Fakulteten för teknik och naturvetenskap

Per Eklund

P-adiska tal

P-adic numbers

Matematik
C-uppsats

Datum/Termin: 2007-05-06
Handledare: Håkan Granath
Examinator: Thomas Martinsson

Karlstads universitet 651 88 Karlstad
Tfn 054-700 10 00 Fax 054-700 14 60
Information@kau.se www.kau.se

Sammanfattning

De p-adiska talen vars främsta användningsområde ligger inom talteorin beskrevs först av den tyske matematikern Kurt Hensel 1897.
För varje primtal p, så utvidgas talsystemet Q av rationella tal till ett större talsystem som betecknas Q_p, de så kallade p-adiska talen.
En annorlunda valuation av rationella tal ger ett så kallat icke-arkimediskt absolutbelopp samt en annan metrik än den vi är vana vid, en ultrametrik. Vilket gör att kroppen av p-adiska tal Q_p får en annorlunda topologi.
Ett icke-arkimediskt absolutbelopp har samma egenskaper som ett vanligt arkimediskt absolutbelopp, samt en extra egenskap nämligen $|x + y| \leq \max\{|x|, |y|\}$.

Avslutningsvis använder vi oss av Hensels lemma, vilken bygger på Newton-Raphsons metoden för att lösa ekvationer, för att bestämma om ett polynom har rötter i Z_p och i så fall vilka de är. Då den p-adiska analysen på många sätt är lättare än den reella analysen så visar Hensels lemma ganska lätt om ett polynomen har rötter i Z_p.

Innehållsförteckning

Sammanfattning 1
Innehållsförteckning 2
1. Inledning 3
1.1 Bakgrund 3
1.2 Introduktion 3
1.3 Kongruenser modulo p^n 8
2. Förberedelser för att kunna räkna p-adiska tal 17
2.1 Absolutbelopp på en kropp 17
2.2 Icke-arkimediskt absolutbelopp 24
2.3 Topologi 26
2.3.1 Ultrametriskt rum 26
2.3.2 Öppna och slutna bollar 30
3. P-adiska tal 35
3.1 Absolutbelopp på Q 35
3.2 Komplettering 36
3.3 Hensels lemma 38
4. Referenser 41

1. Inledning

1.1 Bakgrund

Den här uppsatsen är en introduktion till p-adiska tal. Jag har följt de tre första kapitlen i boken *p-adic numbers, av Fernando Q. Gouvea*. Alla definitioner och satser är tagna ifrån denna bok, samt vissa bevis.
Mitt upplägg har varit att följa boken och svara på utvalda problem. En del är presenterade som exempel, andra som bevis för satser och lemman och en del exempel är egenkomponerade.

1.2 Introduktion

De p-adiska talen beskrevs först av den tyske matematikern Kurt Hensel 1897.
Det p-adiska talsystemet främsta användningsområde ligger inom talteorin där det ger ett alternativt sätt att räkna.

I den vanliga matematiken med reella tal så har vi tal med ett oändligt antal decimaler t.ex. 1/3, som med ett oändligt antal decimaler skrivs som 0,33333….
Två tal som skiljer sig åt på den 10:e decimalen är ungefär lika, två tal som skiljer sig åt på den 20:e decimalen är än mer lika än de föregående två.
Desto större negativ 10 potens desto mindre är differensen.
Ett 10-adiskt tal har en liknande utveckling men med den skillnaden att differensen mellan två tal är mindre om de skiljer sig åt med en stor positiv 10 potens, alltså 2222 är nära 3222, men 222222 är än närmre 322222.
Men de 10-adiska talen har en nackdel, det finns nämligen par av tal skilda från noll vars produkt blir noll. Men de 10-adiska talen är en ring med nolldelare. Detta problem undviks dock genom att använda primtal som bas istället för 10.

Om p är ett primtal, så kan alla positiva heltal skrivas i en utveckling i basen p på formen

$\sum_{i=0}^{n} \alpha_i p^i \quad ,0 \le \alpha_i \le p-1.$

T.ex. 35 binärt är $1\times 2^5 + 0\times 2^4 + 0\times 2^3 + 0\times 2^2 \times 1\times 2^1 + 1\times 2^0$ vilket skrivs som 100011_2.

Utvecklingen i basen p visar om m är delbart med p och i så fall i vilken grad,
t.ex. utveckla 75 i basen 3 ger:
$75 = 0 + 1\times 3 + 2\times 3^2 + 2\times 3^3$, vilket visar att 75 är delbart med 3, men ej med högre potenser.

När vi nu ska gå vidare till rationella tal så betraktar vi formella serier $\sum_{i=0}^{\infty} \alpha_i p^i$ i stället för ändliga summor.

Vi betraktar först det rationella talet

$\alpha = \frac{a}{b} \quad b \neq 0.$ Om vi betraktar fallet $p \nmid b$ då kan vi uttrycka α som

$\alpha = n + \alpha' \qquad n = \text{heltal}, -1 < \alpha' < 0.$

Lemmat nedan kommer att användas för att utveckla ett rationellt tal i basen p.

Lemma 1.2.1

Tag $\alpha = a/b$ där $p \nmid b, \quad -b < a < 0$ och a, b är heltal.

Då finns heltal x och a' så att

$$\frac{a}{b} = x + p\frac{a'}{b} \quad \text{med} -b < a' < 0 \text{ och } 0 \le x \le p-1.$$

Bevis.

Vi vill ha $a = bx + pa'$

då är $a - bx = pa'$, så $p \mid a - bx$

vilket kan utryckas som $a - bx \equiv 0 \pmod{p}$

$a \equiv bx \pmod{p}$.

Det existerar ett unikt $x \in \{0,1,...,p-1\}$ så att $a \equiv bx \pmod{p}$ ty $p \nmid b$.

Sätt $a' = \dfrac{a-bx}{p}$

då är $a' = \dfrac{a-bx}{p} < 0$

$$a' = \frac{a-bx}{p} > \frac{-b-bx}{p} = \frac{-x-1}{p}b \ge \frac{-p}{p}b = -b$$ VSB.

Upprepad tillämpning av lemmat ger oss det rationella talet utvecklat i basen p, vilket ser ut på följande sätt.

Om $-1 < \dfrac{a}{b} < 0$ och $p \nmid b$

så är $\dfrac{a}{b} = x_0 + p\dfrac{a_0}{b}$ med $-b < a_0 < 0$ och $0 \le x_0 \le p-1$.

$\dfrac{a_0}{b} = x_1 + p\dfrac{a_1}{b}$ med $-b < a_1 < 0$ och $0 \le x_1 \le p-1$.

$\dfrac{a_1}{b} = x_2 + p\dfrac{a_2}{b}$ med $-b < a_2 < 0$ och $0 \le x_2 \le p-1$.

osv. på samma sätt.

Vilket ger att $\dfrac{a}{b} = x_0 + p\dfrac{a_0}{b} = x_0 + p\left(x_1 + p\dfrac{a_1}{b}\right) = x_0 + px_1 + p^2\left(x_2 + p\dfrac{a_2}{b}\right) = ...$

Exempel

Det rationella talet $1/7$ utvecklat i basen 3.

Vi blir här tvungna att göra ett förberedande steg, för att $\frac{1}{7} \notin [-1, 0]$

$\frac{1}{7} = 1 + 3\frac{-2}{7}$; $\frac{-2}{7} \in [-1, 0]$.

Vi kan nu använda oss av Lemma 1.2.1 som ger

$\frac{-2}{7} = 1 + 3\frac{-3}{7}$;*

$\frac{-3}{7} = 0 + 3\frac{-1}{7}$

$\frac{-1}{7} = 1 + 3\frac{-2}{7}$. ; tillbaka till *

Alltså $\frac{1}{7} = 3^0 + 3 + 0 \times 3^2 + 3^3 + 3^4 + 0 \times 3^5 + 3^6 + ... = 1 + 3 + 3^3 + 3^4 + 3^6 + ...$

För rationella tal $x = \frac{a}{b}$, så kan man alltså för alla primtal p rent formellt utrycka det på formen

$x = \frac{a}{b} = \sum_{n \geq n_0} a_n p^n$. Det gäller att $n_0 \geq 0$ omm $p \nmid b$ och $n_0 > 0$ omm $p \nmid b$ och $p \mid a$ (antag att a/b är förkortat så långt som möjligt).

Vi kallar detta den *p-adiska utvecklingen* av x
dvs. $x = \sum_{n \geq n_0} a_n p^n \quad 0 \leq a_n \leq p - 1.$

Nu vill vi kunna räkna med sådana serier. Vi kommer att räkna formellt med addition och multiplikation. Det är naturligtvis inte självklart att detta kommer att fungera, senare i uppsatsen kommer det dock att visa sig vara möjligt.
När vi räknar med dessa serier så visar det sig att vi får en kropp,
denna kropp får beteckningen Q_p och kallas *kroppen av p-adiska tal.*

Funktionen $x \mapsto p - adisk\ utveckling\ av\ x$ ger en inbäddning $Q \to Q_p$.

Lemma 1.2.2
Alla rationella tal har en periodisk p-adisk utveckling och omvänt gäller det att en periodisk p-adisk utveckling ger ett rationellt tal.

Bevis
Vi visar först att en periodisk p - adisk utveckling ger ett rationellt tal.

Låt x vara en p - adisk utveckling med perioden n :

$x = a_0 + a_1 p + ... + a_{n-1} p^{n-1} + a_0 p^n + a_1 p^{n+1} ...$

om vi multiplicerar med p^n får vi

$p^n x = a_0 p^n + a_1 p^{n+1} + ...$

$x - p^n x = a_0 + a_1 p + ... + a_{n-1} p^{n-1}$

vilket ger $x = \dfrac{a_0 + a_1 p + ... + a_{n-1} p^{n-1}}{1 - p^n}$.

Alltså x är ett rationellt tal.

Vi ska nu visa att rationella tal har en periodisk p - adisk utveckling.

Om det rationella talet $\dfrac{a}{b} \notin [-1, 0]$ är vi tvungna att använda oss av ett förberedande steg

$$\frac{a}{b} = x_0 + p\frac{a_0}{b} \quad -1 < \frac{a_0}{b} < 0 \text{ och } 0 \le x_0 \le p-1.$$

Då är $\dfrac{a_0}{b} = x_1 + p\dfrac{a_1}{b}$ $\qquad 0 \le x_1 \le p-1$

$\dfrac{a_1}{b} = x_2 + p\dfrac{a_2}{b}$ $\qquad 0 \le x_2 \le p-1$

osv.

$$\frac{a}{b} = x_0 + p\frac{a_0}{b} = x_0 + p\left(x_1 + p\frac{a_1}{b}\right) = x_0 + px_1 + p^2\left(x_2 + p\frac{a_2}{b}\right) = ...$$

Eftersom $-1 < \dfrac{a_i}{b} < 0$ så är $-b < a_i < 0$ så kommer ett a_i att vara det samma som ett tidigare a_i efter högst $b-1$ gånger.

Alltså har det rationella talet a/b en periodisk p - adisk utveckling. VSB.

