Vad är avstånd?

Laura Fainsilber
forskarassistent i matematik
Chalmers och GU
laura@math.chalmers.se
Forskningsområde : algebraisk talteori.

Sammanfattning

Jag bor i Göteborg och känner mig nära Anne, som bor i Frankrike. Vad menar jag med ordet "nära"? I matematik använder man oftast det "reella" avståndet $|x - y|$ men det finns även andra, så kallade "p-adiska", som bygger på hur stora gemensamma delare två tal har. Jag förklarar definitionen för sådana avstånd och visa vad som händer geometriskt när man räknar "p-adiskt". Bland annat är alla trianglar likbenta och varje punkt innanför en cirkel ligger i mitten av cirkeln. P-adiska tal används i forskning i talteori, geometri, analys och även i vissa modeller i fysik. Att fundera på sådana variationer i begreppen ger en bättre förståelse för vad man menar matematiskt med "avstånd".

Inledning

Mitt ambition här är att visa lite av matematikens flexibilitet och kreativitet. Jag skall ge exempel på hur vi räknar i olika talsystem med ändligt många tal eller med en ovanlig mått istället för det vanliga avståndet. Det kanske känns konstigt i början, men jag hoppas att ni kommer att anse, med hjälp av några analogier, att det är helt naturligt.
Jag skulle egentligen påstå att de flesta matematiska begrepp som verkar artificiella i början motsvarar (medvetet eller omedvetet) naturliga begrepp. Annars skulle vi inte kunna hitta på dem. Problemet är att hitta en bra bild för att förstå, och våga ändra på bilden när man sedan lär sig mer om objekten.

Modulär aritmetik

Som uppvärming vill jag föreslå att vi räknar med bara ändligt många tal. När vi nått det sista talet kan vi helt enkelt komma tillbaka till det första.

Låter det artificiellt?
Här är några exempel från vardagslivet:
En strömbrytare räknar med 2 tillstånd. Den är antigen på eller av. Det spelar ingen roll hur många gånger den har ändrats sedan den installerats, bara om det var ett jämt eller udda antal gånger.
Man dansar vals i 3 takt, sedan börjar man om igen... ... ...
Årstiderna är 4, tills det börjar om igen, såsom takter i mycket musik, motorer, gående hästar....
Hela vår liv regeras av de 7 veckodagarna, 12 månaderna, 52 veckor (ungefär) om året, 365 dagar (ungefär) mellan födelsedagar, av de 12 timmar på klockan, de 24 timmar per dag. Och varför tycker vi att år 2000 kanske är lite speciellt?
I aritmetik har vi svårt att hantera ordet "ungefär" så vi använder alltid samma "modul" inom ett system. Däremot kan vi gå långt genom att upprepa det "modulära" processen, som man gör när man räknar 60 sekunder per minut, 60 minuter per timma, alltså $3600 = 60 * 60 = 60^2$ sekunder per timma. Det kan matematiker göra ända till oändligheten...
Med sådana "tal" kan man göra operationer "+" och "-" (10 dagar efter onsdag blir det lördag, 10 dagar före var det söndag), ibland multiplikation och till och med division.

Att mäta avstånd p-adiskt

Nu går vi tillbaka till ett oändligt talsystem (de positiva heltal) men vi skall ändra vår uppfattning av hur stora de är.
Alla här känner till absolutbeloppet, som mäter avståndet mellan två punkter och har följande grundläggande egenskaper :

$$(0) \quad |a| = 0 \iff a = 0$$

$$(1) \quad |a \cdot b| = |a| \cdot |b|$$

$$(2) \quad |a + b| \leq |a| + |b| \quad \text{(triangelolikhet)}$$

Men vad menar vi egentligen med ordet 'avstånd'? Vad betyder 'nära'?
Jag känner mig ganska nära min bror som bor i Paris, och mycket närmare min skolkompis i Lille än min granne i Göteborg. Vi kan säga att två personer är nära varandra om de har mycket gemensamt
Människornas liv har många olika aspekter, olika närhetskriterier.

