Metriska rum, $\mathbb{R}$ och p-adiska tal

Tony Johansson
1MA239: Specialkurs i Matematik II
Uppsala Universitet

VT 2018

När vi säger "avståndet mellan punkt X och punkt Y" där X och Y är punkter i planet (säg) är det underförstått att vi menar det *Euklidiska avståndet*, det vill säga det avstånd som en linjal skulle avslöja. Med koordinater $X = (x_1, \ldots, x_n), Y = (y_1, \ldots, y_n)$ i n dimensioner kan vi defininera det Euklidiska avståndet som

$$d_2(X, Y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}.$$

Inom matematik finns det ofta behov för annorlunda begrepp om avstånd. För $p \geq 1$ skulle vi till exempel kunna definiera *Minkowski-avståndet*

$$d_p(X, Y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p},$$

vilket generaliserar det Euklidiska avståndet. Man brukar även tillåta $p = \infty$, som vi definierar som

$$d_\infty(X, Y) = \max_{i=1,\ldots,n} |x_i - y_i|.$$

Vi ska börja med att definiera en *metrik* (avståndsfunktion), för att sedan se hur vårt grundläggande begrepp om reella tal kan förändras om vi mäter avstånd mellan rationella tal på ett nytt sätt.

1 Metriska rum

Ett *metriskt rum* (S, d) är en mängd S tillsammans med en funktion $d : S \times S \to \mathbb{R}$ sådan att om $x, y, z \in S$ så gäller

$$\begin{aligned} &(i)\ d(x,y) \geq 0, \\ &(ii)\ d(x,y) = d(y,x), \\ &(iii)\ d(x,y) = 0 \ \Leftrightarrow\ x = y, \\ &(iv)\ d(x,z) \leq d(x,y) + d(y,z). \end{aligned} \tag{1}$$

Det är ofta mer eller mindre trivialt att se att en funktion d uppfyller (i) – (iii), och det krav som kan kräva lite jobb är triangelolikheten (iv).

Vi säger att d är en metrik för S om (S, d) formar ett metriskt rum. Mängden S kan vara vad som helst, och d anger hur vi mäter avstånd mellan punkter i S.

Vi kan notera att om (S, d) är ett metriskt rum och $R \subseteq S$ så är (R, d) också ett metriskt rum: om (i) – (iv) håller för alla $x, y, z \in S$ så håller de givetvis för alla $x, y, z \in R$. Så exempelvis om d är en metrik för de komplexa talen $\mathbb{C}$ så är d också en metrik för alla delmängder av $\mathbb{C}$, framförallt $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$.

Här följer en mängd exempel på metriska rum.

1.1 Manhattanmetriken

Manhattanmetriken (*Manhattan metric* eller *taxicab metric* på engelska) är Minkowskimetriken på $\mathbb{R}^n$ med $p = 1$. Namnet beskriver metriken: $d_1(X, Y) = \sum_{i=1}^{n} |x_i - y_i|$ är kortaste vägen mellan X och Y om man bara tillåts resa parallellt med koordinataxlarna.

Vi bekräftar att d_1 är en metrik genom att visa att den uppfyller (i) – (iv) i (1). Låt $x, y, z \in \mathbb{R}^n$. För (ii) har vi

$$d(x,y) = \sum_{i=1}^{n} |x_i - y_i| = \sum_{i=1}^{n} |y_i - x_i| = d(y,x),$$

för (iii) ser vi att $d(x, y) = 0$ om och endast om $|x_i - y_i| = 0$ för alla i, men då måste vi ha $x = y$. För (iv) använder vi triangelolikheten för reella tal:

$|a+b| \leq |a| + |b|$ för alla $a, b \in \mathbb{R}$, så

$$d(x,z) = \sum_{i=1}^{n} |x_i - z_i| = \sum_{i=1}^{n} |x_i - y_i + y_i - z_i|$$
$$\leq \sum_{i=1}^{n} |x_i - y_i| + |y_i - z_i| = d(x,y) + d(y,z).$$

För att visa att Minkowskimetriken uppfyller (iv) för alla $p \geq 1$ används Minkowskis olikhet: för alla $p \geq 1$ gäller

$$\left(\sum_{i=1}^{n} |x_i - z_i|^p \right)^{1/p} \leq \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p} + \left(\sum_{i=1}^{n} |y_i - z_i|^p \right)^{1/p}.$$

Vi kommer inte bevisa Minkowskis olikhet här.

