SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

De p-adiska talen

av

David Abaas

2024 - No K7

De p-adiska talen

David Abaas

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Håkan Granath

2024

Sammanfattning

Även om p-adiska tal spelar en avgörande roll inom områden som talteori, är de ofta inte välkända bland kandidatstudenter i matematik. Denna uppsats syftar till att belysa de p-adiska talens gåtfulla natur genom att bygga upp och redogöra för den bakomliggande teorin, samt att belysa deras tillämpningar i kontexten av Hensels lemma och Newton-Raphsons metod. Dessutom kompletteras den teoretiska diskussionen med konkret implementering i Python, vilket kan möjliggöra en djupare förståelse genom praktiska exempel och tillämpningar.

Abstract

Although p-adic numbers play a crucial role in fields such as number theory, they are often not well known among undergraduate students in mathematics. This essay aims to illuminate the enigmatic nature of the p-adic numbers by building and explaining the underlying theory, as well as highlighting their applications in the context of Hensel's lemma and the Newton-Raphson method. In addition, the theoretical discussion is supplemented with a concrete implementation in Python, which can enable a deeper understanding through practical examples and applications.

Innehåll

1 Introduktion

1.1 Inledande ord

I slutet av 1800-talet påbörjade Kurt Hensel sin forskning kring de p-adiska talen. Hensel, vars tidigare arbete inom området var starkt influerat av hans intresse för algebraiska ekvationer och deras lösningar, inspirerades av tidigare arbeten av matematikerna Krockener, Dedekind och Weber som observerat paralleller mellan primtal och linjära faktorer inom taltoeri och funktionstoeri. Hensels insikt låg i att upptäcka och utforska dessa likheter, varpå han utvecklade en metod för att hantera tal genom deras primtalsfaktorer. Denna metod lade grunden för p-adiska tal, som en utvidgning av de rationella talen med konvergerande serier av potenser av ett primtal p. Hensels insikt var avgörande för utvecklingen av modern algebraisk talteori och har både haft och fortsätter ha långtgående konsekvenser inom området.

Till skillnad från det traditionella, reella talsystemet som vi är vana vid, består det p-adiska systemet istället av potenser av ett primtal p som avgör ett tals 'storlek'. Denna omkastning av perspektiv medför att de p-adiska talen ofta har spännande egenskaper.

Det är i denna kontext som den här uppsatsen utforskar de p-adiska talen. Genom att studera de p-adiska talens grundläggande konstruktion och egenskaper, syftar arbetet till att ge en djupare förståelse kring detta talssystem.

Till en början jobbar vi informellt, med formella potensserier, för att därefter bygga upp en mer robust teori. Vi börjar med att introducera grundläggande egenskaper och aritmetik av p-adiska tal. Därefter utforskar vi specifika problem där p-adiska tal erbjuder erbjuder intressanta lösningar. Sedan studerar vi olika centrala koncept som p-adiska valueringar och Ostrowskis sats, för att senare presentera en mer formell konstruktion av de p-adiska talen betecknade som $\mathbb{Q}_p$. Vi fortsätter med en ytlig genomgång av p-adisk analys, varpå tillämpningar av Hensels lemma och Newton-Raphsons metod behandlas. Som avslutning undersöks praktiska exempel och tillämpningar implementerade i Python.

1.2 Serier i olika talsystem

En matematisk serie representeras som en oändlig summa

$$\sum_{k=0}^{\infty} a_k = a_0 + a_1 + a_2 + \dots$$

Låt oss nu utforska olika sätt tolka konvergensen av en sådan serie.

1.3 Konvergens och divergens i reella talsystemet

Först undersöks serier inom det reella talsystemet, $\mathbb{R}$. En serie sägs konvergera om följden av dess partialsummor $S_n = \sum_{k=0}^{n} a_k$ konvergerar mot ett reellt tal. Ett välkänt exempel är den geometriska serien

$$\sum_{k=0}^{\infty} r^k = \frac{1}{1-r},$$

som är konvergent om kvoten r uppfyller $|r| < 1$. Då $|r| \geq 1$ divergerar serien.

1.4 Konvergens i p-adiska tal

I det p-adiska fallet ser vi annorlunda på serier. Betrakta till exempel serien

$$\sum_{k=0}^{\infty} 2^k = 1 + 2 + 4 + 8 + \dots \tag{1.1}$$

I det reella talsystemet divergerar denna serie med kvoten $r = 2$. Men inom ramen för det 2-adiska systemet visar det sig att denna serien faktiskt konvergerar. I det 2-adiska talsystemet så kan vi säga att

$$1 + 2 + 4 + 8 + 16 + \cdots = \frac{1}{1-2} = -1. \tag{1.2}$$

Varför kan denna till synes divergenta serien konvergera mot -1 i det 2-adiska systemet? Detta väcker frågor om hur vår uppfattning om storlek skiljer sig mellan dessa talsystem.

2 Informell definition av p-adiska tal

Låt p vara ett primtal. Ett p-adiskt tal kan informellt definieras som formella serier och uttryckas på formen

$$\sum_{i \geq n_0} a_i p^i, \tag{2.1}$$

där varje koefficient uppfyller villkoret $0 \leq a_i < p$ för alla a_i och $n_0 \in \mathbb{Z}$ kan vara negativt.

2.1 Rationella tal som p-adiska tal

En intressant aspekt är hurvida alla rationella tal $\mathbb{Q}$ kan uttryckas i detta format (2.1). Precis som vi sett att i det reella talsystemet kan konvergens definieras via partialsummor, kan varje rationellt tal närmas genom deras p-adiska partialsummor. Vi säger att ett tal $x \in \mathbb{Q}$ har en p-adisk representation enligt ovan, om det uppfyller kongruensförhållandet

$$x \equiv \sum_{i=n_0}^{n} a_i p^i \pmod{p^{n+1}} \tag{2.2}$$

för varje heltal n. Här har vi använt en generalisering av det vanliga kongruensbegreppet för heltal enligt följande definition.

Definition 2.3. Låt p vara ett primtal och m vara ett heltal. Två rationella tal x och y sägs vara *kongruenta modulo* p^m, betecknat som

$$x \equiv y \pmod{p^m}$$

om deras skillnad $x - y$ är en multipel av p^m. Dvs, om det finns ett $k \in \mathbb{Q}$ vars nämnare inte är delbar med p sådant att

$$x - y = k \cdot p^m.$$

Exempel 2.4. Betrakta talet -1 i $\mathbb{Q}$. För att visa att serien (1.1), som vi tidigare påstod konvergerade mot -1 enligt ekvation (1.2), uppfyller kongruensförhållandet (2.2), observerar vi följande:

$$\sum_{i=0}^{n} 2^i = 1 \cdot 2^0 + 1 \cdot 2^1 + \ldots + 1 \cdot 2^n = 2^{n+1} - 1 \equiv -1 \pmod{2^{n+1}}.$$

Så serien (1.1) konvergerar mot -1 i det 2-adiska systemet.

Lemma 2.5. *Varje koefficient a_i i en p-adisk representation av ett rationellt tal är unik.*

Bevis. Antag att det finns två olika p-adiska representationer av samma rationella tal, så

$$x = \sum_{i \geq n_0} a_i p^i = \sum_{i \geq n_0} b_i p^i,$$

där alla $0 \leq a_i, b_i < p$. Om dessa två serier verkligen representerar samma tal x, men skiljer sig åt i minst en term, måste det finnas ett minsta index j där $a_j \neq b_j$. För detta index blir skillnaden mellan partialsummorna $\sum_{i=n_0}^{i} a_i p^i$ och $\sum_{i=n_0}^{j} a_i p^i$, $(a_j - b_j)p^j$. För att serierna ska representera samma tal x, måste denna skillnad uppfylla

$$(a_j - b_j)p^j \equiv 0 \pmod{p^{j+1}}.$$

Eftersom $0 \leq a_i, b_i < p$ och $a_j \neq b_j$, kan inte $(a_j - b_j)p^j$ vara delbart med p^{j+1}, vilket leder till en motsägelse. Därför måste varje koefficient a_i vara unik. □

Efter att ha etablerat att koefficienterna i en p-adisk representation är unika, är nästa steg att visa att alla rationella tal faktiskt har en p-adisk representation.

Sats 2.6. *Alla rationella tal $x \in \mathbb{Q}$ har en p-adisk representation.*

Bevis. Låt p vara ett primtal och $x = \frac{a}{b} \in \mathbb{Q}$, där $a, b \in \mathbb{Z}$ och $\mathrm{SGD}(a, b) = 1$. Anta först att $p \nmid a, b$. Vi vill hitta talföljden $a_0, a_1, a_2, \ldots$, där $0 \leq a_i < p$ för alla i så att

$$x = \sum_{i=0}^{\infty} a_i p^i.$$

Vi definierar följden

$$\alpha_n = \sum_{i=0}^{n} a_i p^i$$

för $n \geq -1$. Notera att $x \equiv \alpha_n \pmod{p^{n+1}}$ är ekvivalent med att

$$a - b\alpha_n = k_n p^{n+1} \tag{2.7}$$

för något heltal k_n. Detta gäller för $n = -1$ med $\alpha_{-1} = 0$ och $k_{-1} = a$. Antag att (2.7) gäller för något $n \geq -1$. Vi vill nu hitta nästa term, så vi söker $a_{n+1} \in \{0, 1, \ldots, p-1\}$ och $k_{n+1} \in \mathbb{Z}$ så att om

$$\alpha_{n+1} = \alpha_n + a_n p^n \tag{2.8}$$

så är

$$a - b\alpha_{n+1} = k_{n+1} p^{n+2}. \tag{2.9}$$

Då ger (2.7) och (2.8) att (2.9) blir

$$k_n - b a_{n+1} = k_{n+1} p.$$

Så med a_{n+1} som den unika lösningen till

$$ba_{n+1} \equiv k_n \pmod{p}$$

kan vi sätta

$$k_{n+1} = (k_n - ba_{n+1})/p \in \mathbb{Z}$$

så att (2.9) gäller.

För det allmänna fallet, om $x = p^k \frac{a'}{b'}$ med $k \in \mathbb{Z}$ och $p \nmid a', b'$, låter vi $\frac{a'}{b'} = \sum_{i=0}^{\infty} a_i p^i$ enligt ovan. Då är

$$x = \sum_{i=k}^{\infty} a_{i-k} p^i.$$

Genom att följa dessa steg kan vi konstruera en p-adisk representation för varje rationellt tal, vilket visar att varje sådant tal har en sådan representation □

Vi ska nu se hur vi kan uttrycka p-adiska tal på ett intuitivt och effektivt sätt.

2.2 p-adisk decimalframställning

Precis som vi använder decimaler för att representera tal i det traditionella talsystemet med basen 10, kan vi använda en liknande notation för att representera tal i den p-adiska talsystemet, men med basen p, ett primtal. Termen 'decimaler' är vanligtvis kopplad till basen 10, i det p-adiska systemet bör vi överväga en mer lämplig term, som 'koefficienter'.

