ være antall løsninger av likningen i $\mathbb{Z}_p$. For hvert primtall p setter vi

$$a_p = p - \#E_p$$

I vårt eksempel har vi for $p = 2$ i alt 4 løsninger, $(0,0)$, $(0,1)$, $(1,0)$ og $(1,1)$, dvs. alle mulige rester utgjør løsninger, og dermed $a_2 = -2$. For $p = 3$ har vi også fire løsninger; $(0,0)$, $(0,2)$, $(1,0)$, $(1,2)$, som gir $a_3 = -1$. For de neste primtallene er tallene vi leter etter $a_5 = 1$ og $a_7 = -2$.

Det vi nå ser at for hvert primtall p, så vil tallet a_p for denne elliptiske kurven tilsvare q^p-Fourier-koeffisienten til den modulære formen $f(z) = \sqrt[12]{\Delta(z)\Delta(11z)}$ gitt over. Sammentreff av denne typen ble først observert av Tanyama og Shimura, og resulterte i TSW-formodningen. TSW-formodningen skiftet navn til Modularitetsteoremet etter at Wiles beviste at formodningen faktisk er sann. Wiles beviste at enhver semi-stabil elliptisk kurve er modulær. Det er en vakker måte å si at likheten mellom de to tallrekkene, Fourierkoeffisientene til den modulære formen og antallet løsninger modulo primtall til den elliptiske kurven, ikke er noen tilfeldighet.

Den siste delen i beviset for FLT stammer fra Gerhard Frey. Han påsto at dersom det finnes en ikke-triviell løsning av FLT, så vil det også finnes en ikke-modulær elliptisk kurve. Denne formodningen ble utviklet videre av Jean-Pierre Serre og senere bevist av Ken Ribet. Sammen med modularitetsteoremet gir dette et bevis for FLT.



Figuren illustrerer virkningen av den modulære gruppa $SL_2(\mathbb{Z})$ på det øvre halvplanet. Det skraverte området kalles ofte fundamentalområdet.

p	$\#E_p$	a_p
2	4	-2
3	4	-1
5	4	1
7	9	-2
11	10	1
13	9	4
17	19	-2
19	19	0

Sammenlign sekvensen av tall i høyre kolonne med primtalls-koeffisientene i Fourier-utviklingen til den modulære formen $\sqrt[12]{\Delta(z)\Delta(11z)}$ gitt på forrige side.