.I Minkowskis gitterpunktssats

Minkowskis sats klarar av en mängd problem inom den algebraiska talteorin och teorin för diofantiska ekvationer. Den kan ses som en "kontinuerlig", eller geometrisk, variant, av Dirichlets lådprincip.

Vi visar satsen endast i två dimensioner. Har man förstått idén i detta fall är det inte svårt att generalisera till högre dimension.

Vi visar den först för ett ON-gitter. Det är ingen allvarlig inskränkning; det allmänna fallet återföres lätt på detta genom en lineär avbildning. Det väsentliga är då att lineära avbildningar förändrar alla arear i samma skala.

Vi börjar med att möblera scenen. Vi är i planet. Koordinater hänför sig till ett ON-system. Punkter med heltalskoordinater kallar vi *gitterpunkter*.

Utöver detta gitter betraktar vi också det grövre gittret bestående av punkter med jämna koordinater. Utgående från detta definierar vi en disjunkt övertäckning av planet, bestående av "halvöppna" kvadrater. Närmast origo har vi *fundamentalområdet*, kvadraten med hörn i punkterna $(0,0),(0,2),(2,0),(2,2)$. I denna kvadrat räknar vi in den undre och den vänstra kanten, däremot inte de båda övriga. Genom att förskjuta fundamentalområdet i riktningarna $(2m,2n)$, där m,n är heltal, skapar vi nya kvadrater, som tillsammans täcker hela planet, och inte har gemensamma punkter.

Nu betraktar vi ett område Ω med lite speciella egenskaper. Det ska vara begränsat och ha en bestämd area. I de flesta tillämpningar är området en parallellogram, en cirkel eller en ellips (en lineär bild av en cirkel) vilkas areor är välkända och inte alltför svåra att motivera.

Det ska vidare vara *konvext*. Det betyder att för vilka två punkter som helst ska även den förbindande sträckan ligga helt i området. Intuitionen är att områdets rand inte ska "bukta inåt" någonstans. De redan nämnda områdena är konvexa, en triangel är konvex, en stjärna är det inte.

Speciellt kommer vi att utnyttja att om två punkter (x_1,y_1), och (x_2,y_2) tillhör Ω så gör punkten mitt emellan dem,

$$(\frac{x_1+x_2}{2},\frac{y_1+y_2}{2}),$$

det också.

Vi kräver, beträffande form och läge, även att området är centralsymmetriskt kring origo. Dvs. för varje punkt $(x_0,y_0)\in\Omega$ så gäller att även dess spegelbild i origo, $(-x_0,-y_0)$, tillhör Ω.

Detta gäller t ex om cirklar eller ellipser med medelpunkt i origo. Det gäller också för parallellogrammer med medelpunkten (diagonalernas skärningspunkt) i origo. En sådan parallellogram beskrivs av olikheterna $-m < ax+by < m; \quad -n < cx+dy < n$. Eller ostränga olikheter om även konturen ska ingå. (Här måste vi ha $ad-bc\neq 0$).

En triangel kan, hur den än ligger, aldrig vara centralsymmetrisk kring origo.

Nu kan vi formulera satsen.

.I.1 Sats. *Anta att arean av Ω är större än 4 areaenheter. Då gäller att Ω innehåller minst en gitterpunkt utöver* $(0,0)$

Bevis: Vi relaterar Ω till det "grova" gittret, det med jämna koordinater. Till detta hörde en övertäckning av planet med kvadrater av area 4. Ω träffar ändligt många av dessa. Detta ger oss en uppdelning av Ω i ett antal disjunkta delområden. Vi translaterar alla dessa delområden så att de hamnar i fundamentalområdet, kvadraten med hörn i $(0,0),(2,0),(0,2),(2,2)$.

Translationsvektorerna har genomgående jämna koordinater.

T ex om en bit av Ω träffar kvadraten med hörn i $(-2,-4),(-2,-2),(0,-4),(0,-2)$ så ska denna bit translateras utmed vektorn $(2,4)$, dvs. denna vektor ska adderas till delområdets ortsvektorer.