1.2 Grafmetriken

Låt G vara en graf med nodmängd V. Kantmängden E inducerar en metrik d_E på mängden V. För $x, y \in V$ definierar vi $d_E(x,y)$ som den kortaste vägen mellan x och y som bara använder kanter ur mängden E. Vi låter $d_E(x,y) = \infty$ om ingen sådan väg existerar. Det är uppenbart att (i) – (iii) uppfylls, och (iv) är också enkel: om P_{xy} är den kortaste vägen från x till y och P_{yz} den kortaste vägen från y till z, så får vi en väg från x till z genom att ta vägen $P_{xy} \cup P_{yz}$. Detta visar att

$$d(x,z) \leq |P_{xy} \cup P_{yz}| = d(x,y) + d(y,z).$$

1.3 Den diskreta metriken

Den diskreta metriken har ett teoretiskt värde i att den visar att det finns en metrik för S, oavsett vad S är för mängd. Den brukar betecknas δ, och vi definierar för $x, y \in S$

$$\delta(x,y) = \begin{cases} 1, & x \neq y, \\ 0, & x = y. \end{cases}$$

1.4 $\mathcal{L}^1$-metriken

Låt $C[0,1]$ vara mängden av kontinuerliga funktioner på det slutna intervallet $[0,1]$. För två kontinuerliga funktioner f, g definierar vi en metrik genom

$$d^1(f,g) = \int_0^1 |f(x) - g(x)| dx.$$

Det är uppenbart att $d^1(f,g) \geq 0$, eftersom $|f(x) - g(x)| \geq 0$ för alla x. Symmetrin $d^1(f,g) = d^1(g,f)$ är också enkel. Integralen är 0 om och endast om $|f(x) - g(x)| = 0$ för alla x, vilket ger oss (iii). Triangelolikheten (iv) följer från triangelolikheten för reella tal och linearitet för integraler;

$$\begin{aligned} d^1(f,h) = \int_0^1 |f(x) - h(x)|dx &= \int_0^1 |f(x) - g(x) + g(x) - h(x)|dx \\ &\leq \int_0^1 |f(x) - g(x)| + |g(x) - h(x)|dx \\ &= \int_0^1 |f(x) - g(x)|dx + \int_0^1 |g(x) - h(x)|dx \\ &= d^1(f,g) + d^1(g,h). \end{aligned}$$

Beviset påminner mycket om beviset ovan för Minkowskimetriken, och de två är nära relaterade. För $p \geq 1$ definierar vi $\mathcal{L}^p$-metriken

$$d^p(f,g) = \left(\int_0^1 |f(x) - g(x)|^p dx \right)^{1/p},$$

och Minkowskis olikhet gäller också för funktioner, det vill säga $d^p(f,h) \leq d^p(f,g) + d^p(g,h)$ kallas också Minkowskis olikhet.

Denna metrik är väldigt central inom avancerad analys. För $S \subseteq \mathbb{R}^n$ definierar man $\mathcal{L}^p(S)$ som mängden av funktioner $f : S \to \mathbb{R}$ som uppfyller $\int_0^1 |f(x)|^p dx < \infty$, och många resultat berör dessa så kallade $\mathcal{L}^p$-rum.

1.5 Hammingmetriken

Hammingmetriken är vanligt förekommande inom datavetenskap, och mäter avståndet mellan två ord (även kallade strängar). Vi definierar ett *alfabet* $\mathcal{A}$ som vilken mängd som helst (ofta $\{0,1\}$ inom datavetenskap), och ett *ord av längd* k som en följd av k element ur $\mathcal{A}$. Låt $\mathcal{A}^k$ vara mängden av ord av längd k. Vi skriver $x = x_1 x_2 \dots x_k$, där $x_i \in \mathcal{A}$ för $i = 1, \dots, k$. För $x, y \in \mathcal{A}^k$ definierar vi

$$H(x,y) = |\{i : x_i \neq y_i\}|.$$

Hammingmetriken anger alltså antalet bokstäver där orden x och y skiljer sig åt. Vi har till exempel (om $\mathcal{A}$ är vårt alfabet tillsammans med mellanrum)