Som exempel, för att illustrera principen, om vi har en p-adisk serie,

$$x = \sum_{i \geq -2} a_i p^i = \ldots a_3 p^3 + a_2 p^2 + a_1 p + a_0 + a_{-1} p^{-1} + a_{-2} p^{-2},$$

så skriver vi den som

$$x = \ldots a_3 a_2 a_1 a_0, a_{-1} a_{-2},$$

där alltså varje koefficient a_i är ett heltal som uppfyller $0 \leq a_i < p$. Här fortsätter 'decimalerna' eller 'koefficienterna' till vänster om kommat, till skillnad från det vi är vana vid för reella tal där decimalerna fortsätter åt höger.

Exempel 2.10. Vi återvänder till exemplet med talet -1 och dess 2-adiska representation. Vi såg att $-1 = 1 + 2 + 4 + \ldots$ och uttrycker detta med 2-adisk decimalframställning

$$-1 = \sum_{i=0}^{\infty} 2^i = \ldots 2^2 + 2^1 + 2^0 = \ldots 111.$$

När vi skriver p-adiska tal i text, använder vi subskript för att indikera basen p om det inte framgår på något annat sätt. Dessutom använder vi överstrykning för att beteckna en oändlig repetition av en koefficientsekvens.

Exempel 2.11. Genom att följa algoritmen i Sats 2.6 kan vi hitta den serie som representerar $\frac{2}{3}$ i basen 5.

$$\frac{2}{3} = \ldots 3131314_5 = \ldots \overline{31}4_5.$$

För att sammanfatta det vi gjort hittills så började vi med att introducera p-adiska tal som formella potensserier och visade hur rationella tal kan representeras i det p-adiska talsystemet genom en serie som uppfyller ett specifikt kongruensförhållande. Vidare bekräftade vi att varje koefficient i en p-adisk serie är unik, vilket garanterar att varje rationellt tal har en distinkt p-adisk representation. Vi har även visat att varje rationellt tal faktiskt har en p-adisk representation, vilket utvidgar tillämpbarheten av det p-adiska talsystemet till att omfatta alla rationella tal, och därmed alla heltal. Slutligen har vi infört en effektiv notation för att uttrycka dessa p-adiska tal.

2.3 Grundläggande p-adisk aritmetik

Vi vänder oss nu mot de grundläggande aritmetiska operationerna som addition och multiplikation.

2.4 Addition av p-adiska serier

För att addera två p-adiska tal, som båda kan representeras av serier:

$$\sum_{i \geq n_0} a_i p^i \text{ och } \sum_{i \geq n_0} b_i p^i,$$

där $0 \leq a_i, b_i < p$ adderar vi motsvarande koefficienter a_i och b_i för varje i. Om summan av $a_i + b_i$ är lika med eller större än p, utförs en 'överföring' till nästa högre potens av p. I följande beräkning tillåter vi tillfälligtvis koefficienter större än p för att visa hur det fungerar.

Exempel 2.12. För att illustrera addition kan vi återigen betrakta $-1 = \ldots 111_2$ och addera det med $1 = \ldots 001_2$. Utför vi additionen steg för steg, får vi först

$$\begin{aligned} &\ldots 11111 \\ +\ &\underline{\ldots 00001} \\ &\ldots 11112 \end{aligned}$$

I det 2-adiska systemet innebär detta att

$$\begin{aligned} &\ldots 11112 = \ldots 11120 = \ldots 11200 \\ = \quad &\ldots 12000 = \ldots 20000 = \ldots 00000 = 0. \end{aligned}$$

Varje steg i denna addition representerar överföringen som sker när summan når eller överstiger basen, i det här fallet 2.

2.5 Multiplikation av p-adiska serier

I multiplikation av p-adiska tal multipliceras termerna på ett sätt som är anpassat för p-adiska serier. För två p-adiska serier

$$\sum_{i=0}^{\infty} a_i p^i \text{ och } \sum_{i=0}^{\infty} b_i p^i,$$

utförs multiplikation term för term enligt

$$a_0 b_0 p^0 + (a_0 b_1 + a_1 b_0)\, p^1 + (a_0 b_2 + a_1 b_1 + a_2 b_0)\, p^2 \ldots$$

I varje steg kan summan av produkterna resultera i en koefficient större än eller lika med p, vilket kräver en överföring till högre ordningstermer. För det allmänna fallet har vi att

$$\left(\sum_{i \geq n_0} a_i p^i \right) \left(\sum_{i \geq n_0} b_i p^i \right) = \sum_{i \geq 2n_0} c_i p^i$$

där koefficienterna ges av

$$c_i = \sum_{i_1 + i_2 = i} a_{i_1} b_{i_2}.$$

När summan c_i för ett visst index i överskrider p, sker en överföring. Vi kommer, i senare kapitel, återkomma till de andra grundläggande aritmetiska operationerna.

3 Kvadraträtter och kongruenslösningar

De så kallade p-adiska heltalen, betecknade som $\mathbb{Z}_p$, är en delring av $\mathbb{Q}_p$. Dessa tal representeras av p-adiska serier utan negativa potenser av p, vilket innebär att ett p-adiskt heltal kan uttryckas som

$$x = \sum_{i=0}^{\infty} a_i p^i.$$

3.1 Kvadraträtter i $\mathbb{Z}_p$

I detta avsnitt studerar vi kvadraträtter i $\mathbb{Z}_p$. Vi undersöker om det för ett givet heltal $y \in \mathbb{Z}$, som inte är delbart med p, har en kvadratrot $x \in \mathbb{Z}_p$ så att $x^2 = y$. För att närma oss problemet betraktar vi x i dess p-adiska utveckling

$$x = \sum_{i=0}^{\infty} a_i p^i,$$

och fokuserar på partialsumman $\alpha_n = \sum_{i=0}^{n} a_i p^i$ för olika värden på n. Det vi förväntar oss är att

$$\alpha_n^2 \equiv y \pmod{p^{n+1}}.$$

En nödvändig förutsättning för existensen av en kvadratrot i $\mathbb{Z}_p$ är att den initiala kongruensen $\alpha_0^2 \equiv y \pmod{p}$ måste ha en lösning. Denna kongruens är avgörande eftersom den första termen α_0 lägger grunden för hela serien. Om α_0 inte kan kvadreras till $y \pmod{p}$, finns ingen p-adisk serie som kvadreras till y. Följande exempel illustrerar detta.

Exempel 3.1. Vi undersöker förekomsten av kvadraträtter till 2 i $\mathbb{Z}_3$ genom att försöka lösa kongruensen $\alpha_0^2 \equiv 2 \pmod{3}$, för att se om det finns ett $x \in \mathbb{Z}_3$ så att $x^2 = 2$. Vi observerar att inget värde är kongruent med $2 \pmod{3}$ och konstaterar att $\sqrt{2} \notin \mathbb{Q}_3$.

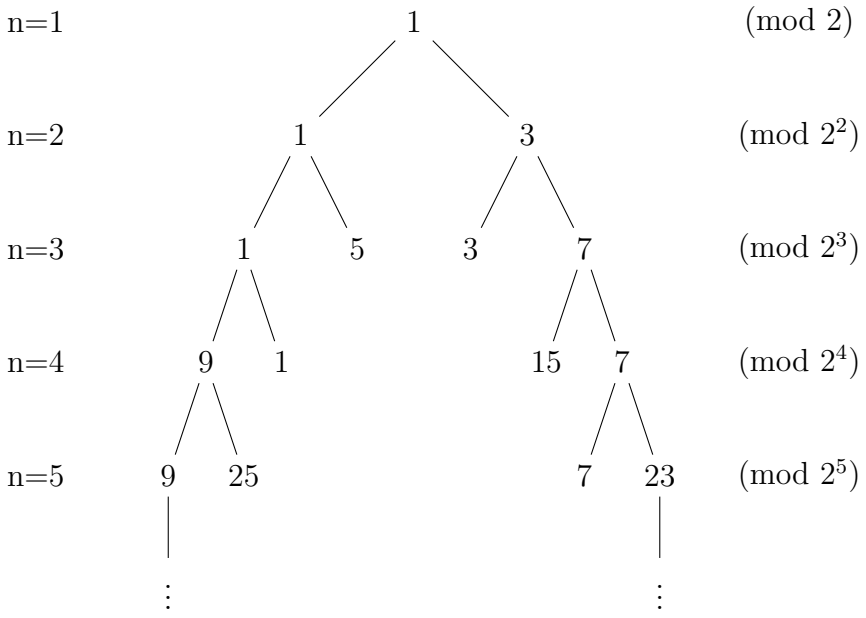
3.2 Utforskande exempel

Nu undersöks hur lösningar till en kvadratisk kongruens kan variera och utvecklas när vi ökar vår modul p^n.

Exempel 3.2. Betrakta ekvationen

$$x^2 \equiv 81 \qquad \pmod{2^n}.$$

För att visualisera lösningarna använder vi ett träd. Varje nod är en specifik lösning till kongruensen för ett visst n. Nodernas förgrening illustrerar hur lösningar utvecklas och 'lyfter' till högre moduler 2^{n+1}.



Figur 1: Lösningar till $x^2 \equiv 81 \pmod{2^n}$

Vi ser att även om vissa lösningar till kongruensen fungerar på en nivå n, kanske den inte lyfts till nästa nivå $n+1$. Det är här begreppet *koherenta sekvenser* blir viktigt.

Definition 3.3. Låt p vara ett primtal. En följd av heltal $\alpha_1, \alpha_2, \alpha_3, \ldots$ kallas för *koherent* om följande villkor är uppfyllda:

1. Varje element α_n i sekvensen uppfyller $0 \leq \alpha_n \leq p^n - 1$.
2. För varje $n \geq 1$, gäller att $\alpha_{n+1} \equiv \alpha_n \mod p^n$.

Då kommer vi att referera till sekvensen som p-adiskt koherent.

Vi visar hur man kan systematisera lösningarna till kongruensekvationer som de i Exempel 3.2 med följande sats.

Sats 3.4. *Låt $a \neq 0$ vara ett heltal, p vara ett primtal och n vara ett positivt heltal. Antag att $a = p^k b$, där $b, k \in \mathbb{Z}$ och $p \nmid b$. Då gäller följande för kongruensekvationen*

$$x^2 \equiv a^2 \pmod{p^n} :$$

i) Om $p \neq 2$ och $n > 2k$, är lösningarna till kongruensekvationen givna av

$$x \equiv \pm a \pmod{p^{n-k}}.$$

ii) Om $p = 2$ och $n > 2k + 3$, är lösningarna till kongruensekvationen givna av

$$x \equiv \pm a \pmod{p^{n-k-1}}.$$

Bevis. Beviset kommer att delas upp i tre delar. Antag inledningsvis att $p \neq 2$ och $p \nmid a$, så $k = 0$ och betraktar först fallet då $n = 1$. Vi kommer att visa att under dessa förutsättningar gäller $x \equiv \pm a \pmod{p^n}$ om $x \equiv \pm a \pmod{p}$ då $k < 1$.