Exempel

Tag det rationella talet $1/5$ och låt $p = 3$, då har vi att

$$\frac{1}{5} = 1 + \frac{-4}{5}$$

$$\frac{-4}{5} = 1 + 3\frac{-3}{5} \qquad ;*$$

$$\frac{-3}{5} = 0 + 3\frac{-1}{5}$$

$$\frac{-1}{5} = 1 + 3\frac{-2}{5}$$

$$\frac{-2}{5} = 2 + 3\frac{-4}{5} \qquad ; \text{tillbaka till } *$$

$$\frac{1}{5} = 1 + 1 + 0p + p^2 + 2p^3 + p^4 + ... =$$

$$= 2 + p^2 + 2p^3 + p^4 + ...$$

$$\frac{1}{5} = 2 + \underbrace{3^2 + 2\times 3^3 + 3^4}_{period} + \underbrace{3^6 + 2\times 3^7 + 3^8}_{period} + \underbrace{3^{10} + 2\times 3^{11} + 3^{12}}_{period} + ...$$

Alltså det rationella talet $1/5$ har en 3 - adisk period på 3.

Om det p - adiska talet är

$$x = a_0 p^{n_0} + a_1 p^{n_0+1} + a_2 p^{n_0+2} + a_3 p^{n_0+3} + ... = \sum_{n \geq n_0} a_n p^n .$$

Vad är då $-x$?

Låt $b_n = p - 1 - a_n$ för alla $n \geq n_0$

och sätt $y = b_0 + b_1 p + b_2 p^2 + ... = \sum_{n \geq n_0} (p - 1 - a_n) p^n .$

Då får vi att $x + y = \sum_{n \geq n_0} (p-1) p^n = \sum_{n \geq n_0} p^{n+1} - \sum_{n \geq n_0} p^n = -p^{n_0}$

vilket ger att $x + y + p^{n_0} = 0$

alltså är $-x = p^{n_0} + y$

dvs. $-x = p^{n_0} + \sum_{n \geq n_0} (p - 1 - a_n) p^n .$

Exempel

$$1 = \sum_{n \geq 0} a_n p^n = 1 + 0p^0 + 0p^1 + 0p^2 + ... \qquad (n_0 = 0)$$

så

$$-1 = 1 + \sum_{n \geq 0} (p - 1 - a_n) p^n = 1 + (p-2)p^0 + (p-1)p^1 + (p-1)p^2 + ... =$$

$$= (p-1) + (p-1)p + (p-1)p^2 + ...$$

1.3 Kongruenser modulo p^n

Om vi nu tittar på kongruensekvationer modulo p^n så kommer vi att se att de påminner om de p-adiska tal vi redan gjort.
De lättaste kongruensekvationerna är givetvis de som har lösning i Q (rationella lösningar), som de 3 följande exemplen visar.

Exempel:

Vi vill lösa $x_n^{\,2} \equiv 16 \pmod{3^n}$ med $0 \le x_n \le 3^{n-1}$

på så sätt att varje lösning $x_{n+1} \equiv x_n \pmod{3^n}$.

Ekvationen $x^2 = 16$ har lösningen $x = \pm 4$,

men vi vill att $x_n \in [0, p^{n-1}]$ vilket gör att vi får arbeta lite med lösningarna.

Vi tittar först på fallet $x = 4$.

Då får vi
$$x_1 \equiv 1 \pmod{3}$$
$$x_2 \equiv 4 = 1 + 3 \pmod{9}$$
$$x_3 \equiv 4 = 1 + 3 \pmod{27}$$

osv.

Sedan på fallet $x = -4$.

Då får vi
$$x_1 \equiv 2 \pmod{3}$$
$$x_2 \equiv 5 = 2 + 3 \pmod{9}$$
$$x_3 \equiv 23 = 2 + 3 + 2 \times 9 \pmod{27}$$
$$x_4 \equiv 77 = 2 + 3 + 2 \times 9 + 2 \times 27 \pmod{81}$$

osv.

Alltså den 3 - adiska utvecklingen av :

$x = 4 = 1 + 1 \times 3$

$x = -4 = 2 + 1 \times 3 + 2 \times 3^2 + 2 \times 3^3 + \ldots$

Definition 1.3.1

Låt p vara ett primtal. Då säger vi att en följd av heltal $x_1, x_2, x_3, \ldots$ sådan att $0 \le x_n \le p^n - 1$ för alla n är koherent om det för alla $n \ge 1$ gäller att :

$x_{n+1} \equiv x_n \pmod{p^n}$

Eftersom p är ett primtal kan vi säga att följden är p-adiskt koherent.

Sambandet mellan formella serier och koherenta följder inses genom att trunkera den formella serien för att få den koherenta följden. För att gå ifrån en koherent följd till en formell serie behöver man endast utveckla x_n, vilket sedan ger x.
Eftersom det är enklare att hantera koherenta följder än serier kommer vi i fortsättningen att göra detta.

Exempel

Vi vill lösa $x_n^{\,2} \equiv 49 \pmod{5^n}$ då $0 \le x_n \le p^n - 1$.

På så sätt att varje lösning $x_{n+1} \equiv x_n \pmod{p^n}$.

Ekvationen $x^2 = 49$ har lösningen $x = \pm 7$.

Vi tittar först på fallet $x = 7$.

Då får vi $x_1 \equiv 2 \pmod 5$

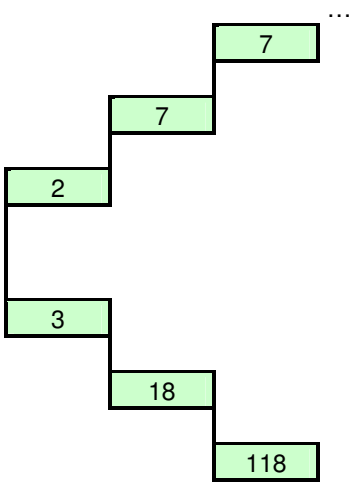
$x_2 \equiv 7 = 2 + 1 \times 5 \pmod{25}$.

Sedan på fallet $x = -7$.

Då får vi $x_1 \equiv 3 \pmod 5$

$x_2 \equiv 18 = 3 + 3 \times 5 \pmod{25}$

$x_3 \equiv 118 = 3 + 3 \times 5 + 4 \times 25 \pmod{125}$.



Alltså den 5 - adiska utvecklingen av :

$x = 7 = 2 + 1 \times 5$

$x = -7 = 3 + 3 \times 5 + 4 \times 5^2 + ...$

Om vi tar *p=2* så blir det hela lite svårare, för ”trädet” av lösningar i modulo 2 är mycket mera komplext, det kommer nämligen att finnas lösningar i modulo 2^n som ej går att ”lyfta” till modulo 2^{n+1}.

Exempel

Vi ska lösa $x_n^{\,2} \equiv 81 \pmod{2^n}$ då $0 \le x_n \le p^n - 1$ $x_{n+1} \equiv x_n \pmod{p^n}$.

$81 \equiv 1 \pmod 2$

om $x_1^{\,2} \equiv 1 \pmod 2$ så är

$x_1 = 1 \pmod 2$.

När vi nu har hittat x_1 så kan vi använda oss av

$x_{n+1} = x_n + k2^n \pmod{2^{n+1}}$ $0 \le k < 2$.

Vi kan använda oss av formeln för att prova oss fram till lösningar, problemet som uppstår är att det kommer att finnas lösningar i $(\mathrm{mod}\ 2^n)$ som ej går att lyfta till $(\mathrm{mod}\ 2^{n+1})$.

Alltså är $x_2 = x_1 + k2 \pmod{2^{n+1}}$ $n = 1$ $0 \le k < 2$,

vilket ger oss två möjliga lösningar : $x_2 \equiv 1, 3 \pmod 4$.

Då $81 \equiv 1 \pmod 4$

så måste $x_2^{\,2} \equiv 1 \pmod 4$ och detta uppfylls för båda $x_2 = 1, 3$.

Nästa steg är $x_3 = x_2 + k2^n \pmod{2^{n+1}}$ $n = 2$ $0 \le k < 2$,

vilket ger oss två möjliga lösningar då $x_2 = 1$: fås $x_3 \equiv 1, 5 \pmod 8$

och för $x_2 = 3$: fås $x_3 \equiv 3, 7 \pmod 8$.

Då $81 \equiv 1 \pmod 8$ så måste $x_3^{\,2} \equiv 1 \pmod 8$ och detta uppfylls då $x_3 = 1, 5, 3, 7$.

Då är $x_4 = x_3 + k2^n \pmod{2^{n+1}}$ $n = 2$ $0 \le k < 2$.

När $x_3 = 1$ ger det oss två möjliga lösningar för $x_4 \equiv 1, 9 \pmod{16}$.

När $x_3 = 5$ ger det oss två möjliga lösningar för $x_4 \equiv 5, 13 \pmod{16}$.

$x_3 = 3$ $x_4 \equiv 3, 11 \pmod{16}$.

$x_3 = 7$ $x_4 \equiv 7, 15 \pmod{16}$.

Då $81 \equiv 1 \pmod{16}$ så måste $x_4^{\,2} \equiv 1 \pmod{16}$ och detta uppfylls då $x_4 = 1, 9, 7, 15$.

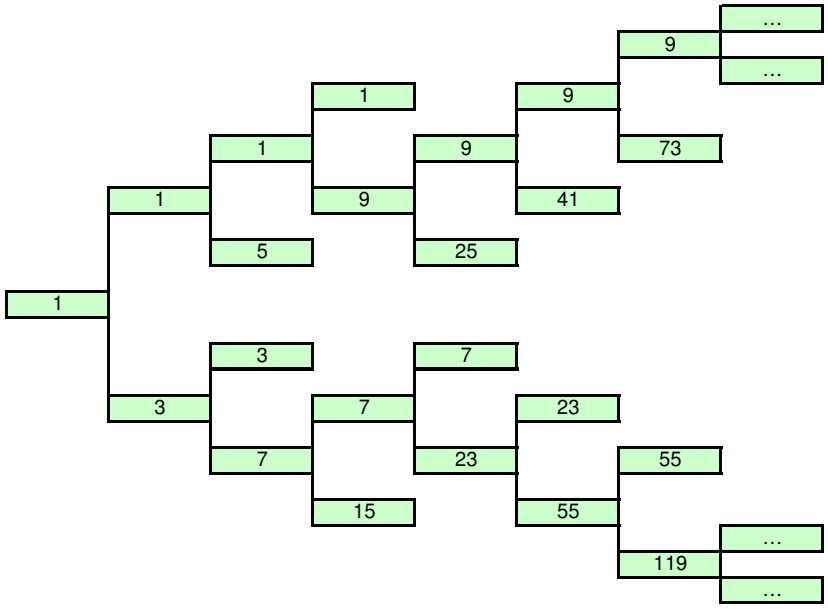
Alltså kunde vi inte lyfta $x_3 = 5, 3$ till x_4 för att $5, 13, 3, 11 \not\equiv 1 \pmod{16}$.

Om vi fortsätter på samma sätt så får vi.

