Selmergrupper – et historisk tilbakeblikk –

Loren D. Olson

Department of Mathematics and Statistics,
University of Tromsø,
N-9037 Tromsø, Norway
loren@math.uit.no

For ca. 60 år siden begynte Selmer på et omfattende prosjekt for å studere løsninger over $\mathbb{Q}$ til ligninger på formen $ax^3+by^3+cz^3 = 0$. Han oppdaget mye underveis som senere har hatt stor betydning for utviklingen i tallteori og aritmetisk algebraisk geometri.

1 Hasseprinsippet eller det lokale-globale prinsippet

Det har i lang tid vært en ledetråd i algebraisk tallteori, diofantiske ligninger og aritmetisk algebraisk geometri at man ønsker å studere et objekt globalt ved å studere det lokalt overalt. Dette kommer ofte til uttrykk når vi snakker om *Hasseprinsippet* eller det *lokale-globale prinsippet* som grovt sett er: En ligning over $\mathbb{Q}$ har en løsning i $\mathbb{Q}$ $\iff$ den har en reell løsning og løsninger over alle p-adiske kropper $\mathbb{Q}_p$, dvs. løsninger lokalt overalt.

Opphavet til dette er Hasse-Minkowski teoremet som sier at dette gjelder for kvadratiske former (over $\mathbb{Q}$ ved Minkowski (1890) og over en tallkropp ved Hasse (1924)). Har vi en ligning/varietet eller en klasse av ligninger/varieteter kan vi spørre om Hasseprinsippet gjelder for slike, eller ikke.

I 1951 publiserte Selmer en svær artikkel på 160 sider i *Acta Mathematica* der han ga mange eksempler på at Hasseprinsippet ikke gjaldt for kubiske former. Det enkleste er kanskje

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

Dette eksempelet trekkes i dag fram nesten hver gang man skal diskutere Hasseprinsippet.

2 Tre artikler av Selmer

Selmer publiserte tre artikler som er relevante for dette foredraget. De er:

1. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.* **85** (1951), s. 203-362.
2. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. Completion of the tables. *Acta Math.* **92** (1954), s. 191-197.
3. A conjecture concerning rational points on cubic curves. *Math. Scand.* **2** (1954), s. 49-54.

Utgangspunktet er kubiske ligninger på formen $ax^3 + by^3 + cz^3 = 0$ med a, b og c kubefrie heltall som er parvis innbyrdes prime der $A = abc$ er positivt. Slike definerer ikke-singulære plankurver D av genus 1. I tilknytning til disse studerer han inngående ligningen

$$X^3 + Y^3 = AZ^3 \tag{2.1}$$

for $A \in \mathbb{Z}, 1 \leq A \leq 500$.

Vi merker oss også at den første artikkelen ikke gjør bruk av datamaskiner i det hele tatt. Noen av løsningene som står i tabellene er derfor ganske imponerende. Som et eksempel, la $A = 284$. Selmer finner da for hånd følgende løsning:

$$\begin{aligned} x &= 111035496427236122887 \\ y &= -43257922194314055637 \\ z &= 16751541717010945845 \end{aligned}$$

I den andre artikkelen brukte han i 1952 en datamaskin på Princeton til å komplettere tabellene.

3 Elliptiske kurver og Mordell-Weil gruppa

La k være en kropp.

Definisjon 3.1. En *elliptisk kurve* E definert over en kropp k er en ikke-singulær kurve av genus 1 samt et k-rasjonalt punkt e på E.

Bemerkning 3.2. Fram til ca. 1966 var eksistensen av et k-rasjonalt punkt ikke med i definisjonen av elliptisk kurve.

La $E(k)$ være mengden av alle k-rasjonale punkter på E. $E(k)$ har en gruppestruktur med e som identitetselement. $E(k)$ kalles for *Mordell-Weil gruppa til* E.

Teorem 3.3. ***Mordell-Weil****. La k være en algebraisk tallkropp. $E(k)$ er endelig generert.*

Skriv $E(k) \cong E(k)_{tors} \oplus \mathbb{Z}^r$ der r er *rangen* til $E(k)$. $E(k)_{tors}$ er grei å beregne. Verre er det å beregne r og et sett generatorer for $E(k)$. Det var nok dette Selmer hadde som mål for de kurvene han undersøkte.

For $n > 1$ har vi $E(k)/nE(k) \cong E(k)_{tors}/nE(k)_{tors} \oplus (\mathbb{Z}/n\mathbb{Z})^r$. Det er viktig å få kjennskap til $E(k)/nE(k)$.