H(kyrka, dyrka) $= 1 + 0 + 0 + 0 + 0 = 1$,

H(matematik, mytomanin) $= 0 + 1 + 0 + 1 + 0 + 0 + 1 + 0 + 1 = 4$

H(nationalencyklopedin, rationell cykelpedal) $= 8$

Återigen är (i) –(iii) uppenbara. Vi visar triangelolikheten (iv). Låt $A \subseteq \{1, 2, \ldots, k\}$ vara mängden av index där x och y skiljer sig åt, så att $H(x, y) = |A|$. Låt B vara samma sak för y och z, och C för x och z. Om $i \in C$, det vill säga om $x_i \neq z_i$, så måste antingen $x_i \neq y_i$ eller $y_i \neq z_i$ hålla. Därför har vi $C \subseteq A \cup B$, och

$$H(x, z) = |C| \leq |A \cup B| \leq |A| + |B| = H(x, y) + H(y, z).$$

Det går också att definiera Hammingavståndet mellan två ord x och y av olika längd genom att införa en extra bokstav $*$ till $\mathcal{A}$, och om x, y har respektive längder $k > \ell$ lägger vi $k - \ell$ stycken $*$ i början av y.

Hammingavståndet används flitigt inom kryptering och kodning. Vid tillämpningar som ligger närmare direkta språktillämpningar, till exempel rättstavningskontroller, använder man istället något som kallas Levenshteinavstånd (eller Levensjtejnavstånd om man föredrar svensk translitteration). Detta för att Hammingmetriken anser att orden *jölk* och *mjölk* ligger långt ifrån varandra, när de i själva verket bör betraktas som näraliggande i många tillämpningar. Levensjtejnavståndet räknar antalet raderingar, infogningar och substitueringar av tecken som krävs för att transformera den ena strängen till den andra, och anser alltså att avståndet mellan jölk och mjölk är 1, då allt som krävs är infogning (eller radering) av bokstaven m. Den här typen av avstånd kallas generellt *edit distance*, och det finns många variationer.

2 Den p-adiska metriken

Ett begrepp av storlek av heltal är antalet siffror i talet. Vi skulle kunna säga att storleken av 1241250 är 7, storleken av 817 är 3, och så vidare. Detta leder till en metrik på $x, y \in \mathbb{Z}$ där $d(x, y)$ är antalet siffror i differensen $x - y$. Här säger vi att talet 0 innehåller 0 siffror. Denna metriken är nära besläktad med den Euklidiska metriken på $\mathbb{Z}$, om än inte exakt samma så är det åtminstone ett begrepp av storlek som är konsekvent med hur vi alla tänker på storleken av ett tal.

Nu ska vi se vad som händer om vi vänder på vårt begrepp om storlek, för att istället anse att ett tal är litet om det *slutar* med många nollor. Alltså om vi anser att 2158192500 är mindre än 1249 enbart för att det slutar på fler nollor. Detta är det p-adiska (eller mer precist det 10-adiska) sättet att mäta storlek.

Definition 1. *Låt $x \in \mathbb{Z}$, och låt y, n vara de unika heltal sådana att $x =$*

$y \cdot 10^n$ *där* y *inte är delbart med* 10. *Den* 10-adiska storleken av x, *betecknad* $|x|_{10}$, *är* 10^{-n}. *Vi definierar* $|0|_{10} = 0$.

Så vi har

$$|1000|_{10} = 10^{-3}, \quad |-23000|_{10} = 10^{-3}, \quad |1581250|_{10} = 10^{-1}.$$

Detta leder till den 10-adiska metriken $d(x, y) = |x - y|_{10}$, så vi har till exempel

$$d(45822, 91822) = |45822 - 91822|_{10} = |-46000|_{10} = 10^{-3}$$
$$d(45822, 45823) = |-1|_{10} = 10^{-1},$$

så 45822 ligger närmare 91822 än 45823.

Än så länge har vi bara ett märkligt begrepp om storlek och avstånd. Det intressanta börjar hända när vi börjar undersöka gränsvärden. Vi säger att a_n konvergerar till a i den 10-adiska metriken om $\lim_{n\to\infty} |a_n - a|_{10} = 0$. Vi har till exempel $10^n \to 0$ och $n! \to 0$ i den 10-adiska metriken. Vi skriver $10^n \overset{10}{\to} 0$ för att göra det mer tydligt i vilken metrik vår konvergens sker.

Det är också sant att om $a_1 = 9, a_2 = 99, a_3 = 999$ och så vidare, alltså $a_n = 10^n - 1$ består av n nior, så gäller $a_n \overset{10}{\to} -1$. Detta bekräftar vi genom

$$|a_n - (-1)|_{10} = |10^n - 1 - (-1)|_{10} = 10^{-n},$$

så $\lim |a_n - (-1)|_{10} = 0$.