(Överstruket innebär att $x_n^{\,2} \not\equiv 81 \pmod{2^n}$)

$81 \equiv 1 \pmod 2$	$x_1^{\,2} \equiv 1$	$x_1 = 1$
$81 \equiv 1 \pmod 4$	$x_2^{\,2} \equiv 1$	$x_2 = 1, 3$
$81 \equiv 1 \pmod 8$	$x_3^{\,2} \equiv 1$	$x_3 = 1, 5, 3, 7$
$81 \equiv 1 \pmod{16}$	$x_4^{\,2} \equiv 1$	$x_4 = 1, 9, \cancel{5}, \cancel{13}, \cancel{3}, \cancel{11}, 7, 15$
$81 \equiv 17 \pmod{32}$	$x_5^{\,2} \equiv 17$	$x_5 = \cancel{1}, \cancel{16}, 9, 25, 7, 23, \cancel{15}, \cancel{31}$
$81 \equiv 17 \pmod{64}$	$x_6^{\,2} \equiv 17$	$x_6 = 9, 41, \cancel{25}, \cancel{57}, \cancel{7}, \cancel{39}, 23, 55$
$81 \equiv 81 \pmod{128}$	$x_7^{\,2} \equiv 81$	$x_7 = 9, 73, \cancel{41}, \cancel{105}, \cancel{23}, \cancel{87}, 55, 119$

Vilket kan sammanfattas som ett träd.



Om det för en given lösning x_n alltid existerar en unik lösning x_{n+1} som uppfyller $x_{n+1} \equiv x_n \pmod{p^n}$ så är följden av lösningar oändlig.

Nästa exempel har inga rationella rötter men lösning i (mod 7^n) existerar.

Exempel

Vi ska lösa $x_n^{\,2} \equiv 2 \pmod{7^n}$ så att $0 \le x_n \le p^n - 1$ och $x_{n+1} \equiv x_n \pmod{p^n}$

Då $n = 1$: Så är $x_1 \equiv 3$ eller $x_1 \equiv -3 \equiv 4 \pmod{7}$.

$n = 2$:

Låt $x_2 = 3 + 7k$:

$(3+7k)^2 \equiv 2 \pmod{49}$

$9 + 2\times 3k \times 7 + 7^2 k^2 \equiv 2 \pmod{49}$; $7^2 k^2 \equiv 0 \pmod{49}$

$7 + 6k \times 7 \equiv 0 \pmod{49}$ dividera nu med 7

$1 + 6k \equiv 0 \pmod{7}$

$6k \equiv 6 \pmod{7}$

$k = 1$

Alltså $x_2 \equiv 10$ eller $x_2 \equiv -10 \equiv 39 \pmod{49}$.

$n = 3$:

Låt $x_3 = 10 + 7^2 k$:

$(10 + 7^2 k)^2 \equiv 2 \pmod{7^3}$; $7^3 = 343$

$98 + 2\times 10k \times 7^2 \equiv 0 \pmod{7^3}$ dividera nu med 7^2

$2 + 2\times 10k \equiv 0 \pmod{7}$

$2 \equiv -6k \pmod{7}$

$k = 2$

Alltså $x_3 \equiv 108$ eller $x_3 \equiv -108 \equiv 235 \pmod{7^3}$.

$n = 4$:

Låt $x_4 = 108 + 7^3 k$:

$(108 + 7^3 k)^2 \equiv 2 \pmod{7^4}$; $7^4 = 2401$

$11662 + 2\times 108k \times 7^3 \equiv 0 \pmod{7^4}$ dividera nu med 7^3

$6 + 6k \equiv 0 \pmod{7}$

$k = 6$

Alltså $x_4 \equiv 2166$ eller $x_4 \equiv -2166 \equiv 235 \pmod{7^4}$.

$n = 5$:

Låt $x_5 = 2166 + 7^4 k$:

$(2166 + 7^4 k)^2 \equiv 2 \pmod{7^5}$; $7^5 = 16807$

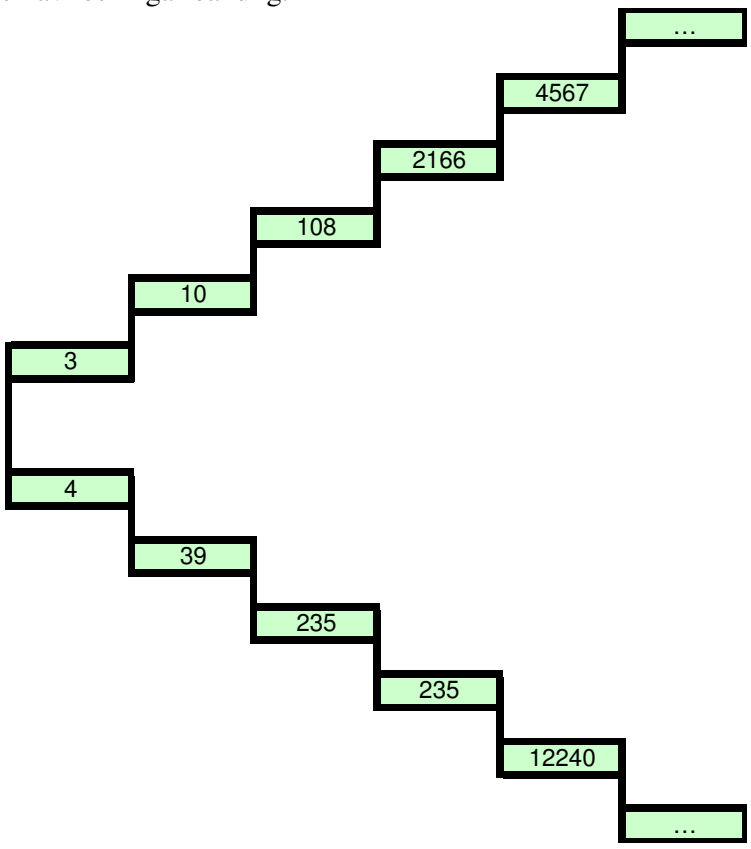
$2401 + 4332k \times 7^4 \equiv 0 \pmod{7^5}$ dividera nu med 7^4

$1 + 6k \equiv 0 \pmod{7}$

$k = 1$

Alltså $x_5 \equiv 4567$ eller $x_5 \equiv -4567 \equiv 12240$.

Vi ska nu visa att varje lösning hela tiden kommer att generera en ny unik lösning, alltså är följden av lösningar oändlig.



Sats 1.3.1

Om m$\in$ Z och $x^2 \equiv m \pmod{p}$ har lösning samt p $\neq 2$ och $p \nmid m$,
så är det möjligt att utvidga lösningen till en kongruent följd av lösningar av

$x_n^{\,2} \equiv \text{m} \pmod{p^n}$; $n = 1, 2, \ldots$

Bevis

För n = 1 har vi en lösning x_1 till $x_1^{\,2} \equiv \text{m} \pmod{p}$ enligt förutsättningarna.

Antag nu att $x_n^{\,2} \equiv m \pmod{p^n}$.

Då ska nästa lösning x_{n+1} uppfylla

$$x_{n+1} = x_n + kp^n \qquad 0 \le k < p$$

och $(x_{n+1})^2 \equiv \text{m} \pmod{p^{n+1}}$

då fås $(x_n + kp^n)^2 \equiv \text{m} \pmod{p^{n+1}}$

$x_n^{\,2} + 2x_n kp^n + k^2 p^{2n} \equiv \text{m} \pmod{p^{n+1}}$. ; $k^2 p^{2n} \equiv 0 \pmod{p^{n+1}}$

Alltså är $x_n^{\,2} + 2x_n kp^n \equiv \text{m} \pmod{p^{n+1}}$

$2x_n kp^n \equiv \text{m} - x_{\text{n}}^{\,2} \pmod{p^{n+1}}$

Eftersom $x_n^{\,2} \equiv m \pmod{p^n}$ så finns det ett heltal l

så att $2x_n kp^n = lp^n$

Dividera nu med p^n

$2x_n k \equiv l \pmod{p}$.

Då $2x_n \not\equiv 0 \pmod{p}$ så finns ett unikt $k \in [0, p-1]$ som löser $2x_n k \equiv l \pmod{p}$
och därmed har vi funnit ett unikt x_{n+1} så att

$x_{n+1}^{\,2} \equiv m \pmod{p^n}$ och $x_{n+1} \equiv x_n \pmod{p^n}$

Då *p=2* medför det lite problem eftersom man får

$$x_n^{\,2} + \underbrace{2x_n}_{\equiv 0} k2^n \equiv m \pmod{2^{n+1}}$$

vilket blir $x_n^{\,2} \equiv m \pmod{2^{n+1}}$

Alltså kommer *k* ej att vara unikt. Det kommer antingen att fungera för alla *k* eller inget.
Det inträffar ibland att det finns lösningar *(mod* p^n*)* som ej går att ”lyfta” till *(mod* p^{n+1}*)*.

Nedan följer ett exempel på hur det kan se ut då *p=2*.

Exempel

Vi ska nu lösa $x_n^{\,2} \equiv 17 \pmod{2^n}$ då $0 \le x_n \le 2^n - 1$ $x_{n+1} \equiv x_n \pmod{2^n}$.

$n = 1 \pmod 2$ 1

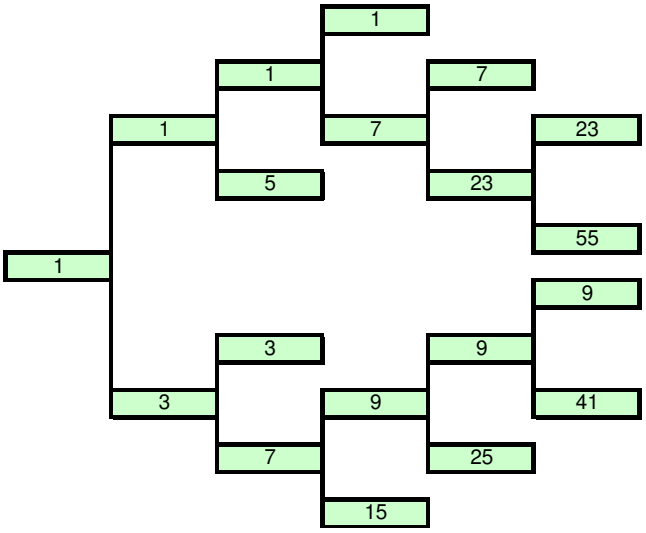
$n = 2 \pmod 4$ 1, 3

$n = 3 \pmod 8$ 1, 5, 3, 7

$n = 4 \pmod{16}$ 1, 9, ~~5~~, ~~13~~, 3, ~~11~~, 7, 15

$n = 5 \pmod{32}$ ~~1~~, ~~17~~, 9, 25, 7, 23, ~~15~~, ~~31~~

$n = 6 \pmod{64}$ 9, 41, ~~25~~, ~~57~~, ~~7~~, ~~39~~, 23, 55



Som ett tidigare exempel visade så finns det lösningar (mod p^n) som ej är rationella lösningar, på samma sätt finns det lösningar för ekvationer som saknar lösning i Q, i kroppen Q_p.
Alltså är vissa p-adiska tal inte (utvecklade från) rationella tal.

Vi ska nu visa att alla p-adiska tal inte är utvecklade ifrån rationella tal.
För enkelhetens skull tar vi $p \ge 7$.

Om m (ej delbart med p) är ett heltal så vet vi från Sats 1.3.1 att varje heltalslösning x till kongruensen

$x^2 \equiv m \pmod p$ ger en lösning då $x \in Q_p$ till $x^2 = m$.

