

*Birch og Swinnerton-Dyer formodningen*

*Foredrag i Eulers Venner*

*30. nov. 2004*

Johan P. Hansen

matjph@imf.au.dk

Institut for Matematiske Fag

Aarhus Universitet



# Diofantiske ligninger

Et polynomium  $f(x, y)$  (med koefficienter fra de rationale tal  $\mathbb{Q}$ ) giver anledning til en diofantisk ligning (Diofantos, ca. 250 år e. kr.)

$$f(x, y) = 0$$

Bestem de rationale løsninger, altså mængden

$$\{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid f(x, y) = 0\}$$

- $x^2 + y^2 = 1$ , Pythagoræiske tripler, uendelig mange f. eks.  $(\frac{3}{5}, \frac{4}{5}), (\frac{5}{13}, \frac{12}{13}), \dots$
- $x^n + y^n = 1$ ,  $n \geq 3$ , Fermats sidste sætning: Kun  $(0, \pm 1), (\pm 1, 0)$  er løsninger (Andrew Wiles, 1995)
- $y^2 = x^3 + ax + b$ ,  $\Delta = 4a^2 + 27b^3 \neq 0$



# Diofantiske ligninger af grad 1 og 2

- De simpleste diofantiske ligninger er lineære og kan umiddelbart løses over  $\mathbb{Q}$ .
- Kvadratiske ligninger løses af en kraftfuld metode af Hasse og Minkowski:
  - Løs den kvadratiske ligning modulo  $p$  (primtal) [ kvadratisk reciprocitet]
  - Brug dette til at løse ligningen over komplette lokale legemer  $\mathbb{Q}_p$  [Hensels lemma]
  - Informationerne bruges til at sammenstykke en eventuel løsning over  $\mathbb{Q}$  [Hasse princippet]
  - Har kurven en rational løsning kan den parametriseres med rationale funktioner, og der er uendelig mange rationale løsninger, som f. eks. i tilfældet  $x^2 + y^2 = 1$



# Diofantiske ligninger og diofantisk geometri. Genus

En (diofantisk ligning) giver anledning til en kurve - et specialtilfælde af en algebraisk varietet. Dette synspunkt giver anledning til at anvende geometriske metoder.

- Til enhver kurve, kan der knyttes et helt tal  $g \geq 0$  - kurvens *genus*
- Kurver med lineære og kvadratiske ligninger har genus 0
- Hilbert og Hurwitz (1890) viste, at enhver kurve af genus 0 kan reduceres til at have en lineær eller kvadratisk ligning

Genus  $g = 0$  tilfældet er altså løst i og med det blot er et spørgsmål om, at løse lineære eller kvadratiske diofantiske ligninger.



# Diofantiske geometri. Genus $g \geq 2$

- En kurve med ligning  $x^n + y^n = 1, n \geq 4$  har  $g = \frac{(n-1)(n-2)}{2} \geq 2$
- Mordell formodede og i 1983 viste Faltings: *Hvis der om kurvens genus  $g$  gælder, at  $g \geq 2$ , så er der kun endelig mange rationale punkter (punkter med koordinater i  $\mathbb{Q}$ ).*
- Sætningen og metoden gav ingen øvre begrænsning på antallet af rationale punkter og viser dermed ikke Fermats sidste sætning.



# Diofantiske geometri. Genus $g = 1$

Det efterlader  $g = 1$  tilfældet til behandling og situationen er meget mere nuanceret:

- Der er ingen kendt metode til at afgøre, hvorvidt en given kurve har eller ikke har punkter med rationale koordinater
- Der er eksempler på:
  - kurver med endelig mange punkter med rationale koordinater
  - kurver med uendelig mange punkter med rationale koordinater

Forudsætter vi, at kurven har mindst et punkt med rationale koordinater har den efter passende koordinatskift en ligning på formen

$$y^2 = x^3 + ax + b, \quad \Delta = 4a^2 + 27b^3 \neq 0$$



# Birch og Swinnerton-Dyer formodningen

Løsningerne  $(x, y)$  over de rationale tal  $\mathbb{Q}$  til ligningen

$$E : y^2 = x^3 + ax + b$$

udgør en gruppe. Punkterne  $P = (x, y)$  af endelig orden udgør en endelig gruppe  $E_{tors}(\mathbb{Q})$  og