Och heltal då? De består av produkter av potenser av olika primtal.
Vad har talen $5, 10, 15, 25$ gemensamt? Jo, de är delbara med 5.
Och $25, 75, 125$? Lite mer : delbarhet med 5^2.
Och $125, 250$ då? Ännu mer : 5^3.
Här har vi räknat med avseende på $p = 5$, alltså 5-adiskt, men vi kan ta vilket primtal p som helst och definiera

$$v_p(a) = \max\{i : p^i | a\}$$

för heltal $a \neq 0$, med $v_p(0) = \infty$; alltså är $v_p(a)$ antalet gånger p delar a. Talet $v_p(a)$ kallas för den **p-adiska valuationen** av a. Vi har $v_5(5) = v_5(10) = v_5(15) = 1$, $v_5(25) = v_5(75) = 2$, $v_5(125) = v_5(250) = 3$, $v_5(6) = v_5(36792) = 0$.
En valuation v_p uppfyller, för samtliga heltal a, b,

$$v_p(ab) = v_p(a) + v_p(b)$$

$$v_p(a + b) \geq \min(v_p(a), v_p(b))$$

(med likhet om $v(a) \neq v(b)$), till exempel $v_5(10+25) = 1$, $v_5(10+15) = 2$. Om valuationen av skillnaden mellan två tal är stor, då har de mycket gemensamt.
Vi kan lägga märke till att det är viktigt att ta ett primtal som bas : om jag försöker ta 10 som bas funkar det inte ty till exempel 10 delar varken 5 eller 4 men delar deras produkt.
Vi definierar ett **p-adiskt avstånd** genom

$$|a|_p = p^{-v_p(a)}$$

så att ett tal med stor valuation, alltså med "mycket gemensamt" med 0, får en liten värde, alltså "ligger nära" 0 Man kollar att det har de egenskaper som nämndes ovan för absolutbeloppet. Triangelolikheten kan t.o.m. ersättas av det strängare villkoret : (2′) $|a + b|_p \leq \max\{|a|_p, |b|_p\}$. Ett avstånd som uppfyller detta krav kallas **icke-arkimediskt** (det vanliga absolutbeloppet kallas arkimediskt).
Vi kan utvidga valuationen (och $|.|_p$) till de rationella talen : $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ och får $\frac{a}{b} = x = p^{v_p(x)} \cdot \frac{c}{d}$ med c, d heltal och $c \cdot d$ inte delbar med p.

Att skriva ett tal i bas p

Vi brukar skriva heltal (och även rationella och reella tal) i bas 10, dvs vi delar upp talet i potenser av 10. Basen 10 kommer förmodligen från hur många

fingrar vi har, men vilket tal som helst kan användas (och andra kulturer har använt bas 12 eller 60, som vi när vi räknar sekunder och minuter). I talteori väljer vi gärna ett primtal som bas. Till exempel är $7 = 6+1 = 2\times 3+1$ och det kan skrivas $[21]_3$ i bas $p = 3$, $25 = 18+6+1 = 2\times 3^2+2\times 3^1+1\times 3^0$ som skrivs $[221]_3$ och $152 = 81+54+9+6+2 = 1\times 3^4+2\times 3^3+1\times 3^2+2\times 3^1+2\times 3^0 = [12122]_3$.
Addition och multiplikation görs med samma metod som vanligt men man får en minnessiffra varje gång summan blir mer än p. Till exempel är $25+7 = [221]_3+[21]_3 = [1012]_3 = 27+3+2 = 32$ och $152+25 = [12122]_3+[221]_3 = [20120]_3 = 162+9+6 = 177$.
Detta sätt att skriva tal visar hur nära varandra talen är : två tal med samma siffror till höger, till exempel $[2121]_3$ och $[1121]_3$, är nära varandra ty skillnaden mellan de (här $[1000]_3$) är "liten" (här 3 gånger delbar med 3, dvs har valuation 3). Ett tal som $3^5 = [100000]_3$ som slutar med många 0-or har hög valuation, dvs är nära 0, alltså "litet".

p-adisk geometri

Nu vill jag nämna några fakta om p-adisk geometri som skiljer sig från den vanliga arkimediska geometrin.
För det första ritar man inte tal på samma plats som när man använder det arkimediska avstånd, på tallinjen eller på ett plan, eftersom $0, 1, 2$ inte är nära varandra, utan det är de höga potenser av p som ligger nära 0.
Ett sätt att framställa tal som tar hänsyn till det p-adiska avstånd är att rita ett "träd" där varje tal sitter på en löv. Vid "roten" börjar p grenar som motsvarar möjliga antal enheter (dvs p^0), var och en av dem delas i p grenar motsvarande antalet p, som delas i p grenar för antalet p^2... Figuren visar trädet för $p = 3$, upp till 3^2. Löven går upp till $[222]_3 = 26 = 3^3 - 1$. Talen som har gemensama delare hamnar på samma gren.
(HÄR TILLHÖR BILDEN AV ETT 3-ADISKT TRÄD)
Följande konstiga egenskap följer nu från det icke-arkimediska villkoret och kan tolkas geometriskt med hjälp av trädet.

- Samtliga trianglar är likbenta : en triangel ges av tre punkter a, b, c. Antag att det finns två sidor med olika längd. Att den tredje sidan (alltså summan av de två första) har samma längd som den längsta följer från det icke-arkimediska villkoret. Kolla med tre löv från trädet.