Vi kan nu titta på den ändliga kroppen F_p.

Det gäller att $\left|F_p^{\,*}\right| = p - 1$

$F_p^{\,*} \cong Z/(p-1)Z$; Z_{p-1} cyklisk jämn ($p \ne 2$) grupp

Isomorfin har egenskapen att de jämna elementen i Z_{p-1} motsvarar de m $(0<m\leq p-1)$ som är sådana att $x^2 \equiv m \pmod{p}$ har en lösning.

Alltså finns det $\frac{p-1}{2}$: *st* m sådana att kongurensen $x^2 \equiv m \pmod{p}$ har en lösning.

Däremot finns endast $\left\lfloor \sqrt{p-1} \right\rfloor$: *st* m $(0 < m \leq p-1)$ sådana att $x^2 = m$ har lösning $x \in Q$.

Nu är $\frac{p-1}{2} > \left\lfloor \sqrt{p-1} \right\rfloor$ för $p \geq 7$,

så det finns fler m som har lösning till $x^2 \equiv m \pmod{p}$ än som har rationell lösning till $x^2 = m$.
När vi har hittat ett m som inte är en kvadrat (rationell lösning) men som har lösning $x_1 \equiv m \pmod{p}$ så kan vi med hjälp av Sats 1.3.1 konstruera en koherent följd (ett p-adiskt tal), alltså en lösning $x \in Q_p$ till $x^2 = m$, men vi har valt m så att $x^2 = m$ ej har lösning i Q.
Vissa p-adiska tal är således inte (utvecklade från) rationella tal. Detta följer också av att rationella tal har periodisk p-adisk utveckling (Lemma 1.2.1).

Vi ser nedan är att för p=3 och 5 så finns det lika många m $(0<m\leq p-1)$ så att ekvationen $x^2=m$ har lösning i Q_p som i Q, men då p>5 så finns det fler m som har lösning i Q_p än i Q.

	Lösningar i Q_p.	Lösningar i Q.	
	$\frac{p-1}{2}$	$\left\lfloor \sqrt{p-1} \right\rfloor$	
	$m = x^2$	$m = x^2$	
$p = 3 \pmod 3$	$1 \equiv 1^2 = 2^2$	$1 = 1^2$	;1 lösn i vardera
$p = 5 \pmod 5$	$1 \equiv 1^2 = 4^2$	$1 = 1^2$	;2 lösn i vardera
	$4 \equiv 2^2 = 3^2$	$4 = 2^2$	
$p = 7 \pmod 7$	$1 \equiv 1^2 = 6^2$	$1 = 1^2$	;3 lösn i Q_7, 2 i Q
	$2 \equiv 3^2 = 4^2$	$4 = 2^2$	
	$4 \equiv 2^2 = 5^2$		

Att det finns fler lösningar i Q_p än i Q gäller även för fallen då *p=2, 3, och 5,* man måste bara titta på kongurenser modulo högre potenser av p.
Att $\sqrt{2} \in Q_7$ kan visas på följande sätt :

$x_1^{\,2} \equiv 2 \pmod 7$

har lösning $x_1 = 3 \text{ eller } 4$; ty $3^2 \equiv 4^2 \equiv 2 \pmod 7$.

När vi har hittat en lösning för $x_1^{\,2} \equiv 2 \pmod 7$,

så säger Sats 1.3.1 att det finns en lösning för $\alpha^2 = 2$ i Q_7.

Till en given ekvation kan man på samma sätt se att för ett visst p så existerar lösning och för ett annat p så saknas lösning.

Exempel

Vi visar att $x^2 + 1 = 0$ har lösning i Q_5 men saknar lösning i Q_7.

Q_5 :

$x_1^{\,2} + 1 \equiv 0 \pmod 5$

$x_1^{\,2} \equiv 4 \pmod 5$ ger att $x_1 \equiv 2$ eller $x_1 \equiv 3$. Lösning existerar.

Q_7 :

$x_1^{\,2} + 1 \equiv 0 \pmod 7$

$x_1^{\,2} \equiv 6 \pmod 7$ saknar lösning x_1. Lösning existerar ej.

Eftersom det för varje p existerar en ekvation där det saknas lösning i Q_p, så kan man säga att: Q_p aldrig är algebraiskt sluten.

Bevis

Betrakta ekvationen $x^2 = m \quad x \in Q_p$

vi vill visa att det finns heltal m $(0 \le m < p)$ så att denna ekvation saknar lösning.

Eftersom det p - adiska talet ser ut på följande sätt

$$x = a_0 + a_1 p + a_2 p^2 + \ldots$$

så ger $x^2 \equiv m \pmod p$

att $a_0^{\,2} \equiv m \pmod p$.

Om detta saknar lösning, så saknas även lösning i Q_p.

Exempel

Vi undersöker om $x^2 = 3$ har lösning i Q_5.

Genom att helt enkelt söka lösning för $x_1^{\,2} \equiv 3 \pmod 5$

vilket visar sig vara omöjligt då $1^2 \equiv 1 \pmod 5$

$2^2 \equiv 4$

$3^2 \equiv 4$

$4^2 \equiv 1$

Alltså saknas lösning i Q_5.

2. Förberedelser för att kunna räkna p-adiska tal

I det här kapitlet kommer vi se att en annorlunda valuation av rationella tal ger ett så kallat icke-arkimediskt absolutbelopp samt en annan metrik än den vi är vana vid, en ultrametrik.

Huvudidén är att introducera annorlunda funktioner för absolutbelopp på kroppen av rationella tal och sedan komplettera Q med avseende på den uppkomna topologin.
Vi vill använda vårt nya icke-arkimediska absolutbelopp för att på ett alternativt sätt mäta ”storleken” på saker och ting.
Med vårt nya absolutbelopp kommer vi att förstå påståendet:
I kroppen Q_3 så är avståndet mellan 1 och 2, större än avståndet mellan 1 och 100.

2.1 Absolutbelopp på en kropp

Låt F vara en kropp och låt $R_+ = \{x \in R : x \geq 0\}$.

Vi börjar med att definiera vad ett absolutbelopp på F är.

Definition 2.1.1:
Ett absolutbelopp på F är en funktion

$$|\ |: F \to R_+$$

som uppfyller följande villkor :

i) $|x| = 0$ omm $x = 0$

ii) $|xy| = |x||y| \quad \forall\, x, y \in F$

iii) $|x + y| \leq |x| + |y| \quad \forall\, x, y \in F$

Vi kallar ett absolutbelopp på F icke - arkimediskt om det även uppfyller

iv) $|x + y| \leq Max\{|x|, |y|\} \quad \forall\, x, y \in F$

Annars är absolutbeloppet arkimediskt.

Det triviala absolutbeloppet.
Sätt $|x| = 1$ om $x \neq 0$ och $|0| = 0$.
Detta fungerar på alla kroppar F och definierar ett icke-arkimediskt absolutbelopp som kallas det triviala absolutbeloppet.

Ändliga kroppar
För ändliga kroppar är hela teorin trivial.

Påstående:
Om F är en ändlig kropp, så är det enda absolutbeloppet på denna kropp det triviala absolutbeloppet.

Bevis:

$|0| = 0$ enl. def.

$1 = 1 \times 1 \quad \Rightarrow \quad |1| = |1| \times |1|$

Eftersom $|1|$ är strikt positivt så är $|1| = 1$.

Låt $x \in F \quad x \neq 0$. Eftersom F är ändlig och q är antal element i F.

Då är $x^q = x$ (se boken Algebraiska strukturer), så

$|x|^q = |x^q| = |x| \quad \Leftrightarrow \quad |x| = 1$

Alltså är absolutbeloppet trivialt. VSB

Vi ska nu definiera funktionen v_p som vi kommer att använda ofta i våra absolutbelopp.

Definition 2.1.2

Tag ett primtal p. Den p - adiska valuationen på Z är funktionen

$v_p : Z - \{0\} \to R$ som definieras på följande sätt.

Tag $n \in Z, n \neq 0$, låt $v_p(n)$ vara det unika positiva heltal som uppfyller

$n = p^{v_p(n)} n' \quad p \nmid n'$.

Vi utvidgar v_p till kroppen av rationella tal som följer :

Om $x = a/b \in Q \ (x \neq 0) \ a, b \in Z$ så sätter vi

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

Innan vi visar att detta är väldefinierat så räknar vi några exempel.

Exempel

$v_5(400)$

Eftersom $400 = 4 \times 100 = 2^2 \times 10^2 = 2^2 \times 2^2 \times 5^2 = 2^4 \times 5^2 = 5^2 \times 16$

så är $v_5(400) = 2$

$v_5(-400)$

Eftersom $-400 = 5^2 \times (-16)$

så är $v_5(-400) = 2$

$v_7(15) = 0$

$v_5(180/3) = v_5(60)$

$60 = 12 \times 5$

$v_5(180/3) = 1$

Alternativt räknar vi detta på följande sätt

$v_5(180/3)$

$180 = 18 \times 2 \times 5 = 36 \times 5$

$3 = 5^0 \times 3$

$v_5(180/3) = 1 - 0 = 1$

Lemma 2.1.3

För alla $x,\ y \in Z$ gäller :

$v_p(xy) = v_p(x) + v_p(y)$

Bevis

Låt $x,\ y$ vara heltal.

Låt $x = p^a x'$ där $a = v_p(x)$ och $p \nmid x'$

och $y = p^b y'$ där $b = v_p(y)$ och $p \nmid y'$.

Då är $xy = p^a x' p^b y' = p^{a+b} x'y'$ med $p \nmid x'y'$ så

$v_p(xy) = v_p(p^{a+b} x'y') = a + b = v_p(x) + v_p(y).$ VSB

Sats 2.1.4

Om $x \in Q$ så beror inte $v_p(x)$ på representationen av kvoten för två heltal, alltså om $a/b = c/d$ så är $v_p(a) - v_p(b) = v_p(c) - v_p(d)$.

Bevis :

Låt $a/b = c/d \quad \Leftrightarrow \quad ad = bc \ ; b, d \neq 0$

$v_p(ad) = v_p(a) + v_p(d) \qquad v_p(bc) = v_p(b) + v_p(c).$

Om $ad = bc$ så är $v_p(ad) = v_p(bc)$ så

$v_p(a) + v_p(d) = v_p(b) + v_p(c).$

Alltså $v_p(a) - v_p(b) = v_p(c) - v_p(d).$ VSB

Exempel

$27/3 = 36/4 \quad \Leftrightarrow \quad 27 \times 4 = 3 \times 36$

$v_3(27 \times 4) = v_3(27) + v_3(4) = 3 + 0 = 3$

$v_3(3 \times 36) = v_3(3) + v_3(36) = 1 + 2 = 3$

Alltså $v_3(27) - v_3(3) = v_3(36) - v_3(4) \quad \Leftrightarrow \quad 3 - 1 = 2 - 0$

Den p - adiska valuationen för alla $x \in Q$ bestäms av :

$$x = p^{v_p(x)} \times \frac{a}{b} \text{ om } p \nmid ab.$$

Grundegenskaperna för den p-adiska valuationen v_p är som följer.