4 Weil-Châtelet og Tate-Šafarevič grupper

Kurven D definert ovenfor ved $ax^3 + by^3 + cz^3$ har Jacobivarietet E gitt ved $X^3 + Y^3 = AZ^3$ der $A = abc$. D har ikke nødvendigvis et k-rasjonalt punkt, men det har E. E er da en elliptisk kurve.

Tar vi utgangspunkt i en gitt elliptisk kurve E kan vi studere ikke-singulære kurver D av genus 1 som har E som Jacobivarietet. Slike har følgende struktur:
(1.) $\mu : D \times E \longrightarrow D$ over k slik at $\mu(y, e) = y$ og $\mu(\mu(y, x_1), x_2) = \mu(y, x_1 + x_2)$ og
(2.) $\nu : D \times D \longrightarrow E$ over k slik at $\mu(y_1, x) = y_2 \iff \nu(y_2, y_1) = x$.

D kalles for et *prinsipalt homogent rom* over (E, e). Vi kan innføre en ekvivalensrelasjon på disse. Weil (1955) definerte en gruppestruktur på disse ekvivalensklassene og vi får $WC(E, k)$, *Weil-Châtelet gruppa*. Det er viktig å legge merke til at en ekvivalensklasse i $WC(E, k)$ er $0 \iff$ kurvene D som representerer klassen har et k-rasjonalt punkt.

Merk at dette var etter at Selmer hadde gjort sitt arbeid.

Dersom K/k er en kroppsutvidelse, så har vi en homomorfi
$WC(E, k) \longrightarrow WC(E, K)$. Spesielt for k en algebraisk tallkropp og k_v en kompletering mht. en tallverdi v, har vi $WC(E, k) \longrightarrow WC(E, k_v)$.

Definisjon 4.1. La (E, e) være en elliptisk kurve over en algebraisk tallkropp k. $Ш = Ш(E) = \cap_v \, ker(WC(E, k) \longrightarrow WC(E, k_v))$ kalles for *Tate-Šafarevič gruppa til* E.

Selmers kurve $3X^3 + 4Y^3 + 5Z^3$ er (dvs. representerer) et ikke-trivielt element i $Ш(E)$ der E er den elliptiske kurven gitt ved $X^3 + Y^3 = 60Z^3$.

Bemerkning 4.2. Vi bruker følgende notasjon: Gitt en abelsk gruppe G og et heltall $n > 1$, la $G[n] = \{x \in G | nx = 0\}$, n-torsjonsdelen til G.

$Ш(E)[n]$ er endelig for alle $n > 1$.

Formodning 4.3. $Ш(E)$ er endelig for alle elliptiske kurver E over en algebraisk tallkropp k.

I 1987 fant Karl Rubin de første eksemplene av elliptiske kurver E der man kunne bevise at $Ш(E)$ var endelig.

Vi har nå to grupper som er vanskelige å beregne: $E(k)$ og $Ш(E)$, alternativt: $E(k)/nE(k)$ og $Ш(E)[n]$. Det vil være kjekt å ha en gruppe som gir en viss kontroll over disse to og som samtidig er litt medgjørelig beregningsmessig.

5 Selmergrupper

For alle $n > 1$, så skulle vi ønske at det eksisterte en endelig abelsk gruppe S_n slik at

$$0 \longrightarrow E(k)/nE(k) \longrightarrow S_n \longrightarrow Ш(E)[n] \longrightarrow 0$$

er eksakt med S_n er effektivt beregnbar.

For å definere Selmergrupper er det mest hensiktsmessig å bruke Galoiskohomologi.

Notasjon. La $E = E(\bar{k})$, $E_v = E(\bar{k_v})$, $G = Gal(\bar{k}/k)$, $G_v = Gal(\bar{k_v}/k_v)$, $H^i(-) = H^i(G,-)$, og $H^i_v(-) = H^i(G_v,-)$.

Vi har $H^0(E) = E(k)$ og $H^1(E) = WC(E,k)$.
Vi har en kort eksakt sekvens

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{n} E \longrightarrow 0$$

Vi får

$$0 \longrightarrow H^0(E[n]) \longrightarrow H^0(E) \xrightarrow{n} H^0(E) \longrightarrow$$
$$H^1(E[n]) \longrightarrow H^1(E) \xrightarrow{n} H^1(E)$$

og dermed

$$0 \longrightarrow E(k)/nE(k) \longrightarrow H^1(E[n]) \xrightarrow{n} H^1(E)[n] \longrightarrow 0$$

eller

$$0 \longrightarrow E(k)/nE(k) \longrightarrow H^1(E[n]) \xrightarrow{n} WC(E,k)[n] \longrightarrow 0$$

