Sammanfattning

Detta examensarbete beskriver några bevis av lagen om kvadratisk reciprocitet. I inledningen ger vi specifika exempel på kvadratiska rester modulo primtal och introducerar begreppet kvadratisk reciprocitet. Kapitel 2 beskriver kortfattat reduceringen från en allmän kvadratisk ekvation modulo ett heltal, till en ekvation på formen, $x^2 \equiv q \pmod p$, där både p och q är primtal. Dessutom ger vi formler som beskriver antalet lösningar till sådana ekvationer, samt två bevis för att det exakta antalet kvadratiska rester modulo ett primtal p är $(p-1)/2$. Kapitel 3 ger en historisk tillbakablick på upptäckten av den Gaussiska reciprocitetslagen. Legendresymbolen definieras och vi ger fyra olika formuleringar av reciprocitetslagen. I Kapitel 4 bevisar vi de två supplementära lagarna, dvs vi beräknar $\left(\frac{-1}{p}\right)$ och $\left(\frac{2}{p}\right)$, för alla primtal p. Dessutom introducerar vi ett berömt lemma av Gauss, som senare används i nästan alla bevis av kvadratiska reciprocitetslagen i Kapitel 6. Kapitel 5 beskriver en generalisering av Legendresymbolen till Jacobisymbolen $\left(\frac{m}{n}\right)$, där m, n är udda heltal. De två sista kapitlen ger ett antal olika bevis av lagen om kvadratisk reciprocitet, varav i Kapitel 7 definieras Gaussummor i ändliga kroppar och vi bevisar reciprocitetslagen med hjälp av dessa summor.

Tack Juliusz Brzezinski för din suveräna handledning under hela arbetets gång! Tack till Peter Hegarty för värdefulla kommentarer.

Dessutom vill jag gärna tacka min familj för ert fina stöd.

Innehåll

1 Inledning

"*Theorerum aurerum*" kallade Gauss lagen om kvadratisk reciprocitet i sina privata anteckningar. Den mera formella benämningen som han använde sig av, bland annat i det banbrytande talteoretiska verket "Disquisitiones Arithmeticae", var "*Fundamentalsatsen*", för han ansåg att satsen uttryckte allt viktigt som kunde sägas om kvadratiska kongruenser. För att förstå vad kvadratisk reciprocitet är, behöver vi först bekanta oss med kvadratiska rester modulo ett primtal.
Är 43 en kvadratisk rest modulo 541? Det vill säga, har ekvationen $x^2 \equiv 43 \pmod{541}$ någon lösning? Om ekvationen har en lösning kallar vi här 43 för kvadratisk rest. Nedan redovisar vi en liten lista på alla kvadratiska rester modulo de 8 första primtalen.

Ekvation	*Kvadratiska rester a*
$x^2 \equiv a \pmod{2}$	0,1
$x^2 \equiv a \pmod{3}$	0,1
$x^2 \equiv a \pmod{5}$	0,1,4
$x^2 \equiv a \pmod{7}$	0,1,2,4
$x^2 \equiv a \pmod{11}$	0,1,3,4,5,9
$x^2 \equiv a \pmod{13}$	0,1,3,4,9,10,12
$x^2 \equiv a \pmod{17}$	0,1,2,4,8,9,13,15,16
$x^2 \equiv a \pmod{19}$	0,1,4,5,6,7,9,11,16,17

Så länge vi betraktar små tal är det enkelt att skriva upp liknande listor för att få reda på alla kvadratiska rester, respektive icke-kvadratiska rester, men hur tar vi enklast (och utan hjälp av datorn), reda på om till exempel primtalet 7411 är en kvadratisk rest modulo primtalet 9283 eller inte?

Notera att det inte verkar finnas något generellt mönster i hur de kvadratiska resterna är fördelade i de olika restklasserna modulo p, där p är ett udda primtal.

Däremot tyder tabellen ovan på att de nollskilda kvadratiska resterna $\pmod{p}$ är $\frac{p-1}{2}$ till antalet. Vi har att hälften av restklasserna modulo ett primtal är kvadratiska rester och den andra hälften är icke-kvadratiska rester. Detta ligger inte särdeles långt borta från vad man kanske vill gissa (för bevis se sidan 8).