Lemma 2.1.5

För alla $x,\ y \in Q$ gäller :

i) $v_p(xy) = v_p(x) + v_p(y)$

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

Bevis

Till att börja med låter vi $x,\ y \in Z$.

Låt $x = p^a x'$ $\quad a = v_p(x)$ $\quad p \nmid x'$

och $y = p^b y'$ $\quad b = v_p(y)$ $\quad p \nmid y'$.

Antag att $a \leq b$.

i) Har visats tidigare (Lemma 2.1.3).

ii) Då är $x + y = p^a x' + p^b y' = p^a (x' + p^{b-a} y')$

$$v_p(x+y) = v_p(p^a(x' + p^{b-a}y')) = a + \underbrace{v_p(x' + p^{b-a}y')}_{\geq 0 \text{ ty } b \geq a} \geq a.$$

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

Om nu $x = t/q$ och $y = r/s$ $\quad t, q, r, s \in Z$.

i) Då är $v_p(xy) = v_p(tr/qs) = v_p(tr) - v_p(qs) = v_p(t) + v_p(r) - v_p(q) - v_p(s) =$

$= v_p(t) - v_p(q) + v_p(r) - v_p(s) = v_p(t/q) + v_p(r/s) = v_p(x) + v_p(y).$

Alltså $v_p(xy) = v_p(x) + v_p(y)$. VSB

ii) $v_p(x+y) = v_p\left(\frac{t}{q} + \frac{r}{s}\right) = v_p\left(\frac{st+qr}{qs}\right) = v_p(st+qr) - v_p(qs) \geq$

$\geq \min\{v_p(st),\ v_p(qr)\} - v_p(qs) = \min\{v_p(s) + v_p(t),\ v_p(q) + v_p(r)\} - v_p(q) - v_p(s) =$

$= \min\{v_p(t) - v_p(q),\ v_p(r) - v_p(s)\} = \min\{v_p(t/q),\ v_p(r/s)\} =$

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

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

Exempel

$v_3(18\times135) = v_3(18) + v_3(135) = 2 + 3 = 5$

$18 = 3^2 \times 2$

$135 = 3^3 \times 5$

$\text{Kontroll}: 18\times135 = 2430$

$v_3(2430) = 5$

$2430 = 3^5 \times 10$

$v_3(18+135) = v_3(153) = 2$

$153 = 3^2 \times 17$

$v_3(18) = 2$

$v_3(135) = 3$

Alltså $v_3(153) = v_3(18+135) = 2 \geq \min\{v_3(18), v_3(135)\}$

Definition 2.1.6

För alla $x \in Q$ definieras det p - adiska absolutbeloppet av x som

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

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

Exempel

$|35|_7 \qquad v_7(35) = 1 \qquad ;35 = 7^1 \times 5$

$|35|_7 = 7^{-1} = 1/7$

$|56/12|_7 \qquad v_7(56) = 1 \qquad v_7(12) = 12 \qquad ;56 = 7^1 \times 8 \qquad 12 = 7^0 \times 12$

$|56/12|_7 = 7^{-(1-0)} = 7^{-1} = 1/7$

$|177553|_7 \qquad v_7(177553) = 0$

$|177553|_7 = 7^{-0} = 1$

$|3/686|_7 \qquad v_7(3) = 0 \qquad v_7(686) = 3 \qquad ;686 = 7\times98 = 7\times7\times14 = 7^3 \times 2$

$v_7(3/686) = v_7(3) - v_7(686) = 0 - 3 = -3$

$|3/686|_7 = 7^{-(-3)} = 7^3 = 343$

Notera vad det p-adiska absolutbeloppet egentligen gör, är att på ett ganska konstigt sätt mäta hur pass delbart talet x är med p.
När x är ”mycket” delbart med p så blir absolutbeloppet litet (”-” i exponenten).
När x är ”lite” delbar med p så blir absolutbeloppet stort.

Exempel

$\left|p^n\right|_p \to 0$ då $n \to \infty$

Detta beror på att vi definierat det p - adiska absolubeloppet som

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

som i detta fall blir

$\left|p^n\right|_p = p^{-v_p(p^n)} = p^{-n} \to 0$ då $n \to \infty$.

Av det följande exemplet kan man se att det 3-adiska avståndet mellan 1 och 2 är längre än det 3-adiska avståndet mellan 1 och 100.

Exempel

$\left|2-1\right|_3 = \left|1\right|_3 = 1$;$1 = 3^0 \times 1$

$\left|10-1\right|_3 = \left|9\right|_3 = 1/9$;$9 = 3^2$

$\left|100-1\right|_3 = \left|99\right|_3 = \left|11\times 9\right| = 1/9$

$\left|101-1\right|_3 = \left|100\right|_3 = 1$

Sats 2.1.7

Man kan definiera ett icke - arkimediskt absolutbelopp på Q,

för alla $c \in R,\ c > 1$ genom

$|x| = c^{-v_p(x)} \qquad x \neq 0$

$|0| = 0.$

Bevis

Låt x, y vara rationella tal $\qquad x, y \neq 0 \qquad$ (då $x, y = 0$ är trivialt visas ej).

Vi behöver visa att

$$|x + y| \leq \max\{|x|, |y|\}.$$

Vi har $|x| = c^{-v_p(x)} \qquad |y| = c^{-v_p(y)}$

och $\qquad |x + y| = c^{-v_p(x+y)}.$

Enligt Lemma 2.1.5 har vi att

$$v_p(x + y) \geq \min\{v_p(x), v_p(y)\} \quad \text{så} \quad c^{-v_p(x+y)} \leq c^{-\min\{v_p(x), v_p(y)\}}.$$

Antag att $|x| \geq |y| \quad$ då $\quad c^{-v(x)} \geq c^{-v_p(y)} \quad$ så $\quad v_p(x) \leq v_p(y)$

dvs. $\quad c^{-\min\{v_p(x), v_p(y)\}} = c^{-v(x)} = |x|.$

Alltså $|x + y| \leq \max\{|x|, |y|\}.$

Vi visar nu att villkor *ii)* i definition 2.1.1 är uppfyllt med hjälp av Lemma 2.1.5.

Alltså att $|xy| = |x||y|.$

Enligt Lemma 2.1.5 har vi att

$v_p(xy) = v_p(x) + v_p(y)$

vilket ger oss att

$|xy| = c^{-v_p(xy)} = c^{-(v_p(x)+v_p(y))} = c^{-v_p(x)} \times c^{-v_p(y)} = |x||y|.$ VSB

Notera att c inte spelar någon roll så länge som det är större än 1.

Man väljer lämpligen c som primtalet p, för då kommer den viktiga produktformeln (som vi kommer att visa längre fram) att gälla.

2.2 Icke-arkimediskt absolutbelopp

Här kommer vi att titta lite på basegenskaperna, samt att förklara den icke-arkimediska egenskapen $|x+y| \le \max\{|x|,|y|\}$.

Låt F vara en kropp och $|\ |$ är ett icke-trivialt absolutbelopp på F.

Lemma 2.2.1

För alla absolutbelopp $|\ |$ på alla kroppar F, gäller :

i) $|1| = 1.$

ii) om $x \in F$ och $|x^n| = 1$, så är $|x| = 1.$

iii) $|-1| = 1.$

iv) för alla $x \in F$, $|-x| = |x|.$

v) om F är en ändlig kropp, så är $|\ |$ trivialt.

Bevis

i) $|1| = |1^2| = |1|^2 = 1.$

ii) Eftersom $|x^n| = |x|^n$ så är $|x| = 1$ om $|x^n| = 1.$

iii) Sätt $n = 2,\ x = -1:$ Enligt *ii*) är $|(-1)^2| = |1| = 1$ alltså $|-1| = |1|.$

iv) $|-x| = |-1| \times |x| = |x|.$

v) Låt q vara antal element i F då har vi $x^{q-1} = 1$ då $x \neq 0,$

använder vi oss sedan av *ii*) så ser vi att $|x^{q-1}| = 1$ vilket ger att $|x| = 1$ alltså $|\ |$ är trivialt.

Satsen som följer ger ett nödvändigt och tillräckligt villkor för att ett absolutbelopp ska vara icke-arkimediskt.

Sats 2.2.2

Låt $A \subset F$ vara bilden av Z i F. Ett absolutbelopp $|\ |$ på F är icke - arkimediskt omm $|a| \leq 1$ för alla $a \in A$.

Speciellt är ett absolutbelopp på Q icke - arkimediskt omm $|n| \leq 1\ \forall n \in Z$.

Bevis (Vi följer här boken p-adic numbers)

Eftersom $|\pm 1| = 1$ alltid gäller, kan vi säga att om $|\ |$ är icke - arkimediskt så får vi

$|a \pm 1| \leq \max\{|a|, 1\}$,

induktivt följer att $|a| \leq 1$ för alla $a \in A$.

Vi vill nu visa att för alla $x,\ y \in F$ har vi

$|x + y| \leq \max\{|x|, |y|\}$ dela med $|y|$ $y \neq 0$, (om $y = 0$ så är påståendet uppenbart) och vi får

$\left|\frac{x}{y} + 1\right| \leq \max\left\{\left|\frac{x}{y}\right|, 1\right\}$ vi behöver nu endast visa att

$|x + 1| \leq \max\{|x|, 1\}$ låt m vara ett positivt heltal

$|x+1|^m = \left|\sum_{k=0}^{m} \binom{m}{k} x^k\right| \leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |x^k|$ eftersom $\binom{m}{k}$ är ett heltal och $\left|\binom{m}{k}\right| \leq 1$ så

$|x+1|^m \leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |x^k| \leq \sum_{k=0}^{m} |x|^k \leq (m+1) \max\{1, |x|^m\}$

Vi tar nu m : te roten ur på bägge sidor och får

$|x + 1| \leq \sqrt[m]{(m+1)} \max\{1, |x|\}$. Denna olikhet gäller för alla positiva heltal m oavsett hur stora dessa är.

Nu är $\lim_{m \to \infty} \sqrt[m]{m+1} = 1$ så om vi låter $m \to \infty$ får vi att $|x + 1| \leq \max\{|x|, 1\}$,

vilket medför att $|\ |$ är icke - arkimediskt.

2.3 Topologi

Vi ska nu använda vårt ”nya” absolutbelopp till att mäta avstånd, vilket kommer att resultera i något som kallas det ultrametriska rummet. I detta rum kommer vi att se att topologin är lite annorlunda än den vi är vana vid, bl.a. att en öppen mängd även är sluten och tvärtom, samt att den starkare alltid vinner!

Vi börjar dock med att definiera avstånd.

Definition 2.3.1

Låt F vara en kropp och $|\ |$ vara ett absolutbelopp på F.

Vi definierar avståndet $d(x,\ y)$ mellan två element $x,\ y \in F$ genom

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

$d(x,\ y)$ har följande egenskaper :

i) $\forall x,\ y \in F, \quad d(x,\ y) \geq 0$ och $d(x,\ y) = 0$ omm $x = y$.

ii) $\forall x,\ y \in F, \quad d(x,\ y) = d(y,\ x)$.

iii) $\forall x,\ y,\ z \in F, \quad d(x,\ z) \leq d(x,\ y) + d(y,\ z)$.