Vi kan byta ut talet 10 mot vilket heltal p som helst. Som bokstaven antyder används oftast ett primtal, då detta leder till fördelaktiga algebraiska egenskaper.

Definition 2. *Låt* $x \in \mathbb{Z}$ *och låt* p *vara ett positivt heltal. Låt* y, n *vara de unika heltal sådana att* $x = y \cdot p^n$ *där* y *inte är delbart med* p. *Den* p-adiska storleken av x, *betecknad* $|x|_p$, *är* p^{-n}. *Vi definierar* $|0|_p = 0$.

Än så länge har vi en definition av p-adisk storlek och avstånd mellan heltal. Kan vi utvidga denna till de rationella talen $\mathbb{Q}$, och de reella talen $\mathbb{R}$? Svaret är ja för $\mathbb{Q}$.

Definition 3. *Låt* $x \in \mathbb{Q}$ *och låt* p *vara ett positivt heltal. Låt* $y, n \in \mathbb{Z}$ *och* $z \in \mathbb{N}$ *vara de unika heltal för vilka* $x = \frac{y}{z}p^n$, *där varken* y *eller* z *är delbart med* p. *Den* p-adiska storleken av x, *betecknad* $|x|_p$, *är* p^{-n}.

Detta storleksbegrepp leder till en p-adisk metrik på $\mathbb{Q}$ via $d(x, y) = |x - y|_p$.

De reella talen $\mathbb{R}$ är en helt annan fråga. För icke-rationella tal såsom $\sqrt{2}$ är det inte bara så att $|\sqrt{2}|_p$ är svårt att definiera på något rimligt sätt: för vissa p kommer inte $\sqrt{2}$ kunna definieras. Mer om det senare.

3 Gränsvärden i metriska rum

Vi definierar nu hur gränsvärden fungerar i metriska rum.

Definition 4. *Låt (S, d) vara ett metriskt rum. För en sekvens $(x_n)_{n\geq 0}$ i S och ett element $x \in S$ säger vi att (x_n) konvergerar till x, betecknat $\lim_{n\to\infty} x_n = x$ eller $x_n \to x$, om det för varje $\varepsilon > 0$ existerar ett N så att $n \geq N$ implicerar $d(x_n, x) < \varepsilon$.*

Notera att detta stämmer perfekt med den definitionen ni känner till när $S = \mathbb{R}^n$ och metriken är det Euklidiska avståndet.

Generellt är det viktigt att påpeka vilket metriskt rum vi arbetar med när vi pratar om konvergens.

4 Reella kontra p-adiska tal

Hur skulle du definiera mängden av reella tal? Ett naturligt sätt är att definiera ett (ändligt) reellt tal x som en sekvens (x_i) för $-\infty < i \leq \ell$ av siffror, så att

$$x = x_\ell x_{\ell-1} x_{\ell-2} \dots x_1 x_0 \,.\, x_{-1} x_{-2} \dots .$$

där alltså $x_\ell, \dots, x_0$ är siffrorna i heltalet, och $x_{-1}, x_{-2}, \dots$ är decimalerna. För π har vi till exempel $\ell = 0$ (eftersom tiotalen, hundratalen etc är noll) och $x_0 = 3$, $x_{-1} = 1, x_{-2} = 4, x_{-3} = 1$ och så vidare. Mer formellt kan vi skriva

$$x = \sum_{i=-\infty}^{\ell} x_i \cdot 10^i, \quad x_i \in \{0, 1, \dots, 9\}.$$

Med denna definitionen definierar vi alltså x som gränsvärdet

$$x = \lim_{n\to\infty} \sum_{i=-n}^{\ell} x_i \cdot 10^i.$$

Eftersom vi jobbar med ett gränsvärde är det viktigt att påpeka vilken metrik vi använder, och i detta fall är det den Euklidiska metriken som används. Utan att använda gränsvärden är det omöjligt att definiera de reella talen. Vissa tal såsom $\sqrt{2}$ kan definieras utifrån polynom ($\sqrt{2}$ är en lösning till $x^2 - 2 = 0$), men mängden av tal som är lösningar till polynom (så kallade algebraiska tal) är en försvinnande liten mängd jämfört med de som inte kan det (så kallade transcendenta tal).

De reella talen definieras alltid som gränsvärden av rationella tal. Gränsvärden är kraftigt beroende av en metrik, och vi använde oss av den Euklidiska

metriken. Frågan är vad som händer om vi använder oss av en annan metrik. För att se det måste vi först ge oss in på en djupare diskussion om exakt hur de reella talen definieras.