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r, \quad (\text{Mordell 1922})$$



# Birch og Swinnerton-Dyer formodningen

Løsningerne  $(x, y)$  over de rationale tal  $\mathbb{Q}$  til ligningen

$$E : y^2 = x^3 + ax + b$$

udgør en gruppe. Punkterne  $P = (x, y)$  af endelig orden udgør en endelig gruppe  $E_{tors}(\mathbb{Q})$  og

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r, \quad (\text{Mordell 1922})$$

Ud fra løsningsantallet til  $E$  modulo hvert primtal konstrueres en funktion  $L(s)$ .  
*Birch og Swinnerton-Dyer formodningen:* Taylor rækken for  $L(s)$  i  $s = 1$  er

$$L(s) = c(s - 1)^r + \text{højere ordens led}, \quad c \neq 0$$





# Birch og Swinnerton-Dyer formodningen

Løsningerne  $(x, y)$  over de rationale tal  $\mathbb{Q}$  til ligningen

$$E : y^2 = x^3 + ax + b$$

udgør en gruppe. Punkterne  $P = (x, y)$  af endelig orden udgør en endelig gruppe  $E_{tors}(\mathbb{Q})$  og

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r, \quad (\text{Mordell 1922})$$

Ud fra løsningsantallet til  $E$  modulo hvert primtal konstrueres en funktion  $L(s)$ . *Birch og Swinnerton-Dyer formodningen*: Taylor rækken for  $L(s)$  i  $s = 1$  er

$$L(s) = c(s-1)^r + \text{højere ordens led}, \quad c \neq 0$$



# Punktantal på elliptiske kurver over $\mathbb{Z}/p\mathbb{Z}$

For ethvert primtal  $p$ , der ikke er divisor i  $\Delta$ , sættes

$$N_p := \#\{(x, y) \mid y^2 \equiv x^3 + ax + b \pmod{p}\}$$

Heuristisk er  $N_p$  stort set lig med  $p$ . Afvigelsen benævner vi

$$a_p := p - N_p, \quad |a_p| \leq 2\sqrt{p} \quad (\text{Hasse}) \quad (1)$$

Eksempel  $y^2 = x^3 + 7x$ ,  $\Delta = 4 \cdot 7^3$  har:

$p$	3	5	7	11	13	17
$N_p$	3	1		9	17	9
$a_p$	0	4		2	-4	8



# Euler-produktet og Dirichlet-rækken

Ud fra tallene  $a_p$ , ( $p$  primtal) dannes (det ufuldstændige) Euler-produkt

$$L(s) := \prod_{p \nmid 2\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

$L(s)$  kan udtrykkes som en Dirichlet-række

$$L(s) = \sum_{n \geq 1} a_n n^{-s}$$

- På næste side vil vi bevise, at rækken konvergerer og dermed definerer en analytisk funktion på en kompleks halvplan, nemlig de  $s \in \mathbb{C}$  med  $\operatorname{Re} s > \frac{3}{2}$ . Af beviset følger formler for  $a_n$
- Hasse formodede, at  $L(s)$  kunne udvides analytisk til hele den komplekse plan
- Det er nu (1995) vist som følge af Wiles arbejde med beviset for Fermats sidste sætning



# Euler-produktet og Dirichlet-rækken. Konvergens

Nævnerpolynomiet  $1 - a_p X + pX^2$  har ifølge (1) negativ diskriminant  $a_p^2 - 4p \leq 0$ , hvorfor der kan faktoriseres

$$\frac{1}{1 - a_p X + pX^2} = \frac{1}{(1 - r_p X)(1 - \bar{r}_p X)} \text{ med } |r_p| = |\bar{r}_p| = \sqrt{p}. \quad (2)$$

Da  $\frac{1}{(1-rX)} = \sum_{i=0}^{\infty} r^i X^i$ , giver entydig faktorisering i primtalsprodukt, at

$$\prod_{p \nmid 2\Delta} \frac{1}{1 - r_p p^{-s}} = \sum_{n=p_1^{s_1} \dots p_k^{s_k}} \overbrace{(r_{p_1})^{s_1} \dots (r_{p_k})^{s_k}}^{c_n} n^{-s} = \sum_{n=p_1^{s_1} \dots p_k^{s_k}} c_n n^{-s}.$$

Da  $|c_n| = \sqrt{n}$ , er rækken konvergent for de  $s \in \mathbb{C}$ , der har  $\operatorname{Re}(\frac{1}{2} - s) < -1$ .