Bevis

i) Avståndet $d(x,\ y) = |x - y| > 0$ då x ≠ y

och $d(x,\ y) = |x - y| = 0$ endast då $x = y$.

ii) $d(x,\ y) = d(y,\ x) \quad \Leftrightarrow$

$|x - y| = |y - x| \quad \Leftrightarrow \quad |x - y| = |-(x - y)| \quad \Leftrightarrow \quad |x - y| = |x - y|$.

iii) $d(x,\ z) \leq d(x,\ y) + d(y,\ z)$,

inses mha. triangelolikheten $|x - z| = |x - y + y - z| \leq |x - y| + |y - z|$.

2.3.1 Ultrametriskt rum

Vid en första anblick verkar vissa satser i det ultrametriska rummet vara ganska konstiga. I detta rum används en annan metrik än den vanliga euklidiska, en så kallad ultrametrik eller även kallad icke-arkimedisk metrik.

Det icke-arkimediska absolutbeloppet kan även uttryckas som:

Lemma 2.3.1.1

Låt $|\ |$ vara ett absolutbelopp på kroppen F och definiera

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

så är $|\ |$ icke - arkimediskt om och endast om för alla $x,\ y,\ z \in F$ då

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

Bevis

Antag att $d(x,\ y) \le \max\{d(x,\ z),\ d(z,\ y)\}$ då är

$|x - y| = d(x,\ y) \le \max\{d(x,\ 0),\ d(y,\ 0)\} = \max\{|x - 0|,\ |y - 0|\} = \max\{|x|,\ |y|\}.$

Antag att $|\ |$ är icke - arkimediskt

$d(x,\ y) = |x - y| = [(x - z) + (z - y)] \le \max\{|x - z|,\ |z - y|\} = \max\{d(x,\ z),\ d(z,\ y)\}.$ VSB

Notera att ett icke - arkimediskt absolutbelopp uppfyller $|x + y| \le \max\{|x|,\ |y|\}$, men om $|x| \ne |y|$, låt oss anta att $|x| > |y|$.

Då är $|x + y| \le \max\{|x|,\ |y|\} = |x|$ men

$x = (x + y) - y$ så $|x| \le \max\{|x + y|,\ |y|\}$ då $|x| > |y|$ så måste $|x| \le |x + y|$.

Men från den första olikheten har vi att

$|x + y| \le |x|$

olikheterna tillsammans blir då

$|x + y| \le |x| \le |x + y|$ alltså $|x + y| = |x|$

Slutsats : Om $|x| \ne |y|$ så är $|x + y| = \max\{|x|,\ |y|\}$

Vi ska nu se att operationerna addition, multiplikation och inversen på kroppen *F* är kontinuerliga med avseende på *d(x, y)*.

i) Vi ska nu visa att addition är en kontinuerlig funktion.

Tag $x_0,\ y_0 \in F$. Vi ska nu visa att för alla $\varepsilon > 0$ så existerar ett $\delta_\varepsilon > 0$ så att om $d(x,\ x_0) < \delta_\varepsilon$ och $d(y,\ y_0) < \delta_\varepsilon$ så är $d(x + y,\ x_0 + y_0) < \varepsilon$.

Sätt $\delta_\varepsilon := \varepsilon/2$. Då är

$$d(x + y,\ x_0 + y_0) = |(x + y) - (x_0 + y_0)| = |x - x_0 + y - y_0| \le |x - x_0| + |y - y_0| \le$$

$$\le \delta_\varepsilon + \delta_\varepsilon = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

ii) Vi ska nu visa att multiplikation är en kontinuerlig funktion.

Tag $x_0,\ y_0 \in F$. Vi ska nu visa att för alla $\varepsilon > 0$ så existerar ett $\delta_\varepsilon > 0$ så att om $d(x,\ x_0) < \delta_\varepsilon$ och $d(y,\ y_0) < \delta_\varepsilon$ så är $d(xy,\ x_0 y_0) < \varepsilon$.

Sätt $\delta_\varepsilon := \min\left\{\sqrt{\varepsilon/2},\ \frac{\varepsilon}{2(|x_0| + |y_0|)}\right\}$. Då är

$$d(xy,\ x_0 y_0) = |xy - x_0 y_0| = |xy - xy_0 + xy_0 - x_0 y_0| = |x(y - y_0) + y_0(x - x_0)| \le$$

$$\le |x|\,|y - y_0| + |y_0|\,|x - x_0| = |(x - x_0) + x_0|\,|y - y_0| + |y_0|\,|x - x_0| \le$$

$$\le |x - x_0|\,|y - y_0| + |x_0|\,|y - y_0| + |y_0|\,|x - x_0| \le \delta_\varepsilon\,\delta_\varepsilon + |x_0|\delta_\varepsilon + |y_0|\delta_\varepsilon =$$

$$= \delta_\varepsilon^{\,2} + (|x_0| + |y_0|)\delta_\varepsilon < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

iii) Vi ska nu visa att invers är en kontinuerlig funktion.

Tag $x_0,\ y_0 \in F$. Vi ska nu visa att för alla $\varepsilon > 0$ så existerar ett $\delta_\varepsilon > 0$ så att om $d(x, x_0) < \delta_\varepsilon$ så är $d(1/x, 1/x_0) < \varepsilon$.

Sätt $\delta_\varepsilon := \min\left\{\frac{\varepsilon|x_0|}{2}, \frac{\varepsilon|x_0|^2}{2}\right\}$. Då är

$$d\left(1/x, 1/x_0\right) = \left|\frac{1}{x} - \frac{1}{x_0}\right| = \left|\frac{x_0 - x}{x\,x_0}\right| = \frac{|x - x_0|}{|x_0||x|} \le \frac{|x - x_0|}{|x_0|\,\big||x_0| - |x - x_0|\big|} \le \frac{|x - x_0|}{|x_0|\frac{|x_0|}{2}} =$$

$$= \frac{2}{|x_0|^2}|x - x_0| \le \frac{2}{|x_0|^2}\delta_\varepsilon \le \varepsilon.$$

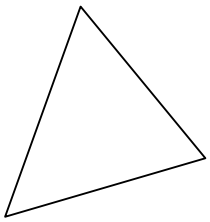
I ett ultrametriskt rum är alla ”trianglar” likbenta.

Låt $x,\ y,\ z \in$ det *ultrametriska rummet*

då är $d(x, y) = |x - y|$

$d(y, z) = |y - z|$

$d(x, z) = |x - z|$



Om $|x - y| \neq |y - z|$ då är $|x - z|$ lika med den större av de två,

dvs. $|x - z| = \max\{|x - y|, |y - z|\}$ då $|x - y| \neq |y - z|$.

Man kan alltså säga att "Den starkare vinner!"

Att ”den starkare alltid vinner” visas nedan, dvs. de två längsta sidorna är alltid lika.

(Vi följer här boken p-adic numbers)

Låt $v_p(x) = n$ och $v_p(y) = m$,

då är $x = p^n x'$ $\quad y = p^m y'$ $\quad p \nmid x'y'$.

Alltså $|x| = p^{-n}$ $\quad |y| = p^{-m}$.

Vi kan anta att $|x| \ge |y|$ (annars byter vi x och y).

i) Fallet $|x| > |y|$.

Då $n < m$, låt $m = n + \varepsilon$, $\varepsilon > 0$, (ε heltal) vilket ger att

$x + y = p^n x' + p^{n+\varepsilon} y' = p^n\left(x' + p^\varepsilon y'\right)$.

Eftersom $p \nmid x'$ så $p \nmid \left(x' + p^\varepsilon y'\right)$

vilket ger att $v_p(x + y) = n$.

Alltså $|x + y| = p^{-n} = |x|$.

ii) Fallet $|x| = |y|$.

Då $n = m$ vilket ger att

$x + y = p^n(x' + y')$ $p \nmid x'$ eller y' men p kan dela $(x' + y')$ så

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

Alltså $|x + y| \leq \max\{|x|, |y|\} = |x| = |y|$.

Notera att i bägge fallen är två av de tre absolutbeloppen $|x|, |y|, |x + y|$ lika

i fallet i) är $|x| = |x + y|$ och

i fallet ii) är $|x| = |y|$.

Även exemplet nedan illustrerar att den starkare alltid vinner!

Exempel

Ge Q den 5-adiska topologin. Ta en triangel med hörnen i

$\left.\begin{array}{l} x = 2/15 \\ y = 1/5 \\ z = 7/15 \end{array}\right\}$ då är dess sidor *d(x,y), d(y,z)* och *d(x,z).*

Avståndet mellan x och y är $d(x, y) = |x - y|_5 = \left|\frac{2}{15} - \frac{1}{5}\right|_5 = \left|\frac{-1}{15}\right|_5 = 5^{-v_p(-1/15)}$

$v_5\left(\frac{-1}{15}\right) = 0 - 1 = -1$; Ty $\frac{-1}{15} = \frac{-1 \times 5^0}{3 \times 5}$

vilket ger $d(x, y) = 5^{-v_5(-1/15)} = 5^{-(-1)} = 5,$

på samma sätt blir $d(y, z) = |y - z|_5 = \left|\frac{1}{5} - \frac{7}{15}\right|_5 = \left|\frac{-4}{15}\right|_5 = 5^{-v_5(-4/15)} = 5^{-(-1)} = 5$

och $d(x, z) = |x - z|_5 = \left|\frac{2}{15} - \frac{7}{15}\right|_5 = \left|\frac{-1}{3}\right|_5 = 5^{-v_5(-1/3)} = 5^{-(0)} = 1.$

Alltså 2 sidor har längden 5 ; Den starkare vinner!

1 sida har längden 1

2.3.2 Öppna och slutna bollar

Om vi nu istället för trianglar tittar på bollar kommer vi att se att även dessa är lite annorlunda i det ultrametriska rummet.

Definition 2.3.2.1

Låt F vara en kropp med ett absolutbelopp $|\ |$.

Låt $a \in F$ (centrum), $r \in R_+$ (radie).

Öppen boll :

$B(a,r) = \{x \in F : d(x,a) < r\} = \{x \in F : |x-a| < r\}$.

Sluten boll :

$\overline{B}(a,r) = \{x \in F : d(x,a) \le r\} = \{x \in F : |x-a| \le r\}$.

Detta är standarddefinitioner för alla metriska rum.

Egenskaper för ett icke-arkimediskt absolutbelopp.

i) Om $b \in B(a,r)$ så är $B(a,r) = B(b,r)$

dvs. alla punkter i en öppen boll, är center i den bollen.

Bevis

Antag att $b \in B(a,r)$, då är $|b-a| < r$.

Tag nu en annan punkt $x \in B(a,r)$, då är $|x-a| < r$.

Den icke - arkimediska egenskapen säger att

$|x-b| \le \max\{|x-a|, |b-a|\} < r$

$|x-b| < r$ så $x \in B(b,r)$.

Alltså $B(a,r) \subset B(b,r)$.

Låt nu istället $x \in B(b,r)$, då är $|x-b| < r$.

Den icke - arkimediska egenskapen säger att

$|x-a| \le \max\{|x-b|, |b-a|\} < r$ så

$|x-a| < r$ så $x \in B(a,r)$.

Alltså $B(b,r) \subset B(a,r)$.