4.1 De reella talen

Vi går nu in på djupet för att se hur de reella talen, mängden $\mathbb{R}$, definieras. I denna och nästa del kommer vi låtsas att vi befinner oss i två olika världar:

- **Värld A:** Vi känner bara till $\mathbb{Q}$ och den Euklidiska metriken på $\mathbb{Q}$.
- **Värld B:** Vi känner bara till $\mathbb{Q}$ och den p-adiska metriken på $\mathbb{Q}$.

I denna delen låtsas vi att vi är i värld A, och ser hur vi definierar $\mathbb{R}$. I nästa del ser vi vad som händer om vi går igenom exakt samma steg i värld B.

Vi börjar med att definiera de rationella talen

$$\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}.$$

I värld A har vi ett problem: ett gränsvärde av rationella tal är inte nödvändigtvis rationellt. Vi kan till exempel definiera en sekvens $(a_0, a_1, \dots)$ via $a_0 = 1$ och för $n \geq 0$,

$$a_{n+1} = \frac{a_n}{2} + \frac{1}{a_n}. \tag{2}$$

Varje tal i den här sekvensen är rationellt. Vi har

$$\begin{aligned} a_1 &= \frac{3}{2} = 1.5, \\ a_2 &= \frac{17}{12} = 1.41\overline{6}, \\ a_3 &= \frac{577}{408} \approx 1.414215686274, \\ a_4 &= \frac{665857}{470832} \approx 1.4142135623746, \end{aligned}$$

och så vidare. Men gränsvärdet $a = \lim a_n$, om det existerar, måste uppfylla $a = a/2 + 1/a$, alltså $a^2 = 2$, och vi vet att inget rationellt tal kan uppfylla $a^2 = 2$. (Sekvensen a_n används vid approximering av $\sqrt{2}$ via den "Babylonska algoritmen".)

I värld A är vi nu förvirrade. Vi har en sekvens (a_n) av rationella tal som verkar konvergera mot något, men utan kännedom om talet $\sqrt{2}$ vet vi inte vad vi ska säga att a_n konvergerar till. Hur vet vi ens säkert att (a_n)

konvergerar när det inte verkar konvergera mot något tal vi känner till? Vi kan inte visa att $\lim |a_n - \sqrt{2}| = 0$, för talet $\sqrt{2}$ existerar inte i värld A.

Vi behöver först och främst kunna avgöra om en sekvens (a_n) av rationella tal konvergerar utan att nödvändigtvis ha något begrepp om vad gränsvärdet är. Lösningen är att definiera en *Cauchysekvens*.

Definition 5. *Låt (S, d) vara ett metriskt rum, och (a_n) en sekvens i S. Vi säger att (a_n) är en* Cauchysekvens *om det för varje $\varepsilon > 0$ existerar ett N sådant att om $m, n \geq N$ så är*

$$d(a_m, a_n) < \varepsilon.$$

Det går att visa att en sekvens konvergerar om och endast om den är en Cauchysekvens. För att avgöra om en sekvens konvergerar räcker det alltså att avgöra om det är en Cauchysekvens, vilket inte kräver någon vetskap om vad gränsvärdet är.

Det går att visa att sekvensen (2) är en Cauchysekvens, så vi vet att (a_n) konvergerar, och att gränsvärdet inte kan vara rationellt eftersom det måste uppfylla $a^2 - 2 = 0$.

Låt nu $\mathbb{Q}^*$ vara mängden av Cauchysekvenser i $\mathbb{Q}$. Vi har nått fram till den riktiga definitionen av $\mathbb{R}$.

Definition 6. *De* reella talen *är mängden av gränsvärden för Cauchysekvenser i $\mathbb{Q}$, det vill säga*

$$\mathbb{R} = \left\{ \lim_{n\to\infty} a_n \middle| (a_n) \in \mathbb{Q}^* \right\},$$

Det här verkar kanske som en onödigt krånglig definition, men den är absolut nödvändig. Om vi tänker efter så är det ändå så här vi brukar tänka på reella tal. Vissa reella tal har en enkel definition, som till exempel

- $\sqrt{2}$ är den unika positiva lösningen till $x^2 - 2 = 0$,
- π är arean av en cirkel med radie 1,
- e är gränsvärdet av $(1 + 1/n)^n$.