Antag att $x \equiv a \pmod{p}$. Detta innebär att $p \mid x - a$. Vi betraktar nu kongruensekvationen

$$(x + a)(x - a) \equiv 0 \pmod{p^n}.$$

Detta medför att p^n måste vara en delare till antigen $x + a$ eller $x - a$, eller båda. Eftersom $x + a \equiv 2a \not\equiv 0 \pmod{p}$, måste p^n dela $x - a$. Därmed får vi

$$x \equiv a \pmod{p^n}.$$

Antag nu istället att $x \equiv -a \pmod{p}$. Detta innebär att $p \mid x + a$. Eftersom $x - a \equiv -2a \not\equiv 0 \pmod{p}$, måste p^n dela $x + a$. Därmed får vi

$$x \equiv -a \pmod{p^n}.$$

Vi har därmed visat *i)* i fallet då $k = 0$.

Vi antar nu att $p \neq 2$ men att $p \mid a$, så $k > 0$. Vi kommer nu att visa att under dessa förutsättningar gäller $x \equiv \pm a \pmod{p^{n-k}}$ om $n > 2k$.

Vi betraktar kongruensekvationen

$$x^2 \equiv p^{2k} b^2 \pmod{p^n}.$$

Detta innebär att $p^n \mid x^2 - p^{2k} b^2$. Eftersom $n > 2k$, får vi att $p^{2k} \mid x^2 - p^{2k} b^2$, vilket ger $p^k \mid x$ då p^{2k} uppenbarligen delar $-p^{2k} b^2$. Låt nu $x = p^k y$. detta leder till att

$$x^2 \equiv a^2 \pmod{p^n} \Leftrightarrow p^{2k} y^2 \equiv p^{2k} b^2 \pmod{p^n},$$

vilket förenklas till

$$y^2 \equiv b^2 \pmod{p^{n-2k}}.$$

Detta ger, enligt det första fallet, att $y \equiv \pm b \pmod{p^{n-2k}}$. Vi kan nu multiplicera båda sidor med p^k,

$$p^k y \equiv \pm p^k b \pmod{p^{n-k}}.$$

Eftersom $p^k y = x$ och $p^k b = a$, får vi att

$$x \equiv \pm a \pmod{p^{n-k}}.$$

Avslutningsvis antar vi att $p = 2$. Vi kommer nu att visa att under dessa förutsättningar gäller $x \equiv \pm a \pmod{p^{n-k-1}}$ om $n > 2k + 3$.

Låt här $a = 2^k b$ och $2 \nmid b$. Vi betraktar kongruensekvationen

$$x^2 \equiv 2^{2k} b^2 \pmod{2^n}.$$

Vi låter nu $x = 2^k y \Leftrightarrow y = x/2^k$ och förkortar med 2^{2k}, för att sedan substituera in y. Då fås

$$y^2 \equiv b^2 \pmod{2^{n-2k}}.$$

Eftersom b är udda, är b^2 udda. Därmed blir det naturligt att att betrakta $y^2 \equiv b^2 \pmod 4$. Vi har då att $y \equiv \pm b + 4s$, för något heltal s. Följaktligen får vi att

$$y^2 \equiv b^2 \pmod{2^{n-2k}} \Leftrightarrow b^2 \pm 8bs + 16s^2 \equiv b^2 \pmod{2^{n-2k}},$$

vilket efter förenkling blir

$$s(b + 2s) \equiv 0 \pmod{2^{n-2k-3}}.$$

Detta går att uttrycka som $2^{n-2k-3} \mid s(b + 2s)$. Uttrycket innanför parentesen är udda. Alltså kan vi säga $s = 2^{n-2k-3} m$, för något heltal m. Efter insättning i antagandet att $y \equiv \pm b + 4s$ får vi att $y = \pm b + 2^{n-2k-1} m$, vilket efter en sista insättning i $x = 2^k y$ ger att

$$x = \pm 2^k b + 2^{n-k-1} m$$

Vi vet sedan tidigare att $a = 2^k b$, vilket innebär att

$$x = \pm a + 2^{n-k-1} m.$$

Detta medför att

$$x = \pm a \pmod{2^{n-k-1}}.$$

□

Med denna sats uppenbaras det att det endast finns två unika koherenta sekvenser som löser kongruensekvationen $x^2 \equiv a^2 \pmod{p^n}$. Vi återvänder nu till Exempel 3.2 med kongruensen $x^2 \equiv 81 \pmod{2^n}$ som illustrerats i figur (1), för att tillämpa vår förståelse av koherenta sekvenser.

Exempel 3.5. Genom att analysera trädet av lösningar kan vi identifiera vilka lösningar som 'lyfts' till högre nivåer. Dessa sekvenser är

$$x_1 = (1, 1, 1, 9, 9, \dots),$$
$$x_2 = (1, 3, 7, 7, 23 \dots).$$

För varje element i en koherent sekvens är den p-adiska utvecklingen en trunkering av nästkommande element. Till exempel, för sekvensen x_2:

$$\begin{aligned} 1 =& 1 \\ 3 =& 1 + 1 \cdot 2 \\ 7 =& 1 + 1 \cdot 2 + \ 1 \cdot 2^2 \\ & \vdots \end{aligned}$$

Detta bygger upp det 2-adiska talet

$$1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 \cdots = \ldots \bar{1}0111_2,$$

där varje steg i sekvensen representerar en trunkering av den fullständiga 2-adiska utvecklingen av -9.

3.3 Icke-rationella p-adiska kvadratrötter

I tidigare exempel har vi sett hur specifika kvadratrötter kan 'lyftas'. Vi utvidgar nu denna diskussion till att omfatta en bredare kategori av tal och undersöka under vilka förhållanden kvadratrötter existerar i $\mathbb{Z}_p$.

Sats 3.6. *Antag att p är ett primtal sådant att $p \neq 2$ och $p \nmid m$. Om kongruensekvationen*

$$x^2 \equiv m \pmod{p},$$

har en lösning, betecknad som α_1, kan α_1 utvidgas till en koherent följd $\alpha_1, \alpha_2, \alpha_3, \ldots$ av lösningar

$$\alpha_n^2 \equiv m \pmod{p^n},$$

för alla heltal $n \geq 1$.

Bevis. Givet en lösning $x = \alpha_n$ till

$$x^2 \equiv m \pmod{p^n}, \tag{3.7}$$

vill vi hitta en lösning $x = \alpha_{n+1}$ till

$$x^2 \equiv m \pmod{p^{n+1}}.$$

Betrakta $\alpha_{n+1} = \alpha_n + p^n k$, för något heltal k. Vi kvadrerar α_{n+1} och ser då att

$$\alpha_n^2 + 2\alpha_n p^n k + p^{2n} k \equiv m \pmod{p^{n+1}}.$$

Eftersom $2n \geq n + 1$ kan vi säga att

$$\begin{aligned} &\alpha_n^2 + 2\alpha_n p^n k \equiv m \pmod{p^{n+1}} \\ &\Leftrightarrow 2\alpha_n p^n k \equiv m - \alpha_n^2 \pmod{p^{n+1}}. \end{aligned}$$

Vi vet från (3.7) att $m - \alpha_n^2 = s \cdot p^n$, för något heltal s. Detta ger att

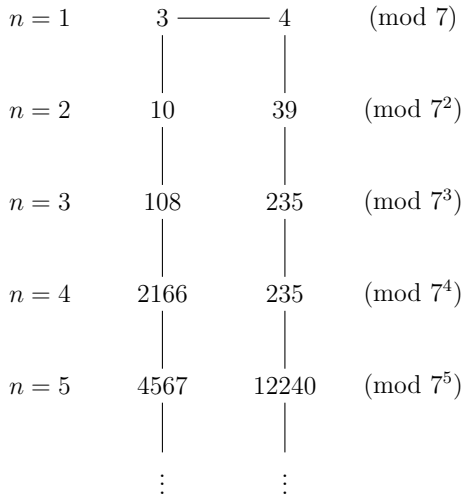
$$\begin{aligned} &2\alpha_n p^n k \equiv sp^n \pmod{p^{n+1}} \\ &\Leftrightarrow 2\alpha_n k \equiv s \pmod{p}. \end{aligned} \tag{3.8}$$

Nu, eftersom $2\alpha_n \not\equiv 0 \pmod{p}$, existerar ett unikt k, där $0 \leq k \leq p-1$ som löser (3.8). Detta ger ett unikt α_{n+1} som uppfyller

$$\begin{aligned} \alpha_{n+1}^2 &\equiv m \pmod{p^n}, \\ \alpha_{n+1} &\equiv \alpha_n \pmod{p^n}, \end{aligned}$$

där $0 \leq \alpha_{n+1} < p^{n+1}$. Sammanfattningsvis har vi visat att om $x^2 \equiv m \pmod{p}$ har en lösning α, då kan denna lösning utvidgas till en koherent följd av lösningar α_n till $x^2 \equiv m \pmod{p^n}$ för alla heltal n. □

Exempel 3.9. Betrakta ekvationen $x^2 = 2$, som saknar lösningar i $\mathbb{Q}$. Däremot kan en koherent följd av lösningar till kongruensekvationen $x^2 = 2 \pmod{7^n}$ ge en 7-adisk lösning till $x^2 = 2$. Vi hittar de koherenta sekvenserna som illustreras med följande figur.



Figur 2: Lösningar till $x^2 \equiv 2 \pmod{7^n}$

Genom att utforska dessa lösningar i exemplet ovan upptäcker vi att vissa tal, som $\pm\sqrt{2}$ i $\mathbb{Q}_7$, inte kan representeras som rationella tal. Detta visar att det p-adiska talsystemet kan representera vissa tal som inte finns i det traditionella talsystemet $\mathbb{Q}$.

4 Valueringar och absolutbelopp

Det första steget för en mer formell konstruktion av $\mathbb{Q}_p$ är att introducera så kallade p-adiska valueringar.

Definition 4.1. Fixera ett primtal $p \in \mathbb{Z}$. Den p-adiska valueringen på $\mathbb{Z}$ är funktionen

$$v_p : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{R}$$

definierad enligt följande: för varje heltal $n \in \mathbb{Z}, n \neq 0$, låt $v_p(n)$ vara det unika positiva heltalet som uppfyller

$$n = p^{v_p(n)} n' \quad \text{där} \quad n' \in \mathbb{Z} \text{ och } p \nmid n'.$$

Nu utvidgas v_p till kroppen av rationella tal enligt följande. Om $x = \frac{a}{b} \in \mathbb{Q} \setminus \{0\}$, så sätter vi

$$v_p(x) = v_p(a) - v_p(b).$$

Om $x = 0$, så säger vi $v_p(0) = +\infty$

Informellt betyder detta att $v_p(n)$ kan tolkas som multipliciteten av p som en divisor av n. Detta koncept illustreras i exemplet nedan.