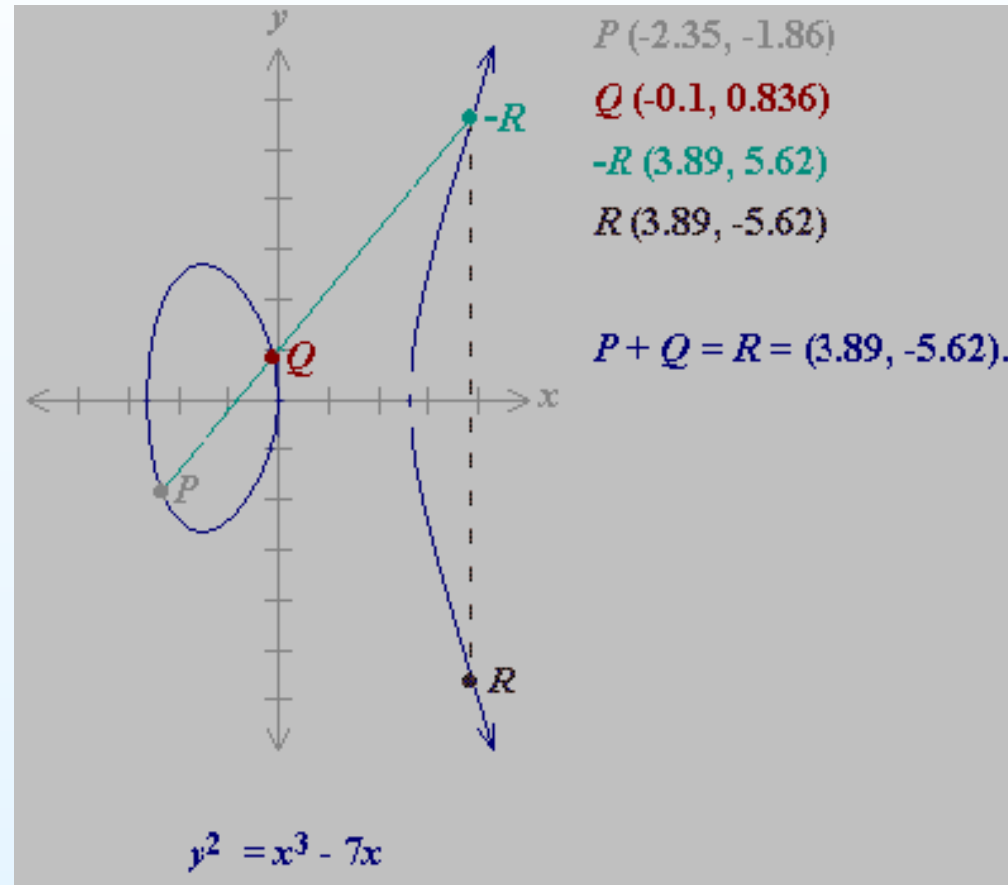
Konvergens for  $L(s)$  følger nu af (2):

$$L(s) = \left( \prod_{p \nmid 2\Delta} \frac{1}{1 - r_p p^{-s}} \right) \left( \prod_{p \nmid 2\Delta} \frac{1}{1 - \bar{r}_p p^{-s}} \right)$$



# Gruppestruktur - geometrisk formulering

Punkterne på  $E$  og et punkt  $\mathcal{O}$  (i uendelig) udgør en Abelsk gruppe.



Hvis linien  $\overline{PQ}$  er lodret er  $P + Q = \mathcal{O}$  ellers er  $P + Q = R$ .  
Endelig er  $P + \mathcal{O} = P$ .