Men generellt är reella tal inte så enkla att beskriva. Om en enkel beskrivning saknas gör vi vårt bästa genom att skriva ner så många decimaler som möjligt, till exempel $a \approx 3.51356476135142$. Det vi *faktiskt* gör är att välja en sekvens a_n som konvergerar till a (förslagsvis sekvensen a_n som anger de första n decimalerna av a), och anger a_n för ett så stort n som vi kan.

4.2 De p-adiska talen

Vi förflyttar oss nu till värld B, där den p-adiska metriken (för något fixt p) är det naturliga begreppet om avstånd mellan rationella tal. Vi kommer igen hamna i situationer där Cauchysekvenser i $\mathbb{Q}$ inte nödvändigtvis konvergerar till något rationellt tal.

Definition 7. *Låt $p \geq 2$ vara ett heltal, och låt $\mathbb{Q}^p$ vara mängden av Cauchysekvenser av rationella tal under den p-adiska metriken. De* p-adiska talen *är*

$$Q_p = \left\{ \lim_{n\to\infty}^{p} a_n \middle| (a_n) \in \mathbb{Q}^p \right\},$$

där $\lim^p$ betecknar gränsvärde i den p-adiska metriken.

Mängden Q_p skiljer sig från $\mathbb{R}$ på många sätt. Till att börja med ser Cauchysekvenser helt annorlunda ut. Om (a_n) är en Cauchysekvens i den Euklidiska metriken kommer alla a_n för tillräckligt stora n överensstämma i de första 100 decimalerna, säg, medan Cauchysekvenser i den 10-adiska metriken är överens om de *sista* 100 siffrorna. En 10-adisk Cauchysekvens kan se ut så här:

$$\begin{aligned} &351981234.33 \\ &11515321.53 \\ &1902409151.53 \\ &686889451.53 \\ &9009451.53 \\ &1000009451.53 \\ &\vdots \end{aligned}$$

Dessa tal kommer närmare och närmare varandra, för att de är överens om fler och fler siffror läst från höger. Så medan reella tal skrivs som

$$x = \pm \sum_{i=-\infty}^{\ell} x_i \cdot 10^i$$

för något ändligt ℓ så skrivs 10-adiska tal som

$$x \overset{10}{=} \sum_{i=-\ell}^{\infty} x_i \cdot 10^i$$

för något ändligt ℓ. Mer generellt kan vi skriva p-adiska tal som

$$x \stackrel{p}{=} \sum_{i=-\ell}^{\infty} x_i \cdot p^i \tag{3}$$

där $x_i \in \{0, 1, \ldots, p-1\}$ och ℓ är ändligt. Vi kan då skriva x som

$$x \stackrel{p}{=} \ldots x_2 x_1 x_0 \, . \, x_{-1} x_{-2} \ldots x_{-\ell},$$

där x_i kallas de "p-adiska siffrorna för x".

4.3 1/3 i p-adiska tal

Som jag hävdar i (3) kan p-adiska tal skrivas som ett tal som har oändligt många siffror åt vänster, men alltid ett ändligt antal siffror åt höger. Samtidigt hävdar jag att $1/3 = 0.3333\ldots$ är ett p-adiskt tal, eftersom Q_p innehåller $\mathbb{Q}$. Detta måste innebära att $1/3$ har en annan representation i p-adiska tal, som vi nu visar för $p = 10$.

Vi konstaterar först att $|1/3|_{10} = |10^0 \cdot 1/3|_{10} = 10^0 = 1$, så i representationen (3) av $1/3$ måste $\ell = 0$. Vi beräknar nu de 10-adiska siffrorna $x_0, x_1, \ldots$. Den grunläggande observationen som används för att beräkna x_i är att för varje $k \geq 1$ gäller

$$\frac{1}{3} \mod 10^k = \left(\sum_{i=0}^{\infty} x_i \cdot 10^i \right) \mod 10^k = \sum_{i=0}^{k-1} x_i \cdot 10^i.$$