Exempel 4.2. Här beräknas valueringen av två heltal och ett rationellt tal:

$$\begin{aligned} &v_5(400) = 5^2 \cdot 16 = 2, \\ &v_2(11) = 0, \\ &v_5\left(\frac{-13}{25}\right) = v_5(-13) - v_5(25) = 0 - 2 = -2. \end{aligned}$$

Följande sats belyser grundläggande egenskaper för den p-adiska valueringen.

Sats 4.3. *För alla x och y i $\mathbb{Q}$, gäller*

i) $v_p(x \cdot y) = v_p(x) + v_p(y)$

ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$

Beviset är inspirerat av tekniker och metoder som presenterats i [7]. Vi börjar med att betrakta $x, y \in \mathbb{Z}$, vi kan anta att $x, y \neq 0$ eftersom $v_p(0)$ är satt till $+\infty$. Skriv $x = p^m x'$ och $y = p^n y'$, där $p \nmid x', y'$. Här noterar vi att $m = v_p(x)$ och $n = v_p(y)$. Vi kan anta att $m \leq n$ utan förlust av generalitet. Då får vi att

$$xy = p^{m+n}x'y', \quad \text{så} \quad v_p(x \cdot y) = m + n = v_p(x) + v_p(y).$$

Detta bevisar del *i)*. För del *ii)* observerar vi att

$$x + y = p^m x' + p^n y' = p^m(x' + p^{n-m}y'),$$

vilket ger

$$v_p(x + y) = m + v_p(x' + p^{n-m}y') \geq m.$$

Detta resultat är giltigt eftersom $v_p(x' + p^{n-m}y') \geq 0$, vilket följer av antagandet att $m \leq n$. Detta fullföljer beviset för heltal.

Nu låter vi $x, y \in \mathbb{Q}$ och skriver $x = \frac{a}{b}$ och $y = \frac{c}{d}$. För del *i)* har vi

$$v_p(x \cdot y) = v_p\left(\frac{ac}{bd}\right) = v_p(a) + v_p(c) - v_p(b) - v_p(d) = v_p\left(\frac{a}{b}\right) + v_p\left(\frac{c}{d}\right).$$

För del *ii)* betraktar vi $v_p(x + y)$. Vi har

$$x + y = \frac{ad + bc}{bd}.$$

Då blir $v_p(x + y) = v_p(a \cdot d + b \cdot c) - v_p(b \cdot d)$.

Notera att $v_p(a \cdot d + b \cdot c) \geq \min\{v_p(a \cdot d), v_p(b \cdot c)\}$ enligt Sats 4.3 del *ii)*. Detta ger oss

$$v_p(x + y) \geq \min\{v_p(a \cdot d), v_p(b \cdot c)\} - v_p(b \cdot d).$$

Eftersom $v_p(a \cdot d) = v_p(a) + v_p(d)$ och $v_p(b \cdot c) = v_p(b) + v_p(c)$, kan vi skriva om detta som

$$v_p(x + y) \geq \min\{v_p(a) + v_p(d), v_p(b) + v_p(c)\} - (v_p(b) + v_p(d)).$$

Förenkla detta ytterligare för att få

$$v_p(x + y) \geq \min\{v_p(a) - v_p(b), v_p(c) - v_p(d)\},$$

vilket är detsamma som

$$v_p(x + y) \geq \min\{v_p(x), v_p(y)\}.$$

□

4.1 Från valuering till det p-adiska absolutbeloppet

Vi fokuserar nu på kroppen av rationella tal $\mathbb{Q}$ och låter $\mathbb{Q}_+ = \{x \in \mathbb{Q} : x \geq 0\}$. Ett absolutbelopp bör ge en uppfattning om storleken på ett element i kroppen $\mathbb{Q}$.

Definition 4.4. En absolutvärdesfunktion $|\cdot|$ på kroppen $\mathbb{Q}$ är en funktion

$$|\cdot| : \mathbb{Q} \to \mathbb{Q}_+$$

som uppfyller följande egenskaper:

i Nollpunkt: $|x| = 0$ om och endast om $x = 0$.

ii Multiplikativitet: $|x \cdot y| = |x| \cdot |y|$ för alla $x, y \in \mathbb{Q}$.

iii Triangelolikheten: $|x + y| \leq |x| + |y|$ för alla $x, y \in \mathbb{Q}$.

Ett absolutvärde som uppfyller dessa villkor kallas för ett arkimediskt absolutvärde.

Definition 4.5. Ett absolutvärde $|\cdot|$ på kroppen $\mathbb{Q}$ sägs vara icke-arkimediskt om det, förutom att vara en absolutvärdesfunktion enligt Definition 4.4, även uppfyller det icke-arkimediska villkoret:

$$|x + y| \leq \max\{|x|, |y|\}, \quad \text{för alla } x, y \in \mathbb{Q}.$$

Det visar sig att den p-adiska valueringen $v_p(x)$ kan användas för att skapa ett nytt slags absolutbelopp på $\mathbb{Q}$. Denna möjlighet stöds av de likheter som finns mellan de egenskaper i Sats 4.3, och de kriterier som anges i Definition 4.4. Särskilt relevant är villkor *ii)* och det icke-arkimediska kriteriet 4.5, vilka båda uppvisar en likhet med egenskaperna hos v_p.

Definition 4.6. För varje $x \in \mathbb{Q}$, definierar vi det p-adiska absolutbeloppet av x som

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

om $x \neq 0$, och vi sätter $|0|_p = 0$.

Bevis. Vi vill visa att det p-adiska absolutbeloppet uppfyller egenskaperna i Definition 4.4 och 4.5.

Inledningsvis vill vi visa att $|x|_p = 0$ om och endast om $x = 0$, dvs nollpunkten. Om $x = 0$ är $v_p(0) = +\infty$ och formeln $p^{-v_p(0)}$ ska tolkas som $|0|_p = p^{-\infty} = 0$. Om $x \neq 0$ är $v_p(x)$ ett ändligt tal, så $|x|_p = p^{-v_p(x)} \neq 0$.

Nu vill vi visa multiplikativiteten. För $x, y \in \mathbb{Q}$ är $v_p(x \cdot y) = v_p(x) + v_p(y)$. Därför blir $|x \cdot y|_p = p^{-v_p(x \cdot y)} = p^{-(v_p(x)+v_p(y))} = |x|_p + |y|_p$.

För det icke-arkimediska villkoret antar vi att $v_p(x) \leq v_p(y)$. Då har vi att $x+y$ är minst lika delbart med p som x, vilket betyder att $v_p(x + y) \geq v_p(x)$. Således är $|x + y|_p = p^{-v_p(x+y)} = \max\{|x|_p, |y|_p\}$.

□

Observera att vår definition av $v_p(0) = +\infty$, stämmer överens med definitionen av p-adiskt absolutbelopp då, formellt, $|0|_p = p^{-v_p(0)} = p^{-\infty} = 0$. En egenskap detta nydefinierade absolutbeloppet har är att det är icke-arkimediskt, vilket väldigt kortfattat innebär att dess egenskaper är ointuitiva.

Exempel 4.7. Betrakta några exempel på p-adiska absolutbelopp:

$$|35|_7 = 1,$$

$$\left|\tfrac{56}{12}\right|_7 = \left|\tfrac{14}{3}\right|_7 = 7^{-(1-0)} = 7^{-1}.$$

4.2 Ostrowskis sats

Efter att ha utforskat p-adiska absolutbelopp ska vi nu översiktligt undersöka relationen mellan olika absolutbelopp, vilket leder oss till följande sats.

Definition 4.8. Två absolutbelopp $|\cdot|_1$ och $|\cdot|_2$ på $\mathbb{Q}$ kallas ekvivalenta om de ger samma topologi, vilket informellt innebär att de ger samma uppfattning om konvergens i $\mathbb{Q}$.

Innan vi går in på Ostrowskis sats definieras det traditionella, arkimediska absolutbeloppet, betecknat $|\cdot|_\infty$ som är det vanliga absolutbeloppet på $\mathbb{Q}$ vi sedan tidigare är bekanta med från studier av de reella talen $\mathbb{R}$. Med detta i åtanke, utan att fördjupa oss i det tekniska, introduceras nu Ostrowskis sats.

Sats 4.9 (**Ostrowskis sats**)**.** *Varje icke-trivialt absolutbelopp på $\mathbb{Q}$ är ekvivalent med ett av absolutbeloppen $|\cdot|_p$ där p är ett primtal eller $p = \infty$.*

Beviset är komplicerat, men finns i [1, s.46-s.49].

Ostrowskis sats fastställer att alla icke-triviala absolutbelopp på $\mathbb{Q}$ är ekvivalenta antigen med det vanliga absolutbeloppet, associerat med det reella talen ($p = \infty$), eller med ett p-adiska absolutbelopp, associerat med $\mathbb{Q}_p$. Poängen är att trots möjligheten av andra absolutbelopp, leder de alla till samma typer av kompletterande strukturer: $\mathbb{Q}_p$ respektive $\mathbb{R}$.

Detta leder oss till produktformeln, som uttrycker en relation mellan dessa absolutbelopp. Den säger att produkten av absolutbeloppen av ett rationellt tal skilt från noll över alla primtal och ∞ är lika med 1.

Sats 4.10 (Produktformeln)**.** *För alla $x \in \mathbb{Q} \setminus \{0\}$, har vi*

$$\prod_{p \leq \infty} |x|_p = 1,$$

där $p \leq \infty$ innebär att vi tar produkten över alla primtal i $\mathbb{Q}$ inklusive 'primtalet vid oändligheten'.

Bevis. Vi börjar med att bevisa satsen för positiva heltal, det generella fallet kommer då att följa som en generalisering. Låt x vara ett positivt heltal, som kan faktoriseras som $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. Då har vi

$$\begin{cases} |x|_q = 1 & \text{om } q \neq p_i \text{ för alla } i = 1, 2, 3, \ldots, k \\ |x|_{p_i} = p_i^{-a_i} & \\ |x|_\infty = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} & \end{cases}.$$

Betrakta nu produkten över alla $p \leq \infty$

$$\prod_{p \leq \infty} |x|_p = 1 \times \left(p_1^{-a_1} \cdot p_2^{-a_2} \cdots p_k^{-a_k}\right) \times (p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}) = 1.$$

För rationella tal $x = \frac{a}{b}$, där a och b är positiva heltal, följer det generella fallet genom att betrakta $|a|_p$ och $|b|_p$ separat och använda egenskapen $|x|_p = |a|_p / |b|_p$.

$$\prod_{p \leq \infty} \left|\frac{a}{b}\right|_p = \prod_{p \leq \infty} |a|_p \quad / \quad \prod_{p \leq \infty} |b|_p = \frac{1}{1} = 1.$$

Detta bevis finns delvis i [1, s.49]. □

Exempel 4.11. Betrakta $x = \frac{12}{5} = \frac{2^2 \cdot 3^1}{5^1}$. Vi har då att $|x|_2 = 2^{-2}$, $|x|_3 = 3^{-1}$, $|x|_5 = 5^1$ och $|x|_\infty = \frac{12}{5}$. Multiplicera dessa enligt

$$\prod_{p \leq \infty} |x|_p = 2^{-2} \times 3^{-1} \times 5^1 \times \frac{12}{5} = 1.$$

En intressant aspekt av produktformeln är att om vi känner till alla absolutbelopp för ett specifikt tal $x \in \mathbb{Q}$, förutom ett, kan det saknade absolutbeloppet bestämmas utifrån de andra.