Slutsats : $B(a,r) = B(b,r)$. VSB

ii) Om $b \in \overline{B}(a,r)$ så är $\overline{B}(a,r) = \overline{B}(b,r)$

dvs. alla punkter i en sluten boll, är center i den bollen.

Bevis

Antag att $b \in \overline{B}(a,r)$, då är $|b-a| \le r$.

Tag nu en annan punkt $x \in \overline{B}(a,r)$, då är $|x-a| \le r$.

Den icke - arkimediska egenskapen säger att

$|x-b| \le \max\{|x-a|, |b-a|\} \le r$

$|x-b| \le r$ så $x \in \overline{B}(b,r)$.

Alltså $\overline{B}(a,r) \subset \overline{B}(b,r)$.

Låt nu istället $x \in \overline{B}(b,r)$, då är $|x-b| \le r$.

Den icke - arkimediska egenskapen säger att

$|x-a| \le \max\{|x-b|, |b-a|\} \le r$ så

$|x-a| \le r$ så $x \in \overline{B}(a,r)$.

Alltså $\overline{B}(b,r) \subset \overline{B}(a,r)$.

Slutsats : $\overline{B}(a,r) = \overline{B}(b,r)$. VSB

iii) Den öppna bollen $B(a,r)$ är både öppen och sluten.

Bevis

Tag ett x på randen av $B(a,r)$,

tag nu ett s så att $0 < s < r$ och betrakta den öppna bollen $B(x,s)$.

Eftersom x är en randpunkt är

$B(a,r) \cap B(x,s) \neq \emptyset$

därför existerar ett $y \in B(a,r) \cap B(x,s)$

$|y-a| < r$ och $|y-x| < s < r$.

Den icke - arkimediska egenskapen ger

$|x-a| \le \max\{|x-y|, |y-a|\} < \max\{s,r\} = r$.

Alltså $x \in B(a,r)$.

Eftersom alla randpukterna i $B(a,r)$ tillhör

$B(a,r)$ så måste $B(a,r)$ vara sluten. VSB

iv) Om $r \neq 0$ så är den slutna bollen $\overline{B}(a,r)$ både sluten och öppen.

Bevis

Antag att $x \in \overline{B}(a,r)$, då är $|x-a| \leq r$.

Tag ett s så att $0 < s < r$ och betrakta den öppna bollen $B(x,s)$,

tag nu ett $y \in B(x,s)$, då är $|y-x| < s$.

Den icke - arkimediska egenskapen säger att

$|y-a| \leq \max\{|y-x|, |x-a|\} \leq \max\{s,r\} = r$.

Alltså $y \in \overline{B}(a,r)$.

Alltså har vi visat att $B(x,s) \subseteq \overline{B}(a,r)$,

dvs $\overline{B}(a,r)$ är både öppen och sluten.

v) Om $a,b \in F$ och $r,s \in R_+$

så $B(a,r) \cap B(b,s) \neq \emptyset$ om och endast om

$B(a,r) \subset B(b,s)$ eller $B(a,r) \supset B(b,s)$

Dvs. två öppna bollar är antingen skilda åt eller inneslutna i varandra.

Bevis

Antag att $r \leq s$

om skärningen ej är tom så

existerar ett $c \in B(a,r) \cap B(b,s)$

Då vet vi från *i*) att

$B(a,r) = B(c,r) \subset B(c,s) = B(b,s)$

vi) Om $a,b \in F$ *och* $r,s \in R_+$

så $\overline{B}(a,r) \cap \overline{B}(b,s) \neq 0$ omm

$\overline{B}(a,r) \subset \overline{B}(b,s) \quad \vee \quad \overline{B}(a,r) \supset \overline{B}(b,s)$

dvs. två slutna bollar är antingen skilda åt eller inneslutna i varandra.

Bevis

Se *v*) och *ii*).

Exempel som beskriver olika bollar för p-adiska absolutbelopp på Q.

$\overline{B}(0,1) := \left\{ \frac{a}{b} : a,b \in Z, \left|\frac{a}{b}\right|_p \leq 1 \right\}$. ;sluten boll radie 1 runt 0

Vi vet att $\left|\frac{a}{b}\right|_p = p^{-v_p(a/b)}$

$|a/b|_p \leq 1 \quad \Leftrightarrow \quad v_p(a/b) \geq 0 \quad \Leftrightarrow \quad p \nmid b$.

Alltså $\overline{B}(0,1) = \left\{ \frac{a}{b} : a,b \in Z,\ p \nmid b \right\}$.

$\overline{B}(3,1) := \left\{ \frac{a}{b} : a, b \in Z, \left| \frac{a}{b} \right|_p \leq 1 \right\}$. ;sluten boll radie 1 runt 3

Då får vi $\left| \frac{a}{b} - 3 \right|_p \leq 1 \quad \Leftrightarrow \quad v_p\left(\frac{a}{b} - 3 \right) \geq 0 \quad \Leftrightarrow \quad p \nmid b$

$\frac{a}{b} - 3 = \frac{a - 3b}{b}$ $p \nmid b$.

Alltså $\overline{B}(3,1) = \left\{ \frac{a}{b} : a, b \in Z,\ p \nmid b \right\}$.

$B(3,1) := \left\{ \frac{a}{b} : a, b \in Z, \left| \frac{a}{b} - 3 \right|_p < 1 \right\}$. ;öppen boll radie 1 runt 3

Då får vi $\left| \frac{a}{b} - 3 \right|_p < 1 \quad \Leftrightarrow \quad v_p\left(\frac{a}{b} - 3 \right) > 0 \quad \Leftrightarrow \quad p \nmid b$

$\frac{a}{b} - 3 = \frac{a - 3b}{b}$ $p \nmid b$ och $p \mid (a - 3b)$.

Alltså $B(3,1) = \left\{ \frac{a}{b} : a, b \in Z,\ p \nmid b \text{ och } p \mid (a - 3b) \right\}$.

Vilka heltal tillhör denna boll?

Låt $b = 1 \quad \Rightarrow \quad p \mid a - 3 \quad \Rightarrow \quad a \equiv 3 \pmod{p}$.

Exempel

$\overline{B}(0,1)$ kan skrivas som en disjunkt union av öppna bollar

$\overline{B}(0,1) = B(0,1) \cup B(1,1) \cup B(2,1) \cup \ldots \cup B(p-1,1)$.

Den slutna bollen är alla bråk a/b där $p \nmid b$.

Betrakta $a, a - b, a - 2b, \ldots a - (p-1)b$

exakt en av dessa är delbar med p ty det är p st heltal och om 2st skulle vara kongurent modulo p så måste p dela skillnaden mellan dessa två och då skulle $p \mid b$, vilket p ej gör.

Men om $p \mid a - ib$ så

$\left| \frac{a}{b} - i \right| = \left| \frac{a - ib}{b} \right| < 1$

då ligger a/b i den öppna bollen $B(i,1)$ center = i och radie = 1.

Eftersom exakt en är delbar med p så måste unionen var disjunkt.

Exempel

Om vi tar det 5 - adiska absolutbeloppet på Q,

då är $B(1,1) = B(1,1/2) = \overline{B}(1,1/5)$.

För att visa detta får vi helt enkelt räkna ut alla bollar och sedan jämföra svaren.

$B(1,1) := \left\{ \frac{a}{b} : a,b \in Z, \left| \frac{a}{b} - 1 \right|_5 < 1 \right\}.$;Öppen boll radie 1 runt 1

Då får vi $\left| \frac{a}{b} - 1 \right|_5 < 1 \quad \Leftrightarrow \quad v_5\left(\frac{a}{b} - 1 \right) > 0$ om $5 \nmid b$

$\frac{a}{b} - 1 = \frac{a-b}{b}$ $\qquad 5 \nmid b$ men $5 \mid a-b.$

Alltså $B(1,1) := \left\{ \frac{a}{b} : a,b \in Z, \left| \frac{a}{b} \right|_5 < 1, 5 \nmid b \right\}.$

Låt $b = 1$ då är $5 \mid a-1$ vilket ger att $a \equiv 1 \pmod 5$.

$B\left(1,\frac{1}{2}\right) := \left\{ \frac{a}{b} : a,b \in Z, \left| \frac{a}{b} \right|_5 < 1/2 \right\}.$;Öppen boll radie $\frac{1}{2}$ runt 1

Då får vi $\left| \frac{a}{b} - 1 \right|_5 < 1/2 \quad \Leftrightarrow \quad \left| \frac{2a-2b}{b} \right|_5 < 1 \quad \Leftrightarrow \quad v_5\left(\frac{2a-2b}{b} \right) > 0$ om $5 \nmid b$

$\frac{2a-2b}{b}$ $\qquad 5 \nmid b$ men $5 \mid 2a-2b.$

Alltså $B\left(1,\frac{1}{2}\right) := \left\{ \frac{a}{b} : a,b \in Z, \left| \frac{a}{b} \right|_5 < 1/2, 5 \nmid b \right\}.$

Låt $b = 1$ då är $5 \mid 2a-2$ vilket ger att $a \equiv 1 \pmod 5$.

$\overline{B}\left(1,\frac{1}{5}\right) := \left\{ \frac{a}{b} : a,b \in Z, \left| \frac{a}{b} \right|_5 \le 1/5 \right\}.$;Sluten boll radie $\frac{1}{5}$ runt 1

Då får vi $\left| \frac{a}{b} - 1 \right|_5 \le 1/5 \quad \Leftrightarrow \quad \left| \frac{5a-5b}{b} \right|_5 \le 1 \quad \Leftrightarrow \quad v_5\left(\frac{5a-5b}{b} \right) \ge 0$ om $5 \nmid b$

$\frac{5a-5b}{b}$ $\qquad 5 \nmid b$ men $5 \mid 5a-5b.$

Alltså $\overline{B}\left(1,\frac{1}{5}\right) := \left\{ \frac{a}{b} : a,b \in Z, \left| \frac{a}{b} \right|_5 \le 1/5, 5 \nmid b \right\}.$

Låt $b = 1$ då är $5 \mid 5a-5$ vilket ger att $a \equiv 1 \pmod 5$.

Att svaret blir det samma för $|\ |_5 < 1$, $|\ |_5 < 1/2$ och $|\ |_5 \le 1/5$ beror på att det 5 - adiska absolutbeloppet endast kan anta värden för 5^n där $n \in Z$.

Alltså ..., 25, 5, 1, 1/5, 1/25, ...

3. P-adiska tal

Vi ska i detta kapitel definiera absolutbelopp på Q samt redogöra lite kort för Q_p och Z_p samt med hjälp av Hensels lemma visa hur lätt det är att se om ett polynom har rötter i Z_p.

3.1 Absolutbelopp på Q

Definition 3.1.1

Två absolutbelopp $|\ |_1$ och $|\ |_2$ på en kropp F kallas ekvivalenta om de definierar samma topologi på F, alltså varje mängd som är öppen med hänsyn till den ena är även öppen med hänsyn till andra.

Definition 3.1.2

Vi definierar $|\ |_\infty$ som det vanliga absolutbeloppet.

Sats 3.1.3 (Ostrowski 1893-1986)

Varje icke-trivialt absolutbelopp på Q är ekvivalent med ett av absolutbeloppen $|\ |_p$, där p är ett primtal eller $p = \infty$.