Vi måste också ha $3 \cdot 1/3 = 1$, och $1 \mod 10^k = 1$ för alla k. Vi får det oändliga ekvationssystemet

$$\sum_{i=0}^{k-1} x_i \cdot 10^i \equiv 1 \mod 10^k, \quad k \geq 1.$$

För $k = 1$ ger detta att $3x_0 \equiv 1 \mod 10$, med lösning $x_0 = 7$. För $k = 2$ får vi

$$3(x_0 + 10x_1) \equiv 21 + 30x_1 \equiv 1 \mod 100,$$

vilket kan skrivas om som $30x_1 \equiv -20 \mod 100$ med lösning $x_1 = 6$. För $k = 3$ får vi

$$3(x_0 + 10x_1 + 100x_2) \equiv 3(7 + 60 + 100x_2) \equiv 201 + 300x_2 \equiv -1 \mod 1000,$$

med lösning $x_2 = 6$. Det visar sig att $x_i = 6$ för alla $i \geq 1$, så den 10-adiska representationen av $1/3$ är

$$\frac{1}{3} \stackrel{10}{=} \ldots 66666667.$$

Det visar sig att den p-adiska representationen av rationella tal alltid har antingen en ändlig representationen eller en som upprepar sig oändligt, precis som för den klassiska representationen av rationella tal.

4.4 p-adisk representation av negativa tal

Notera att (3), till skillnad från representationen av reella tal, saknar ett tecken $\pm$. Detta är för att det inte behövs: som vi noterat tidigare är

$$-1 \stackrel{p}{=} \ldots (p-1)(p-1)(p-1),$$

alltså

$$-1 = \sum_{i=0}^{\infty} (p-1)p^i.$$

Detta för att

$$\sum_{i=0}^{n} (p-1)p^i = (p-1)\sum_{i=0}^{n} p^i = (p-1)\frac{p^{n+1}-1}{p-1} = p^{n+1} - 1 \stackrel{p}{\to} -1.$$

Om nu ett positivt tal $x > 0$ kan skrivas p-adiskt som

$$x \stackrel{p}{=} \sum_{i=-\ell}^{\infty} x_i p^{\ell},$$

så kan vi få representationen för $-x$ som en produkt av serier:

$$-x = (-1)(x) \stackrel{p}{=} \left(\sum_{i=0}^{\infty} (p-1)p^i\right)\left(\sum_{i=-\ell}^{\infty} x_i p^i\right) = \sum_{i=-\ell}^{\infty} y_i p^i$$

där siffrorna ges av

$$y_i = \sum_{j=0}^{i} (p-1)x_{i-j}.$$

Vi visar inget exempel på detta – poängen är att negativa tal kan representeras utan tecken.

4.5 $\sqrt{q}$ i p-adiska tal

Låt oss se om vi kan hitta en p-adisk representation för $\sqrt{2}$. Först testar vi $p = 10$. Vi noterar att för alla 10-adiska tal x gäller

$$|x^2|_{10} = |x|_{10}^2,$$

eftersom

$$x^2 = \left(\sum_{i=-\ell}^{\infty} x_i \cdot 10^i\right)^2 = x_{-\ell}^2 \cdot 10^{-2\ell} + \ldots,$$

och eftersom 10 inte delar $x_{-\ell}$ så delar det inte heller $x_{-\ell}^2$. (Notera att $|xy|_{10} = |x|_{10}|y|_{10}$ inte håller generellt, se Problem 3). Eftersom $|2|_{10} = 1$ så måste vi också ha $|\sqrt{2}|_{10} = 1$. Detta innebär att

$$\sqrt{2} \overset{10}{=} \sum_{i=0}^{\infty} x_i \cdot 10^i$$

där $x_0 \neq 0$. Då har vi

$$2 \equiv (\sqrt{2})^2 \equiv \left(\sum_{i=0}^{\infty} x_i \cdot 10^i\right)^2 \equiv x_0^2 \mod 10, \tag{4}$$

eftersom alla andra termer innehåller minst en 10-faktor. Men en heltalskvadrat slutar aldrig med 2 ($1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 1\underline{6}, 5^2 = 2\underline{5}, 6^2 = 3\underline{6}, 7^2 = 4\underline{9}, 8^2 = 6\underline{4}, 9^2 = 8\underline{1}$), så (4) saknar lösning. Vi drar slutsatsen:

$$\sqrt{2} \textit{ existerar inte i } Q_{10}.$$

Detta låter ju definitivt som en dålig egenskap jämfört med $\mathbb{R}$, men då ska vi komma ihåg att $\mathbb{R}$ inte innehåller någon lösning till $x^2 + 1 = 0$. Kanske gör Q_{10} det? Det visar sig att svaret är nej där också, men vi ska se att andra p ger $\sqrt{-1} \in Q_p$. Ur en algebraisk synpunkt är Q_{10} en ganska dålig mängd, eftersom den inte är ett så kallat *integritetsområde*: det går att hitta $x \neq 0$ och $y \neq 0$ sådana att $xy \overset{10}{=} 0$, vilket inte är särskilt önskvärt.