5 Formell konstruktion av $\mathbb{Q}_p$

I detta avsnitt kommer vi skissa en mer formell konstruktion av de p-adiska talen $\mathbb{Q}_p$. Vårt mål är att ge en grundläggande förståelse av $\mathbb{Q}_p$ och att presentera det på ett tillgängligt sätt, utan att djupgående gå igenom alla detaljer i deras konstruktion. Läsaren hänvisas till [1, s.43-59] för en fullständig genomgång.

Definition 5.1. Låt K vara en kropp och $|\cdot|$ vara ett absolutbelopp på K. Vi definierar avståndet $d(x, y)$ mellan två element $x, y \in K$ genom

$$d(x, y) = |x - y|.$$

Mängden K på vilken denna metrik $d(x, y)$ är definierad på kallas för ett metriskt rum och betecknas (K, d).

Exempel 5.2. Betrakta det 7-adiska avståndet $d(x, y) = |x - y|_7$ på $\mathbb{Q}$. Vi har

$$d(28814, 2) = |28812|_7 = 7^{-4},$$

$$d(3, 2) = |1|_7 = 7^0 = 1.$$

Trots att 28814 och 2 kan verka långt ifrån varande i det traditionella decimala systemet, är deras 7-adiska avstånd mindre än avståndet mellan de närliggande talen 3 och 2. Detta illustrerar hur p-adiska avstånd minskar när avståndet mellan två tal innehåller faktorer av större potenser av p. Detta är en unik egenskap som ibland kan vara både oväntad och förvirrande.

Efter att vi har bekantat oss om metriska rum, är nästa steg att förstå hur följder beter sig i dessa rum. Här kommer Cauchy-följder in i bilden.

Definition 5.3 (Cauchy-följd)**.** Antag att (K, d) är ett metriskt rum och att $(a_n) = (a_1, a_2, \dots)$ är en följd i K. Följden (a_n) kallas för en Cauchy-följd om det, för varje positivt reellt tal $\varepsilon > 0$, finns ett positivt heltal N så att för alla $m, n > N$, följande villkor är uppfyllt:

$$d(a_m, a_n) = |a_m - a_n| < \varepsilon.$$

Cauchy-följder ger oss ett sätt att definiera $\mathbb{Q}_p$ som en förlängning av $\mathbb{Q}$.

Lemma 5.4. *En följd (x_x) av rationella tal är en Cauchy-följd med avseende på ett icke-arkimediskt absolutbelopp $|\cdot|_p$ om och endast om vi har*

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0.$$

Bevis. Följande bevis finns i [1, s.51]. Om $m = n + r > n$, får vi

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \cdots + x_{n+1} - x_n| \\ &\leq \max\left\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \dots, |x_{n+1} - x_n|\right\}, \end{aligned}$$

eftersom absolutbeloppet är icke-arkimediskt. Resultatet följer ur detta. □

Exempel 5.5 (Icke-arkimediskt)*.* För att illustrera att Lemma 5.4 fungerar för icke-arkimediska men inte arkimediska absolutbelopp kan vi betrakta det 2-adiska absolutbeloppet $|\cdot|_2$ och följden (a_n) där $a_n = 2^n$ och n är ett positivt heltal. Vi ser att $|2^{n+1} - 2^n|_2 = |2^n|_2 = 2^{-n}$. Eftersom $2^{-n} \to 0$ då $n \to \infty$, innebär detta att (a_n) är en Cauchy-följd enligt lemmat.

Exempel 5.6 (Arkimediskt motexempel)*.* Betrakta istället den reella följden (a_n) där $a_n = \sqrt{n}$. Även om avståndet mellan två på varandra följande element $|\sqrt{n+1} - \sqrt{n}| \to 0$ när $n \to \infty$, blir inte $\sqrt{n} - \sqrt{m}$ godtyckligt litet för stora n, m. Alltså är detta inte en Cauchy-följd i arkimedisk kontext.

Nu kan vi börja utforska konstruktionen av $\mathbb{Q}_p$.

Sats 5.7. *Låt (x_n) och (y_n) vara två Cauchy-följder av rationella tal. vi definierar addition och multiplikation för dessa följder enligt:*

$$(x_n) + (y_n) = (x_n + y_n),$$

$$(x_n) \cdot (y_n) = (x_n y_n).$$

Dessa operationer av addition och multiplikation ger upphov till nya Cauchy-följder och skapar en kommutativ ring.

Bevis. För att visa att (x_n+y_n) är en Cauchy-följd, måste vi visa att för varje $\varepsilon > 0$ finns det ett positivt N så att för alla $m, n > N$ så gäller $|x_n+y_n-(x_m+y_m)| < \varepsilon$. Vi låter $\varepsilon > 0$. Eftersom (x_n) är en Cauchy-följd existerar ett heltal N_1 så att för alla $m, n > N_1$ gäller $|x_n - x_m| < \varepsilon$. På samma sätt, eftersom (y_n) är en Cauchy-följd, existerar det ett heltal N_2 så att för alla $m, n > N_2$ gäller $|y_n - y_m| < \varepsilon$. Låt $N = \max\{N_1, N_2\}$. För alla $m, n > N$ gäller det enligt det icke-arkimediska villkoret (4.5) att

$$|(x_n - x_m) + (y_n - y_m)| \leq \max\{|x_n - x_m|, |y_n - y_m|\} < \max\{\varepsilon, \varepsilon\} = \varepsilon.$$

För att visa att $(x_n \cdot y_n)$ är en Cauchy-följd, vill vi istället visa att för varje $\varepsilon > 0$ finns det ett positivt heltal N så att för alla $m, n > N$ så gäller $|x_n y_n - x_m y_n| < \varepsilon$. Låt $\varepsilon > 0$. Eftersom (x_n) och (y_n) är Cauchy-följder är de också begränsade, alltså finns det ett positivt tal M så att $|x_n|, |y_n| < M$ för alla n. Då (x_n) är en Cauchy-följd finns det ett heltal N_1 så att $|x_n - x_m| < \varepsilon/(2M)$ för alla $m, n > N_1$. På samma sätt finns det för (y_n) ett heltal N_2 så att $|y_n - y_m| < \varepsilon/(2M)$. Vi låter nu $N = \max\{N_1, N_2\}$. För alla $m, n > N$ gäller det enligt det icke-arkimediska villkoret (4.5) att

$$|x_n(y_n - y_m) + y_m(x_n - x_m)| \leq \max\{|x_n||y_n - y_m|, |y_m||x_n - x_m|\}.$$

Eftersom $|x_n|, |y_m| < M$ för alla m, n får vi att

$$\max\{|x_n||y_n - y_m|, |y_m||x_n - x_m|\} < \max\{M \cdot \varepsilon/(2M), M \cdot \varepsilon/(2M)\} = \varepsilon$$

Då $|x_n y_n - x_m y_m| < \varepsilon$ för alla $m, n > N$, är $(x_n \cdot y_n)$ en Cauchy-följd. □

Vi har etablerat att vi kan addera och multiplicera Cauchy-följder, och att resultatet också är en Cauchy-följd. Nu definieras när två sådana följder anses vara ekvivalenta under det p-adiska absolutbeloppet.

Definition 5.8. Två Cauchy-följder (x_n) och (y_n) sägs vara ekvivalenta med avseende på ett icke-arkimediskt absolutbelopp $|\cdot|_p$ om

$$\lim_{n\to\infty} |x_n - y_n|_p = 0.$$

Differensen mellan motsvarade termer i de två följderna blir obetydlig då n går mot oändligheten i termer av det icke-arkimediska absolutbeloppet.

Två följder som ekvivalenta på detta sätt representerar samma p-adiska tal.

Definition 5.9. Kroppen $\mathbb{Q}_p$ av p-adiska tal definieras som mängden av alla ekvivalensklasser av Cauchy-följder av rationella tal med avseende på det icke-arkimediska absolutbeloppet $|\cdot|_p$. Varje ekvivalensklass i denna mängd representerar ett unikt p-adiskt tal.

Med definitionen ovan tar vi steget från att tänkta på p-adiska tal som enskilda följder av rationella tal till att se dem som hela klasser av följder. Varje ekvivalensklass innehåller alla Cauchy-följder som med hänsyn till det icke-arkimediska absolutbeloppet anses vara ekvivalenta.

Definition 5.10. Om $\lambda \in \mathbb{Q}_p$ är ett element i $\mathbb{Q}_p$, och (x_n) är en Cauchy-följd som representerar λ, definierar vi absolutbeloppet av λ som

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p.$$

(vi har definierat $\mathbb{Q}_p$ så att elementen i $\mathbb{Q}_p$ är ekvivalensklasser av Cauchy-följder.)

Varje rationellt tal $x \in \mathbb{Q}$ kan inbäddas i $\mathbb{Q}_p$ som en konstant talföljd, vilket uttrycks som $x \mapsto (x)$. Denna inbäddning länkar direkt till avsnitt 2, där p-adiska tal beskrivs som serier $\sum_{i\geq n_0} a_i p^i$. Varje sådan serie är alltså ett gränsvärde av en Cauchy-följd av rationella tal, där varje partialsumma av serien närmar sig det p-adiska talet. I avsnitt 2.1 undersöks hur $x \in \mathbb{Q}_p$ kan närmas genom dess partialsummor, som i sin tur representerar successiva närmanden av x i p-adiska termer.

Definition 5.11. En följd (x_n) sägs konvergera mot gränsvärdet A i $\mathbb{Q}_p$ om det för varje positivt p-adiskt tal ε_p, finns ett heltal N så att $|x_n - A|_p < \varepsilon_p$ för alla $n \geq N$, vilket uttrycks som

$$\lim_{n\to\infty} x_n = A.$$

Nu, efter ovannämnda definitioner och exempel är vi redo att formalisera $\mathbb{Q}_p$ som en kropp. Vi såg att rationella tal kan representeras som Cauchy-följder i $\mathbb{Q}_p$ och att dessa följder konvergerar mot p-adiska tal. Följande sats är ett centralt resultat om existensen av kroppen $\mathbb{Q}_p$ med det p-adiska absolutbeloppet.