Eftersom delarnas totala area är större än 4, dvs. större än fundamentalomårdets area, så kommer åtminstone två av de translaterade delområden att träffa varandra. Det betyder att två olika punkter i Ω, (x_1,y_1) och (x_2,y_2) translaterats till samma punkt i fundamentalområdet. Deras koordinater skiljer sig alltså med jämna heltal,

$$(x_1,y_1)-(x_2,y_2)=(2m,2n)$$

där m,n ej båda är lika med noll.

Nu är även $(-x_2,-y_2)$ en punkt i Ω (centralsymmetri). Av konvexiteten följer, som ovan påpekats, också att punkten mitt emellan

$$(x_1,y_1) \text{ och } (-x_2,-y_2)$$

alltså,

$$(\frac{x_1-x_2}{2},\frac{y_1-y_2}{2})=(m,n),$$

tillhör Ω.

Och därmed har vi hittat den påstådda gitterpunkten. ∎

Detta är den version vi behöver för att fastställa existensen av lösningar till Pells ekvation. Nu diskuterar vi generaliseringen, fortfarande i planet.

Vi arbetade med ett gitter bestående av heltalspunkter, dvs. alla heltaliga lineärkombinationer av ortsvektorerna $(1,0),\quad(0,1)$. Den parallellogram som spänns upp av dessa två, gittrets fundamentalområde, är en kvadrat med area 1.

Vi tänker oss allmännare två lineärt oberoende vektorer $\mathbf{v}_1=(a_1,b_1),\quad \mathbf{v}_2=(a_2,b_2)$ och gittret bestående av deras heltaliga lineärkombinationer. Fundamentalområdets area betecknar vi med V. Från den elementära lineära algebran vet du att $V=|a_1b_2-a_2b_1|$, beloppet av en determinant.

Ω är som förut, konvext och centralsymmetriskt, med area $\mu(\Omega)$. Då gäller, med nästan ingen förändring av beviset:

.I.2 Sats. *Anta att $\mu(\Omega) > 4V$ Då innehåller Ω en gitterpunkt $m_1\mathbf{v}_1 + m_2\mathbf{v}_2$ där m_1, m_2 är heltal, ej båda lika med noll.* ∎

Man kan generalisera till högre dimension, också. Säg att dimensionen är d. Vi betraktar alla heltaliga lineärkombinationer av d stycken lineär oberoende vektorer. Man kan definiera fundamentalvolymen V som en d/d–determinant. Området Ω ska fortfarande vara konvext och centralsymmetriskt; definitionerna är omedelbara.

Så förutsätter vi att vi kan definiera en volym $\mu(\Omega)$ som unikt skiljande tal mellan "inre" och "yttre" summor; summor av volymer av hyperkuber som ligger helt i området, resp. helt och hållet täcker detsamma. Då gäller Minkowskis gitterpunktsats under förutsättningen $\mu(\Omega) > 2^d \cdot V$.

.I.3 Exempel: Vi visar Fermats sats, att varje primtal $p \equiv 1 \pmod 4$ kan skrivas $p = x^2 + y^2$ där x, y är heltal.

Medels teorin för primitiva rötter visas lätt (text och/eller föreläsning) att -1 är kvadratisk rest modulo p, dvs. det finns heltal a, n sådana att

$$a^2 + 1 = np$$

Vi betraktar nu det gitter som bestäms av linjerna $y = ax + rp; \quad x = s$ där r, s är heltal. Själva gittret består av linjernas skärningspunkter.

Fundamentalområdet får vi genom att betrakta de fyra linjerna $y = ax + 0, ax + p \quad x = 0, 1$ vilket ger oss hörnen $(0,0), (1,a), (0,p), (1, a+p)$ (rita!). Här ser vi direkt att vi har en parallellogram med bas p utmed y–axeln, och höjden 1. Så fundamentalområdets area $V = p$.

Nu betraktar vi cirkeln $x^2 + y^2 = R^2$ där R^2 är lite mindre än $2p$. Dess area är alltså πR^2, som vi kan förutsätta större än $6p > 4p = 4V$.

Minkowskis sats ger oss nu en gitterpunkt $(s, as + rp)$ med $s^2 + (as + rp)^2 < 2p$. Vi har $s^2 + (as + rp)^2 \equiv s^2(1 + a^2) = ns^2p$ en nollskild positiv multipel av p. På grund av den just fastställda olikheten måste denna multipel vara lika med p själv. ∎

Jämför gärna detta bevis med det som erhålles medels Thues lemma, ex. 14, p.504, i Rosens bok.