Om vi istället låter p vara ett primtal kommer saker se bättre ut. Låt $p = 7$. I Q_7 kan vi hitta $\sqrt{2}$. Om vi går igenom samma steg som ovan har vi

$$2 \equiv \sqrt{2}^2 \equiv \left(\sum_{i=0}^{\infty} x_i \cdot 7^i\right)^2 \equiv x_0^2 \mod 7,$$

med lösning $x_0 = 3$. (Notera att lösningen, precis som vi är vana vid när det kommer till kvadratrötter, inte är unik). Vi får x_1 via

$$2 \equiv (x_0 + 7x_1)^2 \equiv x_0^2 + 14x_1x_0 \equiv 9 + 42x_1 \mod 49,$$

med lösning $x_1 = 1$. I nästa steg kräver vi ($7^3 = 343$)

$$2 \equiv (x_0 + 7x_1 + 49x_2)^2 \equiv (10 + 49x_2)^2 \equiv 100 + 980x_2 \mod 343$$

där termen $(49x_2)^2$ är delbar med 343 och därmed försvinner. Denna ekvation har lösning $x_2 = 2$. Vi har än så länge visat att

$$\sqrt{2} \overset{7}{\approx} 213.$$

Vi har inte lyckats visa att $\sqrt{2}$ faktiskt existerar exakt. Till det har vi Hensels lemma:

Lemma 1 (Hensels lemma, specialfall)**.** *Låt p vara ett primtal och q ett heltal. En lösning $x = \sqrt{q}$ till $x^2 = q$ existerar i Q_p om och endast om det finns ett $x_0 \in \{0, 1, \ldots, p-1\}$ sådant att $x_0^2 \equiv q \mod p$.*

Vi kan hänvisa till Hensels lemma för att dra slutsatsen att $\sqrt{2} \in Q_7$. Hensels lemma säger också att $\sqrt{-1} \notin Q_7$, men vi kan dra slutsatsen att $\sqrt{-1} \in Q_5$, eftersom $2^2 \equiv -1 \mod 5$.

5 Problem

OBS: Alla problem fick inte plats på en sida.
Varje problem är värt totalt 8p.

1. Genom att bekräfta (i)–(iv) i definitionen (1), visa att om $d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ är en metrik på $\mathbb{R}$, $\alpha > 0$ och $\beta > 0$ är reella tal och $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}^2$ så är

$$D(x, y) = \alpha d(x_1, y_1) + \beta d(x_2, y_2)$$

   en metrik på $\mathbb{R}^2$.

2. Visa att Minkowskiavståndet på $\mathbb{R}^2$ inte är en metrik för $p = 1/2$, det vill säga att om $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}^2$ så är

$$d(x, y) = \left(\sqrt{|x_1 - y_1|} + \sqrt{|x_2 - y_2|}\right)^2$$

   inte en metrik.

   Ledtråd: Hitta ett exempel på punkter så att inte alla kraven (i)–(iv) i (1) håller.

3. (a) (4p) Visa att om p är ett primtal så är $|xy|_p = |x|_p|y|_p$ för alla heltal x, y.

   (b) (4p) Anta att p *inte* är ett primtal, det vill säga $p = rs$ för heltal $r, s > 1$. Ge exempel på (ändliga) heltal x, y sådana att $|xy|_p < |x|_p|y|_p$.

4. Anta att d är en metrik i ett metriskt rum (S, d) som uppfyller den *starka triangelolikheten*

$$d(x, z) \leq \max\{d(x, y), d(y, z)\}.$$

   Visa att om $x, y, z \in S$ så gäller minst en av följande likheter:

$$d(x, y) = d(y, z), \quad d(x, y) = d(x, z), \quad d(x, z) = d(y, z)$$

5. Visa att mängden av heltal $\mathbb{Z}$ med den p-adiska metriken (ni får välja ett specifikt p om det underlättar) uppfyller den starka triangelolikheten, alltså att

$$|x - z|_p \leq \max\{|x - y|_p, |y - z|_p\}$$

för alla $x, y, z \in \mathbb{Z}$. (Detta är sant för hela Q_p, men ni behöver bara visa det för $\mathbb{Z}$).

Ledtråd: Låt a, b, m, n vara sådana att $x - y = ap^m, y - z = bp^n$, där a, b ej är delbara med p. Dela in i fall beroende på om $m = n$ och vad summan $a + b$ är.