Sats 5.12. *För varje primtal $p \in \mathbb{Z}$ existerar en kropp $\mathbb{Q}_p$ med ett icke-arkimedisk absolutbelopp $|\cdot|_p$ så att*

i) Det existerar en inbäddning $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, och att absolutbeloppet $|\cdot|_p$ på $\mathbb{Q}$ via denna inbäddning är det p-adiska absolutbeloppet.

ii) För varje element i $\mathbb{Q}_p$ finns det en följd av rationella tal från $\mathbb{Q}$, som när de mappas till $\mathbb{Q}_p$ genom inbäddningen, konvergerar mot detta element i $\mathbb{Q}_p$ med avseende på $|\cdot|_p$.

iii) Varje Cauchy-följd av element i $\mathbb{Q}_p$, med avseende på $|\cdot|_p$ konvergerar mot ett element i $\mathbb{Q}_p$.

Fältet $\mathbb{Q}_p$ som uppfyller (i), (ii) och (iii) är unikt upp till en unik isomorfism som bevarar absolutbeloppen.

För fullständigt bevis, se [1].

6 Grundläggande analys i $\mathbb{Q}_p$

Vi har sett hur enskilda följder konvergerar i $\mathbb{Q}_p$. Nästa steg är att utforska hur funktioner beter sig när deras argument närmar sig en specifik punkt. Precis som i det reella fallet definierar vi gränsvärdet för en funktion vid en punkt i $\mathbb{Q}_p$.

Definition 6.1. Låt $f : \mathbb{Q}_p \to \mathbb{Q}_p$ vara en funktion. Vi säger att f har gränsvärdet A i $\mathbb{Q}_p$ när x går mot a, skrivet som

$$\lim_{x \to a} f(x) = A,$$

om det för varje positivt tal $\varepsilon > 0$, finns ett tal $\delta > 0$ så att för alla $x \in \mathbb{Q}_p$ där $0 < |x - a|_p < \delta$, gäller att

$$|f(x) - A|_p < \varepsilon.$$

Skillnaden mellan denna definition och den motsvarande för det reella fallet ligger bara i hur 'avstånd' definieras, vilket helt beror på valet av absolutbelopp.

Slutligen, för att förstå kontinuitet av funktioner i $\mathbb{Q}_p$, anpassar vi den klassiska definitionen av kontinuitet med hänsyn till det p-adiska absolutbeloppet.

Definition 6.2. Låt $f : D \to \mathbb{Q}_p$ vara en funktion där $D \subseteq \mathbb{Q}_p$ och a vara en punkt i definitionsmängden för f. Funktionen f sägs vara kontinuerlig vid punkten a om för varje $\varepsilon > 0$ finns ett $\delta > 0$ så att för alla $x \in D$ som uppfyller $|x - a|_p < \delta$, gäller att $|f(x) - f(a)|_p < \varepsilon$. Med andra ord, f är kontinuerlig vid a om

$$\lim_{x \to a} f(x) = f(a).$$

6.1 Gränsvärdesregler i $\mathbb{Q}_p$

Efter att ha etablerat grunderna för konvergens och kontinuitet i $\mathbb{Q}_p$ är vi nu rustade att ta oss an de grundläggande gränsvärdesreglerna.

Definition 6.3. Låt $f, g : \mathbb{Q}_p \to \mathbb{Q}_p$ vara två funktioner och låt $A, B \in \mathbb{Q}_p$. Om $\lim_{x\to a} f(x) = A$ och $\lim_{x\to a} g(x) = B$ i den p-adiska normen, då gäller att:

- $f(x) + g(x) \to A + B$ när $x \to a$,
- $f(x) \cdot g(x) \to A \cdot B$ när $x \to a$,

Bevis. Låt $\varepsilon > 0$. Enligt gränsvärdesdefinitionen finns det $\delta_1, \delta_2 > 0$ så att för alla $x \in \mathbb{Q}_p$,

$$|x - a|_p < \delta_1 \Rightarrow |f(x) - A|_p < \frac{\varepsilon}{2}$$

och

$$|x - a|_p < \delta_2 \Rightarrow |g(x) - B|_p < \frac{\varepsilon}{2}.$$

Vi låter $\delta = \max\{\delta_1, \delta_2\}$. För alla $|x - a| < \delta$, gäller enligt det icke-arkimediska villkoret att

$$|(f(x)+g(x))-(A+B)|_p = |(f(x)-A)+(g(x)-B)|_p \leq \max\{|f(x)-A|_p, |g(x)-B|_p\} < \varepsilon.$$

Således konvergerar $f(x) + g(x)$ mot $A + B$ när $x \to a$.

För multiplikation, antag att $|f(x) - A|_p < \varepsilon_1$ och $|g(x) - B|_p < \varepsilon_2$ för några $\varepsilon_1, \varepsilon_2 > 0$. Vi har

$$|f(x)g(x) - AB|_p = |f(x)(g(x) - B) + B(f(x) - A)|_p.$$

Eftersom $|f(x)|_p \leq \max(|f(x) - A|_p, |A|_p)$ kan vi anta att $|f(x)|_p$ är begränsad av någon konstant M för x nära a. Så vi får

$$|f(x)g(x)-AB|_p \leq \max\{|f(x)(g(x) - B)|_p, |B(f(x) - A)|_p\} \leq \max\{M\varepsilon_2, |B|\varepsilon_1\}.$$

Genom att välja $\varepsilon_1, \varepsilon_2$ tillräckligt små kan vi säkerställa att $|f(x)g(x) - AB|_p < \varepsilon$ för alla x nära a, vilket visar att $f(x)g(x)$ konvergerar mot AB. □

Efter att ha granskat gränsvärdesreglerna för funktioner i $\mathbb{Q}_p$, är det naturligt att övergå till att utforska egenskaperna hos specifika klasser av funktioner inom detta område. En av de mest grundläggande och viktiga klasserna av funktioner är polynom. Vi ska nu, med följande sats, utforska egenskaper hos polynom med hänsyn till $\mathbb{Q}_p$ och visa dess kontinuitet. Vi kommer indirekt att använda följande sats i kapitel 7.

Sats 6.4. *Polynom $P(x) \in \mathbb{Q}_p[x]$ är kontinuerliga. Dvs alla polynom med koefficienter i $\mathbb{Q}_p$ är kontinuerliga.*

Bevis. Betrakta inledningsvis den konstanta funktionen $f(x) = c$, där $c \in \mathbb{Q}_p$. För alla $x, a \in \mathbb{Q}_p$ och för varje $\varepsilon > 0$, har vi $|f(x) - f(a)|_p = |c - c| = 0 < \varepsilon$. Detta visar att konstanta funktioner är kontinuerliga.

Vidare vill vi visa att identitetsfunktionen $P(x) = x$ är kontinuerlig. För varje $\varepsilon > 0$ och $a \in \mathbb{Q}_p$, låt $\delta = \varepsilon$. Om $|x - a|_p < \delta$ så är $|x - a|_p < \varepsilon$. Detta innebär att $|x - a|_p = |P(x) - P(a)| < \varepsilon$. Därav är $P(x) = x$ kontinuerlig.

Eftersom vi tidigare har bevisat att gränsvärdesreglerna gäller i $\mathbb{Q}_p$, kan vi dra slutsatsen att alla polynom $P(x) \in \mathbb{Q}_p[x]$ är kontinuerliga. Varje polynom är en kombination av konstanta termer och termer av formen $c_i x^i$, där c_i är en koefficient i $\mathbb{Q}_p$. Dessa termer är, som vi har visat, kontinuerliga, och summan och produkten av kontinuerliga funktioner är också kontinuerliga enligt gränsvärdesreglerna. Därför är hela polynomet kontinuerligt. □

6.2 Egenskaper hos $\mathbb{Q}_p$

Nu ska vi diskutera några intressanta egenskaper hos de p-adiska talen. Följande sats klargör sambandet mellan rationella tal och deras representationer i $\mathbb{Q}_p$.

Sats 6.5. *Låt x vara ett element i $\mathbb{Q}_p$, mängden av p-adiska tal. Då gäller följande:*

i) Om x är ett rationellt tal, då har x en periodisk p-adisk utveckling.

ii) Om x har en periodisk p-adisk utveckling, då är x ett rationellt tal.

Se [1, s.13], Problem 6.

Sats 6.5 visar en egenskap som de p-adiska talen har gemensamt med de reella talen, medan följande lemma nedan visar på en egenskap som inte alls gäller för de reella talen, men som gäller för de p-adiska talen.

Lemma 6.6. *En serie $\sum_{i=1}^{\infty} a_i$, där alla $a_i \in \mathbb{Q}_p$, är konvergent om och endast om $|a_i|_p \to 0$ då $i \to \infty$*

Lemmat ovan innebär, för att serien ska konvergera, måste varje efterföljande term bli mer delbar av p, eller ha en större p-adisk valuering av x, vilket innebär att det p-adiska absolutbeloppet minskar. I det p-adiska systemet är det alltså möjligt för serier med termer som inte nödvändigtvis blir mindre i traditionell mening att ändå konvergera. Denna egenskap använde vi i avsnitt 2 och 2.1, där vi såg hur $\mathbb{Q}_p$ kan närmas genom Cauchy-följder av rationella tal, där varje partialsumma av en p-adisk serie närmar sig det p-adiska talet.

7 Hensels lemma

Från kontinuitet och gränsvärdesregler i $\mathbb{Q}_p$ övergår vi nu till ett av de mer centrala resultaten inom p-adisk matematik: Hensels lemma. Detta lemma lägger grunden för att förstå lösningar till polynomekvationer i $\mathbb{Q}_p$.

Hensels lemma kan betraktas som en p-adisk analog till Newtons metod för att approximera rötter till polynom och ger ett djupt inslag i hur polynom beter sig i den p-adiska världen. Låt oss nu utforska detta viktiga resultat.

Sats 7.1 (Hensels lemma)**.** *Låt $f(x) = a_0 + a_x x + a_2 x^2 + \cdots + a_n x^n$ vara ett polynom med koefficienter i $\mathbb{Z}_p$. Antag att det finns ett p-adiskt heltal $\alpha_1 \in \mathbb{Z}_p$ sådan att*

$$\begin{aligned} f(\alpha_1) &\equiv 0 \pmod{p} \text{ och} \\ f'(\alpha_1) &\not\equiv 0 \pmod{p}, \end{aligned}$$

där $f'(x)$ är den formella derivatan av $f(x)$. Då finns ett unikt p-adiskt heltal $\alpha \in \mathbb{Z}_p$ sådan att

$$\begin{aligned} \alpha &\equiv \alpha_1 \pmod{p} \text{ och} \\ f(\alpha) &= 0. \end{aligned}$$

Bevis. Vi följer [1, s. 70-71] och vill visa att roten α existerar genom att konstruera Cauchy-sekvenser av heltal som konvergerar mot α.