Vi har tilsvarende sekvenser for kroppene k_v. Vi kan da lage

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(k)/nE(k) & \longrightarrow & H^1(E[n]) & \xrightarrow{n} & WC(E,k)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(k_v)/nE(k_v) & \longrightarrow & \prod_v H^1_v(E_v[n]) & \xrightarrow{n} & \prod_v WC(E,k_v)[n] & \longrightarrow & 0 \end{array}$$

Definisjon 5.1. *Selmergruppa* er $S_n = \{c \in H^1(E[n]) |$ c er med i bildet av $\prod_v E(k_v)/nE(k_v)$ i $\prod_v H^1_v(E_v[n])\}$.

Ved å gjennomløpe diagrammet får vi nå den eksakte sekvensen

$$0 \longrightarrow E(k)/nE(k) \longrightarrow S_n \longrightarrow Ш(E)[n] \longrightarrow 0$$

Sitat. "We shall call it a Selmer group because Selmer initiated the present work."

J. W. S. Cassels på s. 262 i: Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups. *Proc. London Math. Soc. (3)* **12** (1962), s. 259-296.

S_n er effektivt beregnbar.

Sitat. "Effectively computable" is not the same as "easy".

Karl Rubin, sagt om Selmergrupper i foredraget "Rational points on abelian varieties" på MSRI den 17. januar 2006.

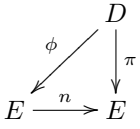
Definisjonen av S_n som en undergruppe i $H^1(G, E[n])$ er ganske abstrakt. Hvordan kan vi tolke S_n mer konkret? Hvordan kan vi regne med elementene i S_n?

6 Descent

Prossessen med å beregne Selmergruppa S_n og å bruke den til å begrense $E(k)/nE(k)$ kalles for *n-descent* eller *å utføre en n-descent*. Det var nettop dette Selmer gjorde i artiklene sine. Arbeidet med n-descenter vokser raskt med n. $n = 2$ er desidert det mest vanlige, men $n = 3$ og $n = 4$ forekommer også.

Bemerkning 6.1. Et helt spesielt tilfelle av det han gjorde går tilbake til Fermat. Fermat innførte "uendelig descent" som en bevismetode i tallteori rundt år 1640. Det går ut på å ta en gitt (eller tenkt) positiv løsning til en ligning og utlede en ny positiv løsning med mindre tallverdi.

Elementene i S_n kan tolkes på forskjellig vis. Blant tolkningene finner vi:
1.) *n-overdekninger*. Vi tar en ikke-singulær kurve D av genus 1 samt en rasjonal avbildning $\pi : D \longrightarrow E$ over k og en isomorfi $\phi : D \longrightarrow E$ over $\bar{k}$ slik at følgende diagram kommuterer:



Isomorfien ϕ innebærer at D er et prinsipalt homogent rom over E. Dette er den klassiske tolkning og tilsvarer Selmers arbeid.
2.) *avbildninger til* $\mathbb{P}^{n-1}$.
3.) *theta grupper*
4.) *via etale algebraer*

Det foregår for tiden svært mye arbeid med å utvikle disse forskjellige tolkningene.

7 Anvendelser av S_n

Vi så at S_n var strategisk plassert midt i sekvensen

$$0 \longrightarrow E(k)/nE(k) \longrightarrow S_n \longrightarrow Ш(E)[n] \longrightarrow 0$$

Selmer brukte S_n til å beregne $E(k)$. Men den er også viktig når man ser på $Ш(E)$.

Poenget er å finne hvilke elementer i S_n som kommer fra $E(k)/nE(k)$ og hvilke som går til ikke-trivielle elementer i Ш(E). Hva gjør vi dersom vi ikke klarer å avgjøre dette for nok elementer i S_n? I så fall, kan vi fortsette med S_{mn} (vanligvis S_{n^2}). Selmer brukte S_4 i tillegg til S_2 av og til. Slikt kalles for *den andre descent*. Alternativt kan man bytte n.

8 Selmergrupper og Fermats siste teorem

Den grunnleggende filosofien som ligger bak Selmergruppa kan anvendes i mye mer generaliserte former. Wiles artikkel med beviset for Fermats siste teorem har fem kapitler. Den tredje heter "Estimates for the Selmer group". Det var nettopp Selmergruppa som skapte mest bry for Wiles.

Sitat. "... the final calculation of a precise upper bound for the Selmer group ... is not yet complete as it stands."

Andrew Wiles, 4/12/1993