Det som kan vara svårt att gissa är att det finns ett samband mellan två udda primtal p och q, som gör det möjligt att avgöra om p är en kvadratisk rest modulo q, eller inte. Sambandet brukar kallas 'Lagen om kvadratisk reciprocitet', ibland 'Gauss reciprocitetslag', eller kortast 'Reciprocitetslagen'. Den lyder som följer:

Reciprocitetslagen *Låt p och q vara olika udda primtal. Då är p en kvadratisk rest modulo q om och endast om q är en kvadratisk rest modulo p, förutom om $p \equiv q \equiv 3 \pmod 4$, då p är en kvadratisk rest modulo q om och endast om q är en icke-kvadratisk rest modulo p.*

Lagens formulering och användning förenklas med hjälp av följande notation. Betrakta relativt prima heltal a och p varav p är ett udda primtal. Legendresymbolen $\left(\frac{a}{p}\right) = 1$ omm a är en kvadratisk rest modulo p och $\left(\frac{a}{p}\right) = -1$ annars. Nu kan reciprocitetslagen formuleras så här enkelt:

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

Vidare gäller om p är ett udda primtal och a, b är heltal att $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ och att $a \equiv b \pmod p$ medför $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. När vi tar hjälp av dessa egenskaper hos Legendresymbolen, kan vi göra en enkel beräkning som visar att 7411 är en icke-kvadratisk rest modulo 9283.

Bägge talen 7411 och 9283 är primtal $\equiv 3 \pmod 4$. Lagen om kvadratisk reciprocitet och $9283 \equiv 1872 \pmod{7411}$ ger att $\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right)$. Eftersom $1872 = 2^4 3^2 13$ följer det att Legendresymbolen är $-\left(\frac{13}{7411}\right)$. Nu använder vi kvadratisk reciprocitet igen och eftersom $13 \equiv 1 \pmod 4$, ser vi att $-\left(\frac{13}{7411}\right) = -\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1$.

Detta illustrerar en av de många användningarna av lagen om kvadratisk reciprocitet, men tyngdpunkten i detta examensarbete ligger inte i hur vi använder lagen, utan på hur vi kan bevisa sambandet på olika sätt. Gauss hittade 8 bevis varav 7 anses vara helt olika. Historiskt sett har man fortsatt hitta nya bevis av lagen ända sedan dess upptäckt på slutat av 1700-talet. Numera finns (minst) 196 bevis av lagen, varav många är varianter på ett och samma tema (en stor del av bevisen bygger på 'Gauss lemma'), men kanske så många som 40 anses vara helt olika. I [6] ges ett belysande citat från en intervju år 1998 med Yuri Manin:

... I was very interested in the fact that Gauss found seven

or eight proofs of the quadratic reciprocity law. What bothered me was why he needed seven or eight proofs. Every time I gained some more understanding of number theory, I better understood Gauss' mind. Of course, he was not looking for more convincing arguments – one proof is sufficiently convincing. The point is that proving is the way we are discovering new territories, new features of the mathematical landscape.

2 Kvadratiska rester

Vi ställer här frågan om, för givna heltal a och n, sådana att $\mathrm{sgd}(a, n) = 1$, ekvationen

$$x^2 \equiv a \pmod{n}, \tag{1}$$

har en lösning eller inte. Om den har en heltalslösning så definierar vi a som **en kvadratisk rest** modulo n. Om ekvationen $x^2 \equiv a \pmod{n}$ inte har någon lösning, så säger vi att a är en **icke-kvadratisk rest** modulo n.

2.1 Reduktionen

Det visar sig att all information om (1) finns att hämta i ekvationerna

$$x^2 \equiv a \pmod{2^k} \tag{2}$$

där k är ett naturligt tal och $2^k \parallel n$ [1], samt

$$x^2 \equiv a \pmod{p}, \tag{3}$$

där p är ett udda primtal som delar n. Detta resultat ges nämligen av de två följande propositionerna och Följdsats 2.3. I Proposition 2.1, vilken följer ur Kinesiska restsatsen, kan p vara ett helt godtyckligt primtal och a ett godtyckligt heltal. k och k_i är naturliga tal.