Vi konstruerar alltså en sekvens $(\alpha_1, \alpha_2, \alpha_3, \dots)$ så att för alla $n \geq 1$ gäller

i) $f(\alpha_n) \equiv 0 \pmod{p^n}$,

ii) $\alpha_n \equiv \alpha_{n+1} \pmod{p^n}$.

Basfallet, då $n = 1$, är givet enligt förutsättningarna i Hensels lemma. Vi har ett $\alpha_1 \equiv c_1 \pmod{p}$ så att $f(\alpha_1) \equiv 0 \pmod{p}$, för något heltal $0 \leq c_1 \leq p-1$, vilket uppfyller villkor *i)*.

För induktionssteget, anta att vi har konstruerat α_n så att villkoren *i)* och *ii)* är uppfyllda för något $n \geq 1$. Vi vill nu konstruera α_{n+1} så att dessa villkor även gäller för $n+1$.

Vi antar att $\alpha_{n+1} = \alpha_n + c_{n+1} p^n$ för något heltal $0 \leq c_{n+1} \leq p-1$. Vi vill att $f(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}}$. Vi utvecklar $f(\alpha_{n+1})$ med Taylorserien för $f(x)$ kring α_n (som för polynom är ändlig):

$$f(\alpha_{n+1}) = \sum_{i=0}^{n} b_i \left(\alpha_{n+1} - \alpha_n\right)^i$$

där $b_i \in \mathbb{Z}_p$ med $b_0 = f(\alpha_n)$ och $b_1 = f'(\alpha_n)$. Detta ger att

$$\begin{aligned} f(\alpha_{n+1}) &= f(\alpha_n + c_{n+1}p^n) \\ &= f(\alpha_n) + f'(\alpha_n)c_{n+1}p^n + \text{högre ordningens termer i } p^n \\ &\equiv f(\alpha_n) + f'(\alpha_n)c_{n+1}p^n \pmod{p^{n+1}}. \end{aligned}$$

Eftersom $f(\alpha_n) \equiv 0 \pmod{p^n}$, kan vi skriva $f(\alpha_n) = p^n \cdot y$ för något heltal y. Då blir ekvationen:

$$p^n \cdot y + f'(\alpha_n)c_{n+1}p^n \equiv 0 \pmod{p^{n+1}}.$$

Efter att ha dividerat med p^n får vi:

$$y + f'(\alpha_n)c_{n+1} \equiv 0 \pmod{p}.$$

Eftersom $f'(\alpha_n)$ inte är delbart med p och därmed är inverterbart i $\mathbb{Z}_p$, kan vi lösa för c_{n+1}:

$$c_{n+1} \equiv -y(f'(\alpha_n))^{-1} \pmod{p}.$$

Med detta val av c_{n+1} sätter vi $\alpha_{n+1} = \alpha_n + c_{n+1}p^n$, vilket kommer att ha de önskade egenskaperna.

Vi definierar nu α som gränsvärdet av sekvensen $\alpha = \lim_{n\to\infty} \alpha_n$ i $\mathbb{Q}_p$. Enligt kontinuiteten av polynom i $\mathbb{Q}_p$ i Sats 6.4, är $f(\alpha) = \lim_{n\to\infty} f(\alpha_n)$. Eftersom $f(\alpha_n) \equiv 0 \pmod{p^n}$, konvergerar $f(\alpha_n)$ mot 0, därmed är $f(\alpha) = 0$. Därav är α en rot till $f(x)$ i $\mathbb{Q}_p$, vilket visar Hensels lemma. □

Detta är essensen i Newton-Raphson metoden, vilket är möjligt eftersom $f(x)$ är kontinuerligt i $\mathbb{Q}_p$ enligt Sats 6.4 och visar att vi kan fortsätta processen: givet α_n, kan vi hitta α_{n+1}.

7.1 Newton-Raphsons metod

I kölvattnet av Hensels lemma kommer vi nu att utforska en p-adisk version av Newton-Raphsons metod, en klassisk metod för att hitta rötter till polynom. I $\mathbb{Q}_p$, där vi hanterar p-adiska heltal och koefficienter, tar denna metod en form som låter oss effektivt beräkna p-adiska rötter.

Låt oss definiera denna metod i p-adisk kontext.

Definition 7.2 (Newton-Raphsons metod i $\mathbb{Q}_p$)**.** Låt $f(x)$ och $f'(x)$ vara polynom med koefficienter i $\mathbb{Q}_p$. Antag att det finns ett p-adiskt heltal $\alpha_1 \in \mathbb{Z}_p$ så att

$$f(\alpha_1) \equiv 0 \pmod{p} \quad \text{och} \quad f'(\alpha_1) \not\equiv 0 \pmod{p}.$$

Då definieras en följd (x_n) i $\mathbb{Q}_p$ enligt

$$\begin{cases} x_1 = \alpha_1, \\ x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, \quad n = 1, 2, 3, \ldots \end{cases}$$

Denna följd (x_n) konvergerar p-adiskt mot ett p-adiskt heltal $\alpha \in \mathbb{Z}_p$ så att $f(\alpha) = 0$ och $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$.

Bevis. Vi vill visa att sekvensen x_n konvergerar mot α, eller att x_n blir allt närmare α för varje ny term. Antag inledningsvis att f är ett polynom i $\mathbb{Z}_p[x]$ och att $f(\alpha) = 0$, samt $f'(\alpha) \not\equiv 0 \pmod{p}$, där α är en rot i $\mathbb{Z}_p$. Vi kan då skriva f som

$$f(x) = (x - \alpha)g(x),$$

där $g(x)$ är ett polynom med $g(\alpha) \not\equiv 0 \pmod{p}$. Detta innebär att $|g(\alpha)|_p = 1$, eftersom $g(\alpha)$ är ett p-adiskt heltal ej delbart med p.

För derivatan av f har vi att

$$f'(x) = g(x) + (x - \alpha)g'(x).$$

Eftersom $f'(\alpha) \not\equiv 0 \pmod{p}$, måste $|f'(\alpha)|_p = 1$ och därmed $|g(\alpha)|_p = 1$.

Antag att vi har en approximation x_n till α så att

$$|x_n - \alpha|_p = p^{-b}$$

för något $b > 0$. Vi vill visa att om $|x_n - \alpha|_p = p^{-b}$ så är $|x_{n+1} - \alpha|_p \leq p^{-2b}$ eller att $|x_{n+1} - \alpha|_p < |x_n - \alpha|_p^2$.

Newton-Raphsons iterativa formel ges av

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} = x_n - \frac{(x_n - \alpha)g(x_n)}{g(x_n) + (x_n - \alpha)g'(x_n)}.$$

Då fås efter förenkling

$$|x_{n+1} - \alpha|_p = \left| \frac{(x_n - \alpha)^2 g'(x_n)}{g(x_n) + (x_n - \alpha)g'(x_n)} \right|_p.$$

När vi tittar på nämnaren, observerar vi att den kan förenklas genom att betrakta den modulo p. Eftersom $|g(\alpha)|_p = 1$ och $g(x)$ är kontinuerlig, vet vi att $|g(x_n)|_p = 1$ när x_n närmar α. Därför är $g(x_n) \equiv 1 \pmod{p}$ när x_n är nära α. Eftersom $|x_n - \alpha|_p < 1$, är termen $(x_n - \alpha)g'(x_n)$ försumbar modulo p, vilket leder till att

$$g(x_n) + (x_n - \alpha)\, g'(x_n) \equiv 1 \qquad (\text{mod } p)).$$

Detta innebär att nämnaren är kongruent med 1 modulo p och därmed har vi

$$|x_{n+1} - \alpha|_p = \left|(x_n - \alpha)^2 g'(x_n)\right|_p .$$

Med antagandet att $|x_n - \alpha|_p = p^{-b}$ och att $|g'(x_n)|_p \leq 1$, kan vi dra slutsatsen att

$$|x_{n+1} - \alpha|_p \leq p^{-2b}$$

vilket visar att Newton-Raphsons metod konvergerar kvadratiskt för p-adiska tal under de givna antagandena. □

Vi har just sett att Newton-Raphsons metod konvergerar kvadratiskt, vilket innebär att antalet korrekta p-adiska siffror ungefär fördubblas efter varje iteration. Efter att nu ha etablerat Hensels lemma och Newton-Raphsons metod i p-adiska tal, undersöker vi i nästkommande kapitel, specifika exempel för att se dessa koncept i praktiken.

8 Implementering av p-adiska tal i Python

I denna del presenteras en Python-klass som kan representera och arbeta med p-adiska tal. Python-koden finns tillgänglig i appendix A.

Qp_klass tar emot ett rationellt tal, basen p och den önskade precisionen för att skapa en p-adisk representation. Den hanterar grundläggande aritmetiska operationer och kan presentera p-adiska tal på ett lättläst format. Metoden _new_m(self) justerar det ursprungliga rationella värdet till ett enklare och mer begränsat tal kongruent med det ursprungliga *modulo* p^{prec}, för att säkerställa att endast relevanta siffror för den angivna precisionen bevaras, vilket förbättrar tidskomplexiteten. Notationen $O(p^n)$ används för att indikera att termer av ordningen p^n eller högre inte betraktas vid beräkning eller representation. Klassen använder Sympy-biblioteket för att hantera rationella tal och faktorisering av heltal.

För att på ett effektivt vis använda klassen rekommenderas en miljö som stödjer typsättning med LaTeX, som Jupyter Notebook, för att visualisera de p-adiska talen på ett lättläst format. Elementen representeras i en dictionary med koefficienter, varav varje koefficient är kopplad till respektive potens p. Dessutom kan klassen även representera p-adiska tal som en sträng i ett kompakt format, i enlighet med tidigare införd notation i avsnitt 2.2.

Det har varit svårt, men roligt att skriva objektorienterad kod överlag. En rad utmaningar har uppstått, såsom att hantera precisionen i alla aritmetiska metoder för att inte förlora information, att korrekt implementera LaTeX-formateringen och den kompakta strängrepresentationen, till hanteringen av olika särfall och allmän testning samt felsökning. Den största insikten var _new_m(self) metodens betydelse för klassens allmänna effektivitet. Alltså hur Sympys Rational och

_new_m(self) används för att kontinuerligt förenkla representationen av rationella tal för att upprätthålla prestanda, och därav vikten av hur klasser lagrar och hanterar data.

