

Mordell's Sætning

Henrik Christensen og Michael Pedersen

17. december 2003

Mordells sætning siger at gruppen $C(\mathbb{Q})$ af rationale punkter over en ellipse C er en endeligt frembragt abelsk gruppe. Elliptiske kurver kan beskrives ved Weierstrass ligningen. Da \mathbb{Q} er et legeme med $\text{Char} \neq 2, 3$ kan vi skrive Weierstrass ligningen for vores elliptiske kurve som

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

Af litteratur har vi hovedsageligt brugt "Rational Points on Elliptic Curves" af J. H. Silverman og J. Tate, men også skelet lidt til "The Arithmetic of Elliptic Curves" af J. H. Silverman.

1 Højdefunktionen

Lad $x = \frac{m}{n} \in \mathbb{Q}$ så definerer vi højden af x til at være $H(x) = \max\{|m|, |n|\}$. Denne funktion har følgende vigtige egenskaber:

1) For ethvert positivt tal M , er mængden $\{x \mid H(x) \leq M\}$ endelig.

- I tælleren har vi mulighederne $-M, \dots, 0, \dots, M$ og i nævneren er der de samme muligheder bortset fra 0.

Lad nu $P = (x, y)$ være et rationelt punkt på kurven C , så definerer vi højden af P til at være højden af x -koordinaten, dvs $H(P) = H(x)$.

Desuden indfører vi $h(P) = \log(H(P))$.

Når 1) gælder for $H(x)$ er det nemt at se at den også gælder for $h(x)$, dvs $\{x \mid h(x) \leq M\}$ er endelig.

For punktet \mathcal{O} sætter vi $H(\mathcal{O}) = 1$ og dermed $h(\mathcal{O}) = 0$.

Egenskaben 1) kan vi nemt udvide til punkter P på C . Til alle punkter under en vis højde er der kun endelig mange muligheder for x -koordinaten og til hver x -koordinat er der kun 2 muligheder for y -koordinaten, så vi har altså følgende lemma:

Lemma 1.1. *For ethvert positivt reelt tal M er mængden $\{P \in C(\mathbb{Q}) \mid h(P) \leq M\}$ endelig*

For at vise Mordell's sætning skal vi desuden bruge yderligere 2 lemmaer, samt den svage udgave af Mordell's sætning som vi vil skitsere et bevis for i næste afsnit:

Lemma 1.2. *Lad P_0 være et rationelt punkt på C , så eksisterer en konstant κ_0 som afhænger af P_0 , a , b og c , så $h(P + P_0) \leq 2h(P) + \kappa_0$ for alle $P \in C(\mathbb{Q})$*

Lemma 1.3. *Der eksisterer en konstant κ som afhænger af a , b og c , så $h(2P) \geq 4h(P) - \kappa$ for alle $P \in C(\mathbb{Q})$*

Lemma 1.2 og 1.3 lader vi stå uden bevis.

2 Den svage udgave af Mordell's sætning

Den svage udgave af Mordells sætning er:

Sætning 2.1. *Lad $m \in \mathbb{N}$, så er ordenen af $C(\mathbb{Q})/mC(\mathbb{Q})$ endelig*

For at vise den stærke udgave kan vi nøjes med at kigge på tilfældet $m=2$:

Ordenen af $C(\mathbb{Q})/2C(\mathbb{Q})$ er endelig

hvor vi med $2C(\mathbb{Q})$ mener billedet af afbildningen

$$C(\mathbb{Q}) \longrightarrow C(\mathbb{Q})$$

$$P \longrightarrow P + P$$

Vi skitserer et bevis for sætning 2.1 ved at opskrive 2 propositioner (2.2, 2.3) samt et rent algebraisk lemma (2.4).

I dette "bevis" begrænser vi os til mængden af elliptiske kurver hvor $f(x) = x^3 + ax^2 + bx + c$ har en rational rod x_0 , hvilket er ensbetydende med at kurven har et rationalt punkt af orden 2. Da a , b og c kan antages at være hele tal må x_0 være et helt tal. Vi kan derfor lave en transformation af C så $(x_0, 0)$ ryger over i $T = (0, 0)$, og vi får dermed en ligning på formen $y^2 = x^3 + ax^2 + bx$. Denne transformation ændrer ikke på gruppen $C(\mathbb{Q})$.