Proposition 2.1 *Ekvationen $x^2 \equiv a \pmod{n}$ har en lösning om och endast om $x^2 \equiv a \pmod{p^k}$ har lösning för varje $p^k \parallel n$.*
Mera exakt formulerat: Om $n = p_1^{k_1} \cdots p_r^{k_r}$, där p_i är olika primtal, så är ekvationen $x^2 \equiv a \pmod{n}$ lösbar då och endast då $x^2 \equiv a \pmod{p_i^{k_i}}$, $(i = 1, 2, \ldots, r)$ är lösbara.

[1] Symbolen $p^k \parallel n$, där p är ett primtal, betyder här att p^k delar n, men att p^{k+1} inte delar n.

Proposition 2.2 nedan ger oss en metod att induktivt hitta lösningarna till

$$x^2 \equiv a \pmod{p^k}, \tag{4}$$

när vi redan vet lösningarna till $x^2 \equiv a \pmod{p}$:

Proposition 2.2 (i) *Låt p vara ett udda primtal och k ett godtyckligt positivt heltal, och antag att s_k är en lösning till $x^2 \equiv a \pmod{p^k}$. Då finns precis en lösning s_{k+1} till $x^2 \equiv a \pmod{p^{k+1}}$ sådan att $s_{k+1} \equiv s_k \pmod{p^k}$.*
(ii) *Lösningen s_{k+1} ges av $s_{k+1} = s_k + p^k t$, där t är den unika lösningen till $2t \equiv -s_k/p^k \pmod{p}$.*

Vi kommer inte att använda andra delen av Proposition 2.2. Det viktiga här är frågan om existensen av lösningar.

Följdsats 2.3 *Låt p vara ett udda primtal, a ett heltal med $(a,p) = 1$, och k ett naturligt tal. Då är $x^2 \equiv a \pmod{p^k}$ lösbar då och endast då $x^2 \equiv a \pmod{p}$ är lösbar. Om $x^2 \equiv a \pmod{p}$ är lösbar så har varje ekvation $x^2 \equiv a \pmod{p^k}$ exakt två lösningar.*

Proposition 2.1 och Följdsats 2.3 använder vi för att begränsa undersökningen av eventuella kvadratiska rester modulo ett udda heltal till dem modulo udda primtal.

(För bevis av alla propositioner i detta avsnitt, samt följdsatsen ovan, hänvisar vi till [1], sidan 106 till 109, eller till [7] för en gruppteoretisk framställning.)

När vi vill bestämma om a är en kvadratisk rest för jämna heltal n, så behöver vi givetvis också besvara frågan om lösningar till (2). Dessa lösningar behandlas separat. (Anledningen till särbehandlingen är att vi undersöker lösningar till kvadratiska kongruenser. Om vi till exempel varit intresserade av lösningarna till $x^5 \equiv a \pmod{p}$ istället, så hade vi behövt behandla potenser av 5 separat.)

För potenser av två är situationen som följer:

Proposition 2.4 *Antag att a är ett udda heltal. Då gäller:*
(i) $x^2 \equiv a \pmod{2}$ *är alltid lösbar och har exakt en lösning,* $x \equiv 1 \pmod{2}$*;*

(ii) $x^2 \equiv a \pmod 4$ *är lösbar om och endast om* $a \equiv 1 \pmod 4$, *då vi har precis två lösningar* $x \equiv 1, 3 \pmod 4$*;*
(iii) $x^2 \equiv a \pmod{2^k}$, *med* $k \geq 3$, *är lösbar om och endast om* $a \equiv 1 \pmod 8$, *då vi har exakt fyra lösningar* $\pmod{2^k}$. *Speciellt gäller att om vi har att* s *är en lösning, så ges alla sådana lösningar av* $\pm s$ *och* $\pm s + 2^{k-1}$.

Huvudtesen i detta kapitel är att vi alltid kan reducera en kvadratisk ekvation modulo ett heltal, till kvadratiska kongruensekvationer modulo udda primtal, eller modulo 2^k där $k \leq 3$. Därför kan vi från och med Kapitel 3 i lugn och ro ägna oss åt ekvation (3).

2.2 Den allmänna kvadratiska ekvationen

Lösningen till den allmänna kvadratiska kongruensen kan delas upp i en linjär ekvation och en kvadratiskt ekvation, enligt följande proposition.