- I en (sluten) p-adisk cirkelskiva kan samtliga punkter räknas som "centrum": Låt $D(c, r) = \{x : |x-c|_p \leq p^{-r}\} = \{x : v_p(x-c) \geq r\}$, dvs mängden av punkter som är nära punkten c. Den motsvarar en gren på trädet som innehåller löven c och r snitt mot roten. Om d är en godtycklig punkt i D, så är $v_p(x-d) = v_p(x-c-(d-c)) \geq r$ för alla $x \in D$.

- Tag två slutna diskar. Antingen skär de inte varandra, eller så innehåller den ena den andra. Tänk på grenar!

p-adisk Analys

Vi kan komplettera $\mathbf{Q}$ på samma sätt som man konstruerar de reella talen. Betrakta alla Cauchy följder av rationella tal, (dvs följder som uppfyller : $\forall \varepsilon > 0$ finns en gräns s.a. avståndet (här det p-adiska avståndet) mellan två element som ligger efter gränsen är mindre än ε). Vi säger att två följder är ekvivalenta om skillnaden mellan de konvergerar mot 0 och låter $\mathbf{Q}_p$ bestå av alla ekvivalensklasser av Cauchy följder. Då har vi en fullständig kropp och kan bedriva (p-adisk) analys.
Hur ser ett p-adiskt tal ut då? På trädet skulle man rita grenar ut till oändligheten. Som ovan skrivs varje tal som summa av potenser av p. När man skriver ett reellt tal kan det finnas oändligt många siffror efter decimaltecknet (t.ex. 3,14159...). De motsvarar mindre och mindre tal, som så småningom blir försumbara. För p-adiska tal är det de stora potenser av p som blir försumbara, så man kan ha oändligt många siffror till höger!
Vi tar några exempel av 5-adiska tal :

$$36 = 1 + 2 * 5 + 1 * 25$$

$$-1 = 4 + 4 * 5 + 4 * 25 + 4 * 125 + 4 * 5^4 + 4 * 5^5 + 4 * 5^6 + \ldots.$$

ty om man läger till 1 till det som stor ovan, så får man en godtyckligt högt potens av 5, dvs ett godtyckligt litet tal, alltså 0.
Varför är detta nyttigt? Därför att de p-adiska kropparna $\mathbf{Q}_p$ speglar aritmetiska egenskaper, dvs faktoruppdelning i primtal, mer än $\mathbf{R}$ gör. Det är faktiskt ofta lättare att räkna med de än att räkna i $\mathbf{Q}$.
När man vill lösa en diofantisk ekvation, till exempel hitta heltal a, b, c sådana att $a^n + b^n = c^n$ (eller visa att det inte finns sådana), kan man till en början leta efter lösningar modulo p. Då arbetar man i en ändlig kropp, och det går

att prova på alla möjligheter. Om man hittar en lösning kan man fortsätta modulo p^2, sedan modulo p^3... och så småningom bygga en följd, t.o.m. en lösning i $\mathbf{Q}_p$. Då återstår det "bara" att göra likadant med alla andra primtal, och att se om de lokala lösningar man får i varje $\mathbf{Q}_p$ härstammer från en global lösning i $\mathbf{Q}$. Det svåra steget här är det senaste, men för vissa typer av problem är detta en väldigt framgångsrik strategi.

Kan man hitta på vad man vill?

Det var den tyske matematikern Kurt Hensel som först definierade de p-adiska tal i 1920-talet, i analogi med polynomringen och ringen av oändliga serier, med Ernst Kummer hade redan använt sig av liknande tal 1894.
Finns det andra typer av avstånd man kan hitta på?
För de rationella tal $\mathbf{Q}$ finns det ett avstånd till, nämligen det "triviala", där 0 har storlek 0 och alla andra element har storlek 1 (det är lätt att kolla att det uppfyller villkoren (0), (1), (2')). Men man kan bevisa att varje funktion över $\mathbf{Q}$ som uppfyller (0), (1) och (2) är ekvivalent med antigen det vanliga euklidiska avståndet, eller det p-adiska avståndet för något primtal p, eller också det triviala avståndet.
För de ändliga talsystem vi nämnde i början finns det bara det triviala avståndet. Varför?

Litteratur

- Capi Corrales Rodriganez, *p-adic number and non-archimedian valuations*, Proceedings of the 8th meeting of EWM : European Women in Mathematics, Trieste 1997 (tillgänglig på websajten http://www.math.helsinki.fi/EWM eller http://www.hindawi.com)

- F. Q. Gouvea, *P-adic numbers, an introduction*, Universitext, Springer-Verlag, Berlin 1997.