Idéen i beviset er at dele $P \rightarrow 2P$ op i to "mindre" afbildninger φ og ψ så $\psi \circ \varphi(P) = 2P$. Afbildningerne φ og ψ går ikke fra $C \rightarrow C$ men derimod gennem en ny kurve \bar{C} , dvs $C \xrightarrow{\varphi} \bar{C} \xrightarrow{\psi} C$, hvor C og \bar{C} er to elliptiske kurver givet ved

$$C : y^2 = x^3 + ax^2 + bx$$

$$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

$$\text{hvor } \bar{a} = -2a \text{ og } \bar{b} = a^2 - 4b$$

Hvis vi på sammen måde laver $\bar{\bar{C}}$ ses det, at denne må være givet ved ligningen $y^2 = x^3 + 4ax^2 + 16bx$, så vi har en isomorfi mellem $\bar{\bar{C}}$ og C givet ved $(x, y) \rightarrow (\frac{x}{4}, \frac{y}{8})$.

Lad os nu se på afbildningerne φ og ψ :

Proposition 2.2. a) Lad $\varphi : C \rightarrow \bar{C}$ være givet ved

$$\varphi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}) & \text{for } P = (x, y) \neq \mathcal{O}, T \\ \bar{\mathcal{O}} & \text{for } P = \mathcal{O} \text{ eller } P = T \end{cases}$$

Så er φ en homomorfi og $\ker(\varphi) = \{\mathcal{O}, T\}$

b) Ved at bruge a) får vi en homomorfi $\bar{\varphi} : \bar{C} \rightarrow \bar{\bar{C}}$. Da $\bar{\bar{C}}$ og C er isomorfe har vi en homomorfi:

$$\psi(\bar{P}) = \begin{cases} (\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}) & \text{for } \bar{P} = (\bar{x}, \bar{y}) \neq \bar{\mathcal{O}}, \bar{T} \\ \mathcal{O} & \text{for } \bar{P} = \bar{\mathcal{O}} \text{ eller } \bar{P} = \bar{T} \end{cases}$$

c) $\psi \circ \varphi : C \rightarrow C$ er multiplikation med 2, dvs $\psi \circ \varphi(P) = 2P$

Et lille kommutativt diagram så vi kan få lidt overblik:

$$\begin{array}{ccccc} C & \xrightarrow{\varphi} & \bar{C} & \xrightarrow{\bar{\varphi}} & \bar{\bar{C}} \\ & \searrow & & \searrow \psi & \downarrow \cong \text{ ved } (x,y) \rightarrow (\frac{x}{4}, \frac{y}{8}) \\ & & & & C \\ & & & & \uparrow 2P \\ & & & & C \end{array}$$

Lad os indføre lidt notation inden vi går videre til den næste proposition.

Lad \mathbb{Q}^* være den multiplikative gruppe af rationale tal forskellige fra 0.

Lad $\mathbb{Q}^{*2} = \{u^2 \mid u \in \mathbb{Q}^*\}$. Det ses at \mathbb{Q}^{*2} er en undergruppe af \mathbb{Q}^* .

Vi indfører en afbildning $\alpha : C(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ ved

$$\alpha(\mathcal{O}) = [1]$$

$$\alpha(T) = [b]$$

$$\alpha(x, y) = [x] \text{ for } x \neq 0$$

Vi påstår nu følgende proposition om afbildningen α

Proposition 2.3. a) $\alpha : C(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ er en homomorfi

b) $\ker(\alpha) = \psi(\bar{C})$, så vi har en injektiv afbildning

$$C/\psi(\bar{C}) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$

c) Lad p_1, p_2, \dots, p_t være forskellige primtal der går op i b . Så er billedet af α indeholdt i undergruppen af $\mathbb{Q}^*/\mathbb{Q}^{*2}$ der består af elementerne

$$\pm p_1^{n_1} p_2^{n_2} \dots p_t^{n_t} \text{ hvor } n_1, n_2, \dots, n_t \in \{0, 1\}$$

d) $|C/\psi(\bar{C})| \leq 2^{t+1}$

Hvis vi betragter d) kan vi se at vi er færdige når vi har vist:

Lemma 2.4. *Lad A og B være abelske grupper, og $\varphi : A \rightarrow B$ og $\psi : B \rightarrow A$ være to homomorfier, og antag at $\psi \circ \varphi(a) = 2a$ for alle $a \in A$ og $\varphi \circ \psi(b) = 2b$ for alle $b \in B$. Antag desuden at $|A/\psi(B)|$ og $|B/\varphi(A)|$ er endelig, så er $|A/2A|$ endelig og der gælder*

$$|A/2A| \leq |A/\psi(B)| \cdot |B/\varphi(A)|$$

3 Mordell's sætning

Ved at kombinere lemma 1.1, 1.2, 1.3 og sætning 2.1 (den svage Mordell sætning) kan vi vise Mordell's sætning (den stærke udgave):

