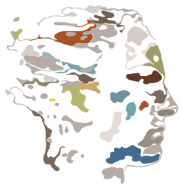


Fra kvadratisk resiprositet til Langlands' program

Å løse likninger har gjennom alle tider vært en viktig matematisk utfordring. Tidlige kilder, som Rhind-papyrusen, skrevet av Ahmes allerede rundt 1650 år før vår tidsregning, inneholder metoder for å løse lineære likninger. Rasjonale tall og komplekse tall oppsto som nødvendigheter for å løse ulike likninger. Og fortsatt er likninger og deres løsninger i ulike tallsystemer en viktig kilde til å utvikle ny kunnskap, såvel i matematikk som i andre vitenskapelige disipliner.

Matematikere har en spesiell interesse av å finne heltallige løsninger av likninger. Årsaken er at denne type løsninger er nært knyttet til de mange forsøkene opp gjennom historien på stadig å trenge dypere ned i mystikken rundt de naturlige tallene, $\mathbb{N} = \{1, 2, 3, \dots\}$. Den additive strukturen til de naturlige tallene er lett tilgjengelig siden et hvert naturlig tall kan skrives som en sum av 1-ere. Derimot er den multiplikative strukturen mye mer subtil. Primtallene, 2, 3, 5, 7, ..., oppfattet som de multiplikative byggestenene for alle positive heltall, skjuler fortsatt en mengde hemmeligheter, f.eks. er det svært vanskelig på en effektiv måte å avgjøre om et vilkårlig valgt tall er et primtall eller ikke.

En slags første grov tilnærming til spørsmålet om hvor vidt en polynomial likning $P(x_1, \dots, x_n) = 0$ har en heltallsløsning, er å redusere problemet modulo m, dvs. lete etter løsninger av likningen i ringen $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ for varierende positive heltall m. Ved å bruke **det kinesiske restteoremet** kan man vise at dette er ekvivalent med å finne løsninger modulo potenser p^k hvor p er et primtall og $k \geq 1$.

Å løse **kongruensen** (likninger kalles ofte kongruenser når de relateres til moduloregning)

$$P(x_1, \dots, x_n) \equiv 0 \pmod{p^k}$$

kalles et "lokalt" problem siden vi fokuserer på ett primtall eller "en plass" $p \in \mathbb{Z}$ av gangen. Motsatsen, det å løse likningen over de hele tallene $\mathbb{Z}$, kaller vi på samme måte et "globalt" problem.

Kurt Hensel (1861-1941) reformulerte det lokale problemet i 1897 ved å introdusere de **p-adiske heltallene**;

$$\hat{\mathbb{Z}}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$$

en konstruksjon som omfatter alle potenser p^k, for $k \geq 1$, på en gang. Hensels reformulering sier at å finne løsninger av kongruensen modulo et vilkårlig heltall m, er ekvivalent med å finne løsninger i de p-adiske heltallene for hvert primtall p. I tillegg til å finne løsninger for hvert primtall p er det selvfølgelig nødvendig at likningen har reelle løsninger for at vi i det hele tatt skal ha noen mulighet til å finne heltallige løsninger.

De p-adiske tallene er definert som en invers grense og de kommer derfor utstyrt med den tilhørende "kompletterings-topologien". Topologien defineres ved hjelp av den **p-adiske metrikken**:

Definisjon 1. *For et rasjonalt tall*

$$q = \frac{p^\alpha m}{n}$$

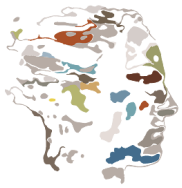
hvor n og m ikke er delelige med p, er den p-adiske metrikken til q gitt ved

$$|q|_p = p^{-\alpha}$$

Det følger at to naturlige tall er p-nære (dvs. med hensyn på den p-adiske metrikken) hvis deres differanse er delelig med en høy potens av p. På denne måten vil ikke 14 og 15 være spesielt 2-nærme hverandre siden differansen ikke er delelig med noen positiv potens av 2. Tallene 31 og 63 er derimot mye 2-nærmere hverandre siden differansen $63 - 31 = 32 = 2^5$ og avstanden blir da 2^{-5}.

Vi kan lokalisere $\hat{\mathbb{Z}}_p$ i den multiplikative mengden av ikke-trivielle elementer og danne de **p-adiske tallene** $\hat{\mathbb{Q}}_p$. Siden de reelle tallene $\mathbb{R}$ er kompletteringen av $\mathbb{Q}$ med hensyn på den vanlige normen, velger vi å skrive disse på samme form som de p-adiske kompletteringene, rett og slett ved å bruke notasjonen $|q|_\infty$ for denne normen. Vi sier da at de reelle tallene $\mathbb{R}$ er kompletteringen av $\mathbb{Q}$ i det "uendelige primtallet $p = \infty$", dvs $\mathbb{R} = \hat{\mathbb{Q}}_\infty$.