Bevis:

Se *p-adic numbers, Fernando Q. Gouvea.*

Produktformeln 3.1.4

För alla $x \in Q$ har vi att

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

$p \le \infty$ innebär att vi tar alla primtal på Q inklusive "primtalet" ∞.

Bevis

Låt x vara ett heltal, som vi kan faktorisera som

$$x = \pm p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_k^{a_k}$$

då får vi
$$\begin{cases} |x|_q = 1 & \text{om } q \neq p_i \quad i = 1,2,\ldots,k \\ |x|_{p_i} = p_i^{-a_i} & i = 1,2,\ldots,k \\ |x|_\infty = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_k^{a_k} \end{cases}$$

Låt x vara ett rationellt tal, dvs $x = a/b \quad a,b \in Z \qquad b \neq 0$

då får vi

$$\prod_{p \le \infty} \left| \frac{a}{b} \right|_p = \frac{\prod |a|_p}{\prod |b|_p} = \frac{1}{1} = 1.$$

Exempel

$x = \frac{-50}{7^3}$

Då har vi $|x|_\infty = 50/7^3$.

Vi börjar med $p = 2$ $\quad |x|_2 = 1/2 \qquad$ (komihåg att $|x|_p = p^{-v_p(x)}$)

$|x|_3 = 1$

$|x|_5 = 1/5^2$

$|x|_7 = 7^3$

$|x|_{11} = 1$

$|x|_{13} = 1. \qquad$; alla nästkommande $|\ |_p = 1$

Alltså $\prod_{p \le \infty} |x|_p = \frac{1}{2} \times 1 \times \frac{1}{5^2} \times 7^3 \times 1 \times 1 \times \ldots \times 1 \times \frac{50}{7^3} = 1.$

Notera att om c inte är ett primtal utan endast ett positivt heltal större än 1 som vi använde oss av tidigare i sats 2.1.7 sidan 23 så skulle inte produktformeln gälla.

3.2 Komplettering

Vi ska nu definiera Q_p men för att göra detta måste vi först definiera följande:
(För en utförligare definiering av Q_p se boken p-adic numbers kapitel 3.2, har här endast presenterat de viktigaste definitionerna.)

Definition 3.2.1

Låt $|\ | = |\ |_p$ vara ett icke - arkimediskt absolutbelopp på Q. Vi definierar C (eller $C_p(Q)$ om vi vill poängtera p och Q), mängden av alla Cauchy följder av element i Q :

$C = C_p(Q) = \{(x_n) : (x_n)$ är en Cauchy följd med hänsyn till $|\ |_p\}$

Addition och multiplikation definieras som

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

$(x_n)(y_n) = (x_n y_n)$

vilket gör att C är en kommutativ ring.

Definition 3.2.2

Vi definierar $N \subset C$ till att vara idealet

$N = \{(x_n) : x_n \to 0\} = \{(x_n) : \lim_{n\to\infty} |x_n|_p = 0\}$

av följder som med hänsyn till absolutbeloppet $|\ |_p$ går mot noll.

Definition 3.2.3
Vi definierar kroppen av p - adiska tal till att vara kvoten av ringen *C* med dess maximala ideal *N* :

$Q_p = C/N$

(Bevis se Abstrakt algebra sats 14.33 sidan 320)

Definition 3.2.4
Om $\lambda \in Q_p$ är ett element i Q_p, och (x_n) är en Cauchy följd som representerar λ,
så definierar vi $|\lambda|_p = \lim_{n\to\infty} |x_n|_p$.

Sats 3.2.5
För alla primtal p ∈ Z existerar en kropp Q_p med ett icke - arkimediskt absolutbelopp $|\ |_p$, s.a :

i) det existerar en inbäddning $Q \to Q_p$ och att absolutbeloppet $|\ |_p$ på Q via denna inbäddningen är det p - adiska absolutbeloppet.

ii) bilden av Q under denna inbäddning är tät i Q_p.

iii) Q_p är fullständig med hänsyn till absolutbeloppet $|\ |_p$.

Bevis
Se *p-adic numbers, Fernando Q. Gouvea*.

Sats 3.2.6

Då $x_n \in Q_p$, då konvergerar $\sum_{n=1}^{\infty} x_n$ om och endast om $|x_n|_p \to 0$ då $n \to \infty$.

Bevis

Antag att $|x_n|_p \to 0$ och låt $\lambda_N = \sum_{n=1}^{N} x_n$

om $M > N$ så är

$|\lambda_M - \lambda_N|_p = |x_{N+1} + x_{N+2} + ... + x_M|_p \leq$

$\leq \max\{|x_{N+1}|, |x_{N+2}|, ..., |x_M|\} \to 0$ då $N \to \infty$.

Exempel

$\sum_{n=0}^{\infty} p^n$ konvergerar ty $|p^n|_p = \frac{1}{p^n} \to 0$ då $n \to \infty$.

I själva verket vet vi att $\sum_{n=0}^{\infty} p^n = \frac{1}{1-p}$ $\qquad \left(ty\ (1-p)\sum_{n=0}^{\infty} p^n = 1 \right)$

Om vi fortsätter med att utforska kroppen Q_p så ser vi att.

Lemma 3.2.7

För alla $x \in Q_p$, $x \neq 0$ så finns det ett heltal $v_p(x)$ så att $|x|_p = p^{-v_p(x)}$.

Eftersom Q_p är en kropp med en icke-arkimedisk valuation så ger det oss följande valuationsring.

Definition 3.2.8

Ringen av p - adiska heltal är valuationsringen

$Z_p = \{x \in Q_p : |x|_p \leq 1\}$

3.3 Hensels lemma

Med hjälp av Hensels lemma kan man ganska lätt bestämma om ett polynom har rötter i Z_p och i så fall vilka de är.
Hensels lemma bygger på Newton-Raphsons metoden för att lösa ekvationer.

Newton-Raphsons metoden är en numerisk metod för att hitta en rot till en ekvation *F(x)=0*.

$$x_{n+1} = x_n - \frac{F(x_n)}{F'(x_n)}$$

Då den p-adiska analysen på många sätt är lättare än den reella analysen så visar Hensels lemma ganska lätt om ett polynomen har rötter i Z_p.

Hensels lemma 3.3.1

Låt $F(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ vara ett polynom med koefficienter i Z_p,

antag att det finns ett p - adiskt heltal $\alpha_1 \in Z_p$ s.a

$F(\alpha_1) \equiv 0 \pmod{pZ_p}$

$F'(\alpha_1) \not\equiv 0 \pmod{pZ_p}$.

Då existerar det ett unikt p - adiskt heltal $\alpha \in Z_p$ s.a

$\alpha \equiv \alpha_1 \pmod{pZ_p}$

$F(\alpha) = 0$

Bevis

Se *p-adic numbers, Fernando Q. Gouvea.*

Exempel
För att undvika jobbet med att hitta inverser till tal så tar vi ett exempel som vi redan har räknat ut.

$x^2 \equiv 2 \pmod{7^n}$

Där vi fick lösningen : $3, 10, 108, 2166, 4567, \ldots$ (se sidan 7)

och $4, 39, 235, 235, 12240, \ldots$

Vi ska söka lösning för $F(x) = x^2 - 2$ i Z_7

$F(x_1) \equiv 0 \pmod{pZ_p}$.

Alltså $x_1^{\,2} \equiv 2 \pmod 7$ vilket ger att $x_1 \equiv 3$ eller $4 \pmod 7$.

Tag $x_1 = 3$

$F(x) = x^2 - 2 \quad F'(x) = 2x$

$F(3) \equiv 0 \qquad F'(3) \equiv 6 \not\equiv 0$ villkoren för Hensel's lemma är alltså uppfyllda.

Om vi nu använder oss av Newton-Raphsons metoden så får vi

$$x_{n+1} \equiv x_n - \frac{F(x_n)}{F'(x_n)} \equiv x_n - \frac{x_n^{\,2} - 2}{2x_n} \equiv \frac{x_n^{\,2} + 2}{2x_n} \pmod{7^{n+1}}$$

$x_1 = 3$ ger att :

$$x_2 \equiv \frac{3^2 + 2}{2 \times 3} \equiv \frac{11}{6} \pmod{49}.$$

Alltså $6x_2 \equiv 11 \pmod{49}$.

Eftersom vi tidigare har räknat detta vet vi att

$x_2 \equiv 10 \pmod{49}$;$6 \times 10 \equiv 11 \pmod{49}$

vilket ger att :

$$x_3 \equiv \frac{10^2 + 2}{2 \times 10} \equiv \frac{102}{20} \equiv \frac{51}{10} \pmod{343}.$$

Alltså $10x_3 \equiv 51 \pmod{343}$

$x_3 \equiv 108 \pmod{343}$;$10 \times 108 \equiv 51 \pmod{343}$

osv.

Kvadratisk reciprocitet

Med hjälp av kvadratisk reciprocitet kan man ganska lätt se för vilka p i Z_p en kvadratisk ekvation har lösningar. Då måste vi först titta på Legendresymbolen.

Def 3.3.2 Legendresymbol (Taget från Wikipedia)

Legendresymbolen definieras som följer:

Om p är ett udda primtal och a är ett heltal, så är Legendresymbolen

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{om } p \mid a. \\ 1 & \text{om } a \text{ är en kvadrat (mod } p\text{), dvs det finns ett } k \text{ s.a } k^2 \equiv a \pmod{p}. \\ -1 & \text{om } a \text{ inte är en kvadrat (mod } p\text{).} \end{cases}$$

Def 3.3.3 Kvadratisk reciprocitet **(Gauss)** (Taget från Wikipedia)

Om både p och q är två olika udda primtal så är

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

Då är

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ om en eller både p och q är på formen $4k+1, k \in Z$

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ om både p och q är på formen $4k+3, k \in Z$

Exempel

Vi ska nu undersöka om $F(x) = x^2 - 5$ någon lösning i Z_p.

Enligt Hensels lemma behöver vi endast titta på dessa 2 kongruenser

$F(x_1) = x_1^{\,2} - 5 \equiv 0 \pmod{p}$

$F'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$ (Uppfyllt ty $2x \neq p$, $p \neq 2$)

Vi kan alltså fråga oss om ekvationen

$x^2 \equiv 5 \pmod{p}$

har någon lösning x i Z.

Detta kan lösas med hjälp av kvadratisk reciprocitet för att

$$\left(\frac{p}{5}\right)\left(\frac{5}{p}\right) = (-1)^{(p-1)} = 1$$ eftersom 5 kan skrivas på formen $4k+1$

så är $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)$ då får vi att

$x^2 \equiv p \pmod{5}$;$1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 4$, $4^2 \equiv 1$

$p \equiv \pm 1 \pmod{5}$;$-1 \equiv 4 \pmod{5}$.

Alltså har vi visat att för alla primtal p med

$p \equiv \pm 1 \pmod{5}$ har $x^2 \equiv 5 \pmod{p}$ en lösning.

Dvs. lösning finns för $p = 11, 19, 29, \ldots$

4. Referenser

p-adic numbers	Fernando Q. Gouvea
Abstrakt algebra	Per Anders Svensson
Introduction to real analysis	Robert G. Bartle, Donald R. Sherbert
www.wikipedia.org	