Sætning 3.1. *Lad C være en glat kurve givet ved en ligning $y^2 = x^3 + ax^2 + bx + c$ med et rationelt punkt af orden 2, så er gruppen af rationelle punkter $C(\mathbb{Q})$ en endeligt frembragt abelsk gruppe*

Bevis

Sætning 2.1 giver os at ordenen af $C(\mathbb{Q})/2C(\mathbb{Q})$ er endelig. Lad os sige der er n elementer, så vi kan vælge en repræsentant til hver af sideklasserne i $C(\mathbb{Q})/2C(\mathbb{Q})$, dem kalder vi Q_1, Q_2, \dots, Q_n .

Lad nu $P \in C(\mathbb{Q})$ være et vilkårligt punkt, så må P ligge i en af sideklasserne, og dermed findes et index i_1 så

$$P - Q_{i_1} \in 2C(\mathbb{Q})$$

hvilket vil sige at der findes et $P_1 \in C(\mathbb{Q})$ så vi kan skrive

$$P - Q_{i_1} = 2P_1$$

Disse argumenter gentages for P_1 så vi kan skrive

$$P_1 - Q_{i_2} = 2P_2$$

og forsætter vi lidt endnu får vi

$$P_2 - Q_{i_3} = 2P_3$$

$$P_3 - Q_{i_4} = 2P_4$$

...

$$P_{m-1} - Q_{i_m} = 2P_m$$

Hvor alle $Q_{i_1}, Q_{i_2}, \dots, Q_{i_m}$ vælges blandt Q_1, Q_2, \dots, Q_n . Ved at indsætte alle disse ligninger i den første får vi

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + 8Q_{i_4} + \dots + 2^{m-1}Q_{i_{m-1}} + 2^m P_m$$

Vi mangler nu at vise at ved at vælge m stor nok får vi højden af P_m til at være begrænset. Når vi har gjort det, vil $C(\mathbb{Q})$ være frembragt af Q_i 'erne samt den endelige mængde af punkter med højde mindre end denne grænse.

Vi skal nu til at bruge lemma 1.2 og 1.3:

For alle Q_i bruger vi lemma 1.2 (hvor vi udskifter P_0 med $-Q_i$) og får dermed

$$h(P - Q_i) \leq 2h(P) + \kappa_i$$

da der er endelig mange Q_i kan vi finde den største af κ_i 'erne som vi kalder κ' , dvs

$$h(P - Q_i) \leq 2h(P) + \kappa' \text{ for alle } Q_i$$

Brug nu lemma 1.3 til at vurdere

$$\begin{aligned} 4h(P_j) &\leq h(2P_j) + \kappa \\ &= h(P_{j-1} - Q_{i_j}) + \kappa \\ &\leq 2h(P_{j-1}) + \kappa + \kappa' \\ &\Rightarrow \\ h(P_j) &\leq \frac{1}{2}h(P_{j-1}) + \frac{1}{4}(\kappa' + \kappa) \\ &= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa)) \end{aligned}$$

Dvs så længe vi har at $h(P_{j-1}) \geq \kappa' + \kappa$ får vi at

$$\begin{aligned} h(P_j) &\leq \frac{3}{4}h(P_{j-1}) \\ &\Downarrow \\ h(P_j) &\leq \left(\frac{3}{4}\right)^j h(P) \end{aligned}$$

men da $(\frac{3}{4})^j \rightarrow 0$ for $j \rightarrow \infty$ får vi at fra et vist trin, lad os sige m , må

$$h(P_m) \leq \kappa' + \kappa$$

Lemma 1.1 fortæller os at der nu kun kan være endelig mange punkter tilbage, så vi kan altså skrive ethvert punkt P som

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + 8Q_{i_4} + \dots + 2^{m-1}Q_{i_{m-1}} + 2^m R$$

for et punkt R som opfylder $h(R) \leq \kappa' + \kappa$. Vi har altså en endelig frembringende mængde:

$$\{Q_1, Q_2, \dots, Q_n\} \cup \{R \in C(\mathbb{Q}) \mid h(R) \leq \kappa' + \kappa\}$$