# Gruppestuktur - $E(\mathbb{Q})$ en Abelsk gruppe

$$E : y^2 = x^3 + ax + b, \quad \Delta = 4a^2 + 27b^3 \neq 0$$

Lad  $P = (x_1, y_2)$ ,  $Q = (x_2, y_2)$  og  $-R = (x_3, y_3)$  være de tre skærningspunkter mellem  $E$  og linien  $\overline{PQ}$ . Hvis linien har en ligning på formen  $x = x_1$  sættes  $P + Q = \mathcal{O}$  ellers har  $P + Q$  koordinaterne

$$P + Q = \left( \alpha^2 - x_1 - x_2, -\alpha x_3 - (y_1 - \alpha x_1) \right),$$

hvor

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1}, \text{ hvis } (P \neq Q) \quad \text{og} \quad \alpha = \frac{3x^2 + a}{2y}, \text{ hvis } (P = Q, y \neq 0)$$

Bemærk at det er rationale udtryk, altså kan beregnes over ethvert legeme. Specielt er  $E(\mathbb{Q})$  en Abelsk gruppe.



# Gruppestruktur - algebraisk udredning

Ligningen for  $\overline{PQ}$  er under den givne betingelse på formen:

$$y = \alpha x + (y_1 - \alpha x_1),$$

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1}, \text{ hvis } (P \neq Q) \quad \text{og} \quad \alpha = \frac{3x^2 + a}{2y}, \text{ hvis } (P = Q, y \neq 0).$$

Førstekordinaterne  $x_1, x_2, x_3$  er løsninger til trediegradsligningen:

$$(\alpha x + (y_1 - \alpha x_1))^2 = x^3 + ax + b,$$

hvor koefficienten til  $x^2$  er  $\alpha^2$ . Derfor er

$$x_1 + x_2 + x_3 = \alpha^2 \Rightarrow x_3 = \alpha^2 - x_1 - x_2 \Rightarrow y_3 = \alpha x_3 + (y_1 - \alpha x_1).$$



# Mordells sætning: $E(\mathbb{Q})$ endelig frembragt

Vi har set, at punkterne  $P = (x, y)$ , hvor koordinaterne  $x, y \in \mathbb{Q}$  er løsninger til ligningen

$$E : y^2 = x^3 + ax + b$$

sammen med  $\mathcal{O}$  udgør en Abelsk gruppe.

I 1922 viste Mordell, at der findes endelig mange punkter  $P_1, \dots, P_k \in E(\mathbb{Q})$ , der frembringer  $E(\mathbb{Q})$ . Altså ethvert  $P \in E(\mathbb{Q})$  er på formen:

$$P = n_1 \cdot P_1 + \dots + n_k \cdot P_k, \quad n_i \in \mathbb{Z}.$$

Nogle af disse frembringerpunkter har endelig orden og frembringer torsionsundergruppen  $E_{tors}(\mathbb{Q})$ , der er endelig, de øvrige frembringer en fri gruppe.





# Mordells sætning: $E(\mathbb{Q})$ endelig frembragt - rangen

---

Det indebærer, at vi har en isomorfi af grupper

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r, \quad (\text{Mordell 1922})$$

Tallet  $r$  kaldes rangen af  $E$ .



# Mordells sætning: $E(\mathbb{Q})$ endelig frembragt - rangen

Det indebærer, at vi har en isomorfi af grupper

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r, \quad (\text{Mordell 1922})$$

Tallet  $r$  kaldes rangen af  $E$ .

- Rangen er vanskelig, at bestemme.
- Det formodes, at der findes elliptiske kurver af vilkårlig høj rang.



# Mordells sætning: $E(\mathbb{Q})$ endelig frembragt - rangen

Det indebærer, at vi har en isomorfi af grupper

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r, \quad (\text{Mordell 1922})$$

Tallet  $r$  kaldes rangen af  $E$ .

- Rangen er vanskelig, at bestemme.
- Det formodes, at der findes elliptiske kurver af vilkårlig høj rang.



# Elliptiske kurver med rang 0, 1 og 2

- Kurven med ligningen

$$y^2 = x^3 + 7x$$

har rang 0.

- Kurven med ligningen

$$y^2 = x^3 + 5x$$

har rang 1. Punktet  $(\frac{1}{4}, \frac{9}{8})$  er en frembringer.

- Kurven med ligningen

$$y^2 = x^3 + 73x$$

har rang 2. Punkterne  $(\frac{9}{16}, \frac{411}{64})$ ,  $(36, 222)$  er uafhængige frembringere.