.I.4 Exempel: Vi studerar här Pells ekvation $x^2 - Dy^2 = 1$ där D är positivt och inte någon jämn kvadrat.

Den *triviala lösningen* är $x = \pm 1, y = 0$. Vi ska visa att det finns andra lösningar.

Ett viktigt steg är att visa att det finns ett k sådant att ekvationen $x^2 - Dy^2 = k$ har oändligt många lösningar.

Betrakta först området

$$|x - \sqrt{D}y| \leq 1; \quad |x + \sqrt{D}y| \leq 1$$

Rita figur!

Det är en parallellogram, rentav en romb. Dess hörn får vi genom att skära linjerna $x - \sqrt{D} = \pm 1, \quad x + \sqrt{D} = \pm 1$ parvis. Vi erhåller $(\pm 1, 0)$, $(0, \pm 1/\sqrt{D})$. Romben kan naturligt delas i två trianglar och vi kan lätt avläsa basen 2 i bägge, och höjden $1/\sqrt{D}$. Så arean är $2/\sqrt{D}$.

Nu betraktar vi området

$$|x - \sqrt{D}y| \le a; \quad |x + \sqrt{D}y| \le b; \quad a, b > 0$$

Detta uppstår ur det gamla området genom skalning faktorn a på en ledd, faktorn b på en annan. Så dess area är $2ab/\sqrt{D}$. Det är konvext och centralsymmetriskt kring origo.

Väljer vi nu ab lika med konstanten $2\sqrt{D} + 1$ så är arean >4. Området innehåller alltså en gitterpunt skild från origo. Genom att låt a gå mot oändligheten och b mot noll, så att produkten förblir konstant kan vi hitta oändligt många gitterpunkter (x, y) sådana att

$$|x - \sqrt{D}y| \le a; \quad |x + \sqrt{D}y| \le b; \quad a, b > 0; \qquad |x^2 - Dy^2| \le ab = 2\sqrt{D} + 1$$

Begränsningen innebär att oändligt många punkter ger upphov till ändligt många värden på $x^2 - dy^2$ Då måste det gälla att något värde k antages oändligt många gånger.

Vi kan därför hitta ett k och två punkter $(x_1, y_1), \quad (x_2, y_2)$ sådana att

$$x_i^2 - Dy_i^2 = k$$

och samtidigt

$$x_1 \equiv x_2 \pmod{k}; \quad y_1 \equiv y_2 \pmod{k}; \qquad |x_1| \ne |x_2|, |y_1| \ne |y_2|$$

Nu bildar vi

$$x_0 + y_0\sqrt{D} = \frac{x_1 + y_1\sqrt{D}}{x_2 + y_2\sqrt{D}}$$

där x_0, y_0 är rationella.

För dess konjugat gäller

$$x_0 - y_0\sqrt{D} = \frac{x_1 - y_1\sqrt{D}}{x_2 - y_2\sqrt{D}}$$

Och för produkten har vi

$$x_0^2 - Dy_0^2 = \frac{x_1^2 - Dy_1^2}{x_2 - Dy_2^2} = \frac{k}{k} = 1$$

Allt är klart om vi kan visa att x_0, y_0 är heltal, $(x_0, y_0) \neq (\pm 1, 0)$.

Konjugatförlängning ger

$$x_0 + y_0\sqrt{D} = \frac{x_1 + y_1\sqrt{D}}{x_2 + y_2\sqrt{D}} = \frac{(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D})}{(x_2 + y_2\sqrt{D})(x_2 - y_2\sqrt{D})}$$

P g a av de förutsatta kongruenserna visar vi lätt att koefficienterna i täljaren, $x_1x_2 - Dy_1y_2$ och $-x_1y_2 + x_2y_1$, är delbara med k.

Vidare är nämnaren lika med k, så x_0, y_0 är heltal. Vi kan inte ha $x_0 = \pm 1, y_0 = 0$, ty då vore $x_1 + y_1\sqrt{D} = \pm x_2 + y_2\sqrt{D}, \quad x_1 \pm x_2, \quad y_1 = \pm y_2$ vilket vi uteslutit.