Hver $\hat{\mathbb{Q}}_p$ for $p \leq \infty$ kalles en "lokal kropp", mens $\mathbb{Q}$ selv er en "global kropp". Hasse-Minkowski-teoremet gir et positivt svar på det **lokalt-globalt-prinsippet**: *En påstand er gyldig over den globale kroppen $\mathbb{Q}$ hvis og bare hvis den er gyldig over alle lokale kropper $\hat{\mathbb{Q}}_p$ for $p \leq \infty$.*



Teorem 2 (Hasse-Minkowski)**.** *La Q være en ikke-degenerert kvadratisk form. Da vil*

$$Q(x_1, \ldots, x_n) = 0$$

ha en ikke-triviell heltallsløsning hvis og bare hvis likningen har en reell løsning og en p-adisk løsning for et hvert primtall p.

Vi merker oss at Hasse-Minkowski-teoremet sier noe om løsninger av kvadratiske likninger. Resultatet er ikke sant for polynomiale likninger av høyere grad. Det var kjent så tidlig som i 1909 at Fermat-likningen $x^n + y^n = z^n$ har p-adiske løsninger for alle primtall p. Men som vi nå vet har den ingen heltallige løsninger.

Et annet eksempel på en likning som kan løses lokalt, men ikke globalt, ble funnet av **Ernst Selmer** (1920-2006) i 1951. Likningen er gitt ved

$$3x^3 + 4y^3 + 5z^3 = 0$$

og Selmer viste at denne likningen kan løses modulo p for et hvert primtall p, og selvfølgelig over $\mathbb{R}$, men den har ingen løsninger over $\mathbb{Q}$ (og derfor heller ikke over $\mathbb{Z}$).

En relativt uskyldig utseende likning som gjennom historien har vært gjenstand for omfattende studier, er den kvadratiske likningen

$$x^2 = d$$

hvor d er et positivt heltall. Likningen tillater en heltallsløsning hvis og bare hvis d er et kvadrattall.

Anta at d ikke er et kvadrattall. Hasse-Minkowski-teoremet sier da at det må finnes et primtall p slik at kongruensen

$$x^2 \equiv d \pmod{p^k}$$

ikke har noen løsning, dvs. at det finnes en primtallspotens p^k slik at tallet d ikke er en **kvadratisk rest**. **Adrien-Marie Legendre** (1752-1833) reformulerte denne påstanden i mer symbolsk notasjon;

Definisjon 3. *La p være et odde primtall og d et heltall.* ***Legendre-symbolet*** $\left(\frac{d}{p}\right)$ *er definert ved*

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{hvis } x^2 \equiv d \text{ (mod } p\text{) er løsbar} \\ -1 & \text{hvis } x^2 \equiv d \text{ (mod } p\text{) } \textbf{ikke} \text{ er løsbar} \\ 0 & \text{hvis } p \text{ deler } d \end{cases}$$

Legendre-symbolet er multiplikativt og p-periodisk i topp-argumentet, og man kan vise at symbolet tilfredsstiller **den kvadratiske resiprositets-satsen**:

Teorem 4. *La p og q være to odde primtall. Da har vi at*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Den spesielle verdien for primtallet $p = 2$ er gitt ved

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Legendre-symbolet kan beregnes ved hjelp av Eulers formel, introdusert av **Leonhard Euler** (1707-1783) i 1748:

Teorem 5. *La p være et odde primtall og d et heltall. Da har vi*

$$\left(\frac{d}{p}\right) \equiv d^{\frac{p-1}{2}} \pmod{p}$$

En umiddelbar og svært nyttig konsekvens av Eulers formel er det faktumet at

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Eulers kriterium kan lett vises ved hjelp av Fermats lille teorem,

$$d^{p-1} \equiv 1 \pmod{p}$$

Denne kongruensen kan vi skrive om som

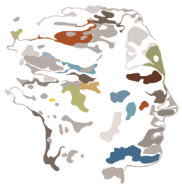
$$(d^{\frac{p-1}{2}} - 1)(d^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

og det følger av at p er primtall at minst en av de to faktorene er kongruent med 0 (mod p). Dersom d er en kvadratisk rest, dvs. at det finnes en x slik at $x^2 \equiv d \pmod{p}$, så vil

$$d^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$$

Dette gir at den første faktoren er lik med 0. Siden polynomet $x^2 - d$ har grad 2 kan det maksimalt ha to røtter, x og $-x$. Mao. finnes det minst $\frac{p-1}{2}$ ikke-trivielle kvadratiske rester. På den annen side er polynomet

$$x^{\frac{p-1}{2}} - 1$$



av grad $\frac{p-1}{2}$ og kan derfor ha maksimalt $\frac{p-1}{2}$ ikke-trivielle røtter. Det følger at de gjenstående $\frac{p-1}{2}$ ikke-kvadratiske restene må være røtter i den andre faktoren, dvs. at de tilfredsstiller

$$d^{\frac{p-1}{2}} \equiv -1 \,(\text{mod } p)$$

Det betyr at vi har $d^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, avhengig av om d er en kvadratisk rest eller ikke.