Exempel 8.1. Här följer en kort demonstration av klassens grundläggande funktionalitet.

```
from Qp_klass import Qp, Rational, factorint

# Skapar en instans av talet -3 och basen 2.
x = Qp(-3, 2)
print(x)
```

```
...1111111101
```

```
# Utför aritmetiska operationer med det 2-adiska talet x
(x**2 - 7) / (13*x + x*x)
```

$$1 + 1 \cdot 2^4 + 1 \cdot 2^8 + O\left(2^9\right)$$

```
# Skapar en instans av talet -3/100 och basen 2.
q = Qp(-3, 2)/100
print(q)
```

```
...11100001,01
```

```
#Jämför q med -3/100
q == Rational(-3,100)
```

```
True
```

Exempel 8.2. Vi vill hitta en p-adisk kvadratrot till 2 i $\mathbb{Q}_7$ och definierar vårt polynom som $f(x) = x^2 - 2$ där $f'(x) = 2x$. Därefter uppmärksammas det att vi har två lämpliga startpunkter som uppfyller kraven i Hensels lemma, $\alpha_1 = 3, 4$. Vi väljer $\alpha_1 = 3$ och tillämpar Newton-Raphsons metod för att iterativt närma oss kvadratroten. Följande kod utför denna iteration.

```
x = Qp(3, 7, 16)
for i in range(4):
    x = (x*x + 2) / (2*x)
    print(x)
```

```
...1111111111111113
...3062113523306213
...1623525321216213
...2011266421216213
```

Den 2-adiska representationen av $\sqrt{2}$ blir

$$3 + 1 \cdot 7^1 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 + 2 \cdot 7^5 + 1 \cdot 7^6 + 2 \cdot 7^7 + 4 \cdot 7^8 + 6 \cdot 7^9 + 6 \cdot 7^{10} + 2 \cdot 7^{11} + 1 \cdot 7^{12} + 1 \cdot 7^{13} + 2 \cdot 7^{15} + O\left(7^{16}\right).$$

Efter bara 4 iterationer har vi fått 16 korrekta termer, eftersom konvergensen är kvadratisk, som vi såg i avsnitt 7.1.

Exempel 8.3. Vi kan definiera en funktion som hittar lösningar till allmänna polynomekvationer. I följande kod får kan man anpassa polynomekvationen och dess derivata manuellt samt ange en rimlig startpunkt. Precis som i exemplet ovan kan vi hitta den 2-adiska representationen för $\sqrt{2}$, fast med ännu högre precision.

```
def newton_raph(f, df, p, start, prec=10, verbose=False):
    if f(start) % p != 0 or df(start) % p == 0:
        raise ValueError("Startpunkt uppfyller ej villkoret")
    x = Qp(start, p, prec)
    for i in range(prec):
        new_x = x - f(x) / df(x)
        if new_x == x:
            return x
        if verbose:
            print(f"Iteration {i+1}: x = {new_x}")
        x = new_x

f = lambda x: x**2 - 2
df = lambda x: 2*x
root = newton_raph(f, df, p=7, start=3, prec=41, verbose=True)
```

```
Iteration 1: x = ...11111111111111111111111111111111111113
Iteration 2: x = ...13523306211352330621135233062113523306213
Iteration 3: x = ...25504256513604254524006401623525321216213
Iteration 4: x = ...65361650444540551321333302011266421216213
Iteration 5: x = ...60454661654365536623164112011266421216213
Iteration 6: x = ...42640361054365536623164112011266421216213
```

Exempel 8.4. Vi kan med samma kod som i Exempel 8.3 även hitta den n:te roten av ett tal i $\mathbb{Q}_p$. I detta fall den tredje roten av två i $\mathbb{Q}_{17}$. Precis i Exempel 8.2 är vårt polynom nu istället $f(x) = x^3 - 2$ där $f'(x) = 3x^2$ och vi noterar att $f(8) = 510 \equiv 0 \pmod{17}$ samt $f'(8) = 192 \not\equiv 0 \pmod{17}$. Därför väljer vi vår startpunkt $\alpha_1 = 8$.

```
f = lambda x: x**3-2
df = lambda x: 3*x**2
root = newton_raph(f, df, p=17, start=8)
display(root)
print(root)
```

$$8+11\cdot 17^1+6\cdot 17^2+3\cdot 17^3+5\cdot 17^4+12\cdot 17^5+8\cdot 17^6+13\cdot 17^7+15\cdot 17^8+O\left(17^{10}\right)$$

```
...0_15_13_8_12_5_3_6_11_8
```

Här separeras varje koefficient med '_' för tydliggöra koefficienter större än nio.

A Kod för $\mathbb{Q}_p$-klassen

Python-koden finns tillgänglig här.

```python
from sympy import Rational, factorint

class Qp:

    def __init__(self, m, p, prec=10):
        self.p = p
        self.prec = prec
        m = Rational(m, 1)
        v = Qp.valuation(m, p)
        if m and v >= prec:
            v = None
        self.v = v
        self.digits = self._digits(m)
        self.m = self._new_m()

    @staticmethod
    def valuation(m, p):
        num, den = m.p, m.q
        if num == 0:
            return None
        a = factorint(num, limit=p).get(p, 0)
        b = factorint(den, limit=p).get(p, 0)
        return a - b

    def _digits(self, m):
        digits = {}
        if not self:
            return {self.prec-1: 0}
        m0 = (Rational(self.p, 1)**(-self.v))*m
        k_n = m0.p
        b_prime = m0.q
        for n in range(self.v, self.prec):
            a_n = (k_n * pow(b_prime, -1, self.p)) % self.p
            k_n = (k_n - b_prime * a_n) // self.p
            digits[n] = a_n
        return digits

    def _new_m(self):
        """Skapar en ny representation av det p-adiska talet
           med minsta möjliga potenser av p"""
        new_m = 0
        for power, digit in self.digits.items():
            if power < self.prec:
                new_m += digit * (Rational(self.p, 1) ** power)
        return Rational(new_m, 1)

    def __repr__(self):
        return (f"Qp(Rational({self.m.p}, {self.m.q}), "
                f"p = {self.p}, prec={self.prec})")

    def _latex(self):
        if self.m == 0:
            return f"O\\left({self.p}^{{ {self.prec} }}\\right)"
```

```
        p_adic_terms = [ f"{digit} \\cdot {self.p}^{{ {power} }}"
                         if power != 0 else str(digit)
                         for power, digit in sorted(self.digits.items())
                         if digit != 0 ]
        highest_power = max(self.digits.keys(), default=-1)
        return (f"{' + '.join(p_adic_terms)} "
                f"+ O\\left({self.p}^{{ {highest_power + 1} }}\\right)")

    def _repr_latex_(self):
        return f"$ {self._latex()} $"

    def __str__(self):
        compact_str = ['...']
        separator = '_' if self.p >= 11 else ''
        highest_power = max(self.digits.keys(), default=0)
        for power in range(highest_power, -1, -1):
            compact_str.append(str(self.digits.get(power, 0)))
            if power != 0:
                compact_str.append(separator)
        lowest_power = min(self.digits.keys(), default=-1)
        if lowest_power < 0:
            compact_str.append(',')
            for power in range(-1, lowest_power - 1, -1):
                digit = self.digits.get(power)
                if digit is None:
                    compact_str.append('.')
                else:
                    compact_str.append(str(digit))
                compact_str.append(separator)
        return ''.join(compact_str).rstrip(separator)

    def __add__(self, other):
        if not isinstance(other, Qp):
            return Qp(self.m + Rational(other,1), self.p, prec=self.prec)
        else:
            if not self.p == other.p:
                raise ValueError("Addition av p-adiska tal med olika baser.")
            min_prec = min(self.prec, other.prec)
            new_m = self.m + other.m
            return Qp(new_m, self.p, prec=min_prec)

    def __radd__(self, other):
        return self + other

    def __neg__(self):
        return Qp(-self.m, self.p, prec=self.prec)

    def __pos__(self):
        return self

    def __sub__(self, other):
        return self + (-other)

    def __rsub__(self, other):
        return other + (-self)

    def __mul__(self, other):
        if not isinstance(other, Qp):
```

```
112             other = Rational(other, 1)
113             if other == 0: return 0
114             v = Qp.valuation(other, self.p)
115             return Qp(self.m * other, self.p, prec=self.prec + v)
116         if not self.p == other.p:
117             raise ValueError("Multiplikation av p-adiska tal med olika baser.")
118         if not self or not other:
119             max_prec = max(self.prec, other.prec)
120             return Qp(0, self.p, max_prec)
121         min_prec = min(self.v + other.prec, other.v + self.prec)
122         return Qp(self.m * other.m, self.p, prec=min_prec)
123 
124     def __rmul__(self, other):
125         return self * other
126 
127     def __invert__(self):
128         if not self:
129             raise ZeroDivisionError
130         min_prec = -self.v + self.prec
131         return Qp(1 / self.m, self.p, prec=min_prec)
132 
133     def __pow__(self, n):
134         if n < 0 and not self:
135             raise ZeroDivisionError("Kan inte upphöja 0 till ett negativt tal.")
136         if n == 0:
137             return Qp(1, self.p, prec=self.prec)
138         if not self:
139             return Qp(0, self.p, prec=self.prec ** n)
140         new_m = self.m ** n
141         new_v = self.v * n
142         new_prec = self.prec + (new_v - self.v)
143         return Qp(new_m, self.p, prec=new_prec)
144 
145     def __truediv__(self, other):
146         if not isinstance(other, Qp):
147             if other == 0: raise ZeroDivisionError
148             return self * Rational(1,other)
149         return self * ~other
150 
151     def __rtruediv__(self, other):
152         return ~self * other
153 
154     def __eq__(self, other):
155         if not isinstance(other, Qp):
156             other = Qp(other, self.p, prec=self.prec)
157         if self.p != other.p:
158             return False
159         min_prec = min(self.prec, other.prec)
160         for i in range(min_prec):
161             if self.digits.get(i, 0) != other.digits.get(i, 0):
162                 return False
163         return True
164 
165     def __bool__(self):
166         return self.v is not None
167 
168     def __abs__(self):
169         return 0 if not self else Rational(self.p, 1)**(-self.v)
```

Referenser

[1] Gouvêa, Q. F. (2003). *p−adic Numbers: An introduction*. 2nd ed. Springer-Verlag.

[2] Koblitz, N (1984). *p−adic Numbers, p−adic Analysis, and Zeta-Functions*. 3rd ed. Springer-Verlag.

[3] Bachman, G. (1964). *Introduction to p-Adic Numbers and Valuation Theory*. 1st ed. Academic Press Inc.

[4] Persson, A. L. Böiers (2010). *Analys i en variabel*. 3rd ed. Studentlitteratur.

[5] Ullrich, P. (1998). *The Genesis of Hensel's p-adic Numbers*. I: Butzer, P. L., Jongen, H. Th., & Oberschelp, W. (edd.), *Charlemagne and his Heritage. 1200 Years of Civilization and Science in Europe / Karl der Große und sein Nachwirken. 1200 Jahre Kultur und Wissenschaft in Europa*, Vol. 2. Mathematical Arts. Turnhout: Brepols, s. 163-178.

[6] Wilson, Joseph Colton, (2013). *Comparing the algebraic and analytical properties of p-adic numbers with real numbers*. Theses Digitization Project. 4198.. Tillgänglig här.

[7] Harrington, Charles I, (2011). *An Introduction to the p-adic Numbers*. Honors Theses. 992. Tillgänglig här.

[8] Conrad, K. *Rationals in* $\mathbb{Q}_p$. Tillgänglig här.