# Birch og Swinnerton-Dyer formodningen

---

Lad  $E$  være en elliptisk kurve med ligningen

$$y^2 = x^3 + ax + b, \quad \Delta = 4a^2 + 27b^3 \neq 0$$

Så er

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r$$



# Birch og Swinnerton-Dyer formodningen

Lad  $E$  være en elliptisk kurve med ligningen

$$y^2 = x^3 + ax + b, \quad \Delta = 4a^2 + 27b^3 \neq 0$$

Så er

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r$$

Lad

$$L(s) := \prod_{p \nmid 2\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}, \quad a_p := p - N_p, \quad N_p := \#\{(x, y) | y^2 \equiv x^3 + ax + b \pmod{p}\}$$

*Birch og Swinnerton-Dyer formodningen* er nu, at Taylor rækken for  $L(s)$  i  $s = 1$  er

$$L(s) = c(s-1)^r + \text{højere ordens led}, \quad c \neq 0$$



# Birch og Swinnerton-Dyer formodningen

Lad  $E$  være en elliptisk kurve med ligningen

$$y^2 = x^3 + ax + b, \quad \Delta = 4a^2 + 27b^3 \neq 0$$

Så er

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r$$

Lad

$$L(s) := \prod_{p \nmid 2\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}, \quad a_p := p - N_p, \quad N_p := \#\{(x, y) \mid y^2 \equiv x^3 + ax + b \pmod{p}\}$$

*Birch og Swinnerton-Dyer formodningen* er nu, at Taylor rækken for  $L(s)$  i  $s = 1$  er

$$L(s) = c(s-1)^r + \text{højere ordens led}, \quad c \neq 0$$



# Status

Birch og Swinnerton-Dyer formodningen er kun vist i specialtilfælde:

- I 1976 viste J. Coates and A. Wiles, at en elliptisk kurve med kompleks multiplikation og med  $L(1) \neq 0$  kun har endelig mange rationale punkter, altså er rangen lig med 0.
- I 1983 viste B. Gross and D. Zagier, at en modulær elliptisk kurve, hvor  $L(s)$  har et simpelt nulpunkt for  $s = 1$ , faktisk har et rationalt punkt af uendelig orden, altså er rangen  $> 0$ .
- I 1990 viste V. Kolyvagin, at en modulær elliptisk kurve med  $L(1) \neq 0$  har rang 0 og en modulær elliptisk kurve, hvor  $L(s)$  har et simpelt nulpunkt for  $s = 1$ , har rang 1.
- I 1999 viste A. Wiles og R. Taylor, at alle elliptiske kurver er modulære (Taniyama-Shimura), hvorved de to ovenstående resultater gælder for alle elliptiske kurver.





# Tilblivelsen af Birch og Swinnerton-Dyer formodningen

I begyndelsen af 60'erne beregnede Birch og Swinnerton-Dyer (Cambridge University)  $N_p$  for elliptiske kurver med kendt rang  $r$  for rigtig mange primtal  $p$ .

Fra dette talmateriale fremsatte de formodningen om en asymptotisk lov:

$$\prod_{p < x} \frac{N_p}{p} \approx \log(x)^r \text{ for } x \rightarrow \infty.$$

Det førte dem til (1965) at fremsætte Birch og Swinnerton-Dyer formodningen. Det var dristigt - på daværende tidspunkt viste man ikke, at  $L(s)$  kunne fortsættes analytisk til  $s = 1$ , dengang var det blot vist for kurver med kompleks multiplikation (Deuring).



# Birch og Swinnerton-Dyer formodningen - stærk form

Formodningen udvidede de yderligere (1982) til at omfatte en formel for konstanten  $c$  i Taylorrækken for  $L(s)$  i  $s = 1$  udtrykt ved invarianter knyttet til  $E$ :

$$c = \lim_{s \rightarrow 1} \frac{L(s)}{(s-1)^r} = 2^r \Omega \frac{\#\text{III}(E/\mathbb{Q}) R(E/\mathbb{Q}) \prod_p c_p}{(\#E_{tors}(\mathbb{Q}))^2}$$

Her er  $\text{III}(E/\mathbb{Q})$ , den såkaldte Shafarevich-Tate gruppe.

J. Tate:

*“This remarkable conjecture relates the behavior of a function  $L(s)$  at a point where it is not at present known to be defined to the order of a group  $\text{III}(E/\mathbb{Q})$  which is not known to be finite!”*