Et generelt rammeverk for å beskrive løsninger av likninger ble introdusert av **Évariste Galois** (1811-1832) i 1832, kun få dager før han døde av skader han pådro seg i en duell, bare 20 år gammel. Anta at vi har gitt en polynomial likning med heltallige koeffisienter. Da kan vi utvide de rasjonale tallene med løsningene til likningen (som vi finner blant de komplekse tallene) og danne en **kroppsutvidelse** E av de rasjonale tallene $\mathbb{Q}$. Galois sin ide var å se på automorfier av den utvidede kroppen, som fikserer de rasjonale tallene, og dermed også fikserer den opprinnelige likningen. Mengden av slike automorfier danner en **gruppe**, den såkalte **Galois-gruppa** $G(E/\mathbb{Q})$ til kroppsutvidelsen. Galois-gruppa har en rik struktur som reflekterer mange av egenskapene til den opprinnelige likningen. F.eks. er Galois-gruppa triviell hvis og bare hvis polynomet splitter fullstendig i lineære faktorer med heltallige koeffisienter.

Likningen $x^2 - d = 0$ har maksimalt to røtter, og de eneste mulige automorfiene av $E = \mathbb{Q}(\sqrt{d})$ som fikserer $\mathbb{Q}$ er konjugasjonsavbildningen $\sigma : \sqrt{d} \mapsto -\sqrt{d}$ og identitetsavbildningen. Galois-gruppa i dette tilfellet er derfor den entydige gruppa på to elementer $\mathbb{Z}_2 = \{Id, \sigma\}$ hvor $\sigma^2 = Id$.

Gruppa $\mathbb{Z}_2$ opptrer også i en aritmetisk kontekst, nemlig som den multiplikative gruppa $(\mathbb{Z}_4)^* = \{1, 3\}$ av enheter i $\mathbb{Z}_4$. I denne gruppa virker 1 som enhetselementet, og 3 oppfyller $3^2 \equiv 1 \pmod{4}$. Vi definerer en avbildning

$$\phi : (\mathbb{Z}_4)^* \to G(E/\mathbb{Q})$$

ved $(p \,(\text{mod } 4)) \mapsto \left(\frac{d}{p}\right)$. Ved Eulers kriterium er denne avbildningen er veldefinert for alle odde primtall, og den er også en gruppe-homomorfi.

Avbildningen ϕ kalles **Artin-avbildningen**, og bildet av et primtall $\phi_p := \phi(p)$ kalles **Frobeniuselementet** (til p) i Galoisgruppa $G(E/\mathbb{Q})$. Frobenius-elementet svarer til den såkalte Frobenius-avbildningen i en endelig kropp. La E_p være en utvidelse av den entydig gitte kroppen av p elementer. Frobenius-avbildningen avbilder E_p på seg selv. Den er definert ved $x \mapsto x^p$. Siden E_p er en utvidelse av $\mathbb{F}_p$, så vil Frobenius-avbildningen være en ring-homomorfi. Det følger av at $p = 0$ i $\mathbb{F}_p$. For en såkalt **uramifisert** kroppsutvidelse kan Frobenius-avbildningen, på en entydig måte, løftes fra $G(E_p/\mathbb{F}_p)$ to $G(E/\mathbb{Q})$. Resultatet av denne løftingen er Frobenius-elementet.

Over kroppen $\mathbb{F}_p$ gir Fermats lille teorem at Frobenius-avbildningen er lik identitetsavbildningen. I det kvadratiske eksemplet, som vi har sett på over, kan vi beregne $x \mapsto x^p$ for et vilkårlig element $v + w\sqrt{d} \in \mathbb{F}_p[\sqrt{d}]$. Vi har

$$\begin{aligned}(v + w\sqrt{d})^p &= v^p + w^p(\sqrt{d})^p \\ &= v + wd^{\frac{p-1}{2}}\sqrt{d}\end{aligned}$$

Det betyr at verdien av $d^{\frac{p-1}{2}} \pmod{p}$ bestemmer hvilken automorfi vi har med å gjøre. Igjen bruker vi Fermats lille teorem og får

$$0 = d^p - d = d \cdot (d^{\frac{p-1}{2}} - 1)(d^{\frac{p-1}{2}} + 1)$$

Siden $\mathbb{F}_p$ er en kropp, må en av de tre faktorene være 0. Vi kan anta at p ikke deler d, noe som ekskluderer den første faktoren. For

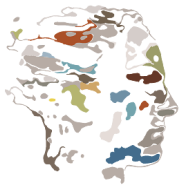
$$d^{\frac{p-1}{2}} = 1,$$

vil Frobenius-avbildningen være identieten, mens for

$$d^{\frac{p-1}{2}} = -1,$$

vil Frobenius-avbildningen svare til konjugasjons-automorfien $\sigma : \sqrt{d} \mapsto -\sqrt{d}$. Samtidig har vi at det første tilfellet svarer til at d er en kvadratisk rest, det andre til at d ikke er det. Merk også at dersom d er en kvadratisk rest, så vil polynomet $x^2 - d$ splitte fullstendig i lineære faktorer.

Selv om Artin-avbildningen i dette eksemplet virker svært uskyldig, så uttrykker den en dyp sammenheng mellom to objekter av ulikt opphav. Galois-gruppa til likningen på den ene siden, og aritmetikken i $\mathbb{F}_p$ på den andre siden.



I 1923 formulerte den østerrikske matematikeren **Emil Artin** (1898-1962) det som i dag kalles *Artins resiprositets-sats*. Resultatet ble først formulert som en formodning, men Artin klarte selv å bevise resultatet noen år senere. Artins resiprositets-sats kan gjerne betraktes som en generalisering av den kvadratiske resiprositets-satsen.

Artins resiprositets-sats omhandler en større klasse av kroppsutvidelser E av $\mathbb{Q}$, men fortsatt er vi avhengig av at Galois-gruppa $G(E/\mathbb{Q})$ er abelsk. Den tilsvarende generaliseringen av venstresiden i Artin-avbildningen er **adele-ringen**, introdusert av **Claude Chevalley** (1909-1984) tidlig på 1950-tallet. Adele-ringen er det såkalte **restrikterte produktet** av alle kompletteringer $\hat{\mathbb{Q}}_p$, $p \leq \infty$, av de rasjonale tallene. Vi kan betrakte adele-ringen som samlingen av alle de lokale egenskaper til den globale kroppen $\mathbb{Q}$.

Artins resiprositets-sats gir en presis korrespondanse mellom en abelsk kroppsutvidelse, dvs. en kroppsutvidelse med tilhørende abelsk Galois-gruppe, og adele-ringen. Vi kan tenke på denne korrespondansen som et slags lokalt-globalt prinsipp, hvor Galois-teorien representerer den globale innfallsvinkelen, og adele-ringen den lokale. I eksemplet over er Galois-gruppen syklisk av orden 2 og $(\mathbb{Z}_4)^*$ er den tilsvarende kvotienten av **idele-klasse-gruppa**, som igjen svarer til enhetene i adele-ringen.

Artins resiprositets-sats ble generalisert videre av Robert P. Langlands. Grunnlaget for hans generalisering ble klarlagt i brevet til **André Weil** i 1967. Med bakgrunn i Artins behandlig av det abelske tilfellet var det naturlig å spørre seg om det var mulig å generalisere Artin-avbildningen til ikke-abelske Galois-grupper. Spørsmålet er svært relevant siden allerede rot-kroppen til polynomet $x^3 - 2$ har ikke-abelsk Galois-gruppe over $\mathbb{Q}$. Svaret på spørsmålet var å introdusere en form for ikke-kommutativitet også på "adele-siden" av korrespondansen.

Som en forberedelse til en slik utvidelse til en ikke-abelsk setting endrer vi vår oppfattelse av Artins resiprositets-sats som noe som befinner seg i den kommutative verdenen. Stikkordet er representasjonsteori for grupper og en nøkkel-observasjon er at en abelsk gruppe er fullstendig beskrevet av sine 1-dimensjonale representasjoner. Istedenfor å studere gruppa i seg selv, betrakter vi mengden av 1-dimensjonale representasjoner $\rho : G \to \mathbb{C}^* = GL_1(\mathbb{C})$, uten å miste noe informasjon. På den andre siden erstatter vi adele-ringen med en passende kvotient av $GL_1(\mathbb{A})$, den multiplikative gruppa av enheter i $\mathbb{A}$.

Langlands' forslag gikk ut på å finne en tilsvarende beskrivelse for høyere-dimensjonale representasjoner $\rho : G \to GL_n(\mathbb{C})$ av de ikke-abelske Galois-gruppene. Slike representasjoner skulle svare til representasjoner av $GL_n(\mathbb{A})$ på en passende kvotient av seg selv; såkalte **automorfe former**. Denne korrespondansen er nå kjent under navnet **Langlands-korrespondansen**.