Proposition 2.5 *Låt* a, b, c, n *vara heltal. Antag vidare* $(a, n) = 1$. *Den allmänna kvadratiska kongruensen*

$$ax^2 + bx + c \equiv 0 \pmod n \tag{5}$$

är ekvivalent med en kongruensekvation av formen

$$y^2 \equiv d \pmod N, \tag{6}$$

där $y = 2ax + b$, $N = 4an$ *samt* $d = b^2 - 4ac$.

Bevis Multiplicera (5) med $4a$. Vi får då att

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4an},$$

och därför

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4an}.$$

$\square$

2.3 Antalet lösningar modulo ett heltal

Om det finns en lösning till (1), hur många finns det? Denna fråga är inte alltför komplicerad att besvara och vi skall göra det nu direkt. Till att börja med konstaterar vi att vi redan vet svaret för ekvationen (3), samt för $x^2 \equiv a \pmod{p^k}$. I bägge fallen är svaret två, förutom när $p = 2$. Då ges resultatet av Proposition 2.4.

Här presenteras några enkla exempel på lösningar till kvadratiska ekvationer.

$$x^2 \equiv 1 \pmod 7,$$

har 2 lösningar $x \equiv 1, -1 \pmod 7$,

$$x^2 \equiv 2 \pmod 7$$

har 2 lösningar $x \equiv 3, -3 \pmod 7$,

$$x^2 \equiv 1 \pmod 9$$

har 2 lösningar $x \equiv 1, -1 \pmod 9$,

$$x^2 \equiv 1 \pmod 8,$$

har 4 lösningar $x \equiv 1, 3, -3, -1 \pmod 8$,

$$x^2 \equiv 1 \pmod{30},$$

har 4 lösningar $x \equiv 1, 11, -11, -1 \pmod{30}$.

Betrakta nu kongruensen

$$x^2 \equiv a \pmod{105}, \tag{7}$$

där a är ett godtyckligt heltal.

Ekvation (7) har lösning när a är en kvadratisk rest modulo 3,5 respektive 7. Detta händer för $1, 4, 16, 64, 46$ och $79 \pmod{105}$. De kvadratiska resterna hittas enkelt med hjälp av kinesiska restsatsen. De bildar en cyklisk delgrupp till gruppen av enheter $\mathbb{Z}^*_{105}$, med generator $\bar{4}$. I vart och ett av fallen $a = 1, 4, 16, 46, 64, 79$ finns $2^3 = 8$ lösningar. Till exempel för $a = 64$ har vi $x = \pm 8, \pm 13, \pm 22$ samt ytterligare två lösningar, som lämnas åt läsaren att hitta.

Anmärkning Här har vi inte inkluderat de kvadrater vilka har gemensam delare med 105. Det vill säga till exempel 9 eller 25 eller 49. Enligt definitionen vid ekvation (1) i början av första kapitlet bör vi avstå att kalla dessa tal kvadratiska rester modulo 105 (trots att de är kvadrater), för en kvadratisk rest är per definition både en kvadrat och en enhet. Enheterna modulo ett naturligt tal n har en gruppstruktur med avseende på multiplikation. 9 är en nolldelare modulo 105, eftersom till exempel $9 \cdot 35 \equiv 0 \pmod{105}$. Därför är 9 ingen enhet i restringen $\mathbb{Z}_{105}$ och därmed inte heller en kvadratisk rest.

Om heltalen a, n är relativt prima och a är en kvadratisk rest modulo n, hur många lösningar har då kongruensen $x^2 \equiv a \pmod{n}$? Resultatet ges av följande proposition:

Proposition 2.6 *Låt $n = 2^k p_1^{k_1} \cdots p_r^{k_r}$ och $(a, n) = 1$. Om $x^2 \equiv a \pmod{n}$ är lösbar, så finns det 2^r lösningar när $k = 0$ eller $k = 1$, 2^{r+1} lösningar när $k = 2$, och 2^{r+2} lösningar när $k \geq 3$.*

För bevis av Proposition 2.6 hänvisar vi till [1].

Exempel 2.1 Om det udda talet n har exakt r distinkta primfaktorer, så har kongruensen $x^2 \equiv 1 \pmod{n}$ exakt 2^r lösningar.

2.4 Antalet kvadratiska rester modulo ett primtal

Följande lemma beskriver hur många kvadratiska rester, respektive hur många icke-kvadratiska rester det finns för ett udda primtal p.

Lemma 2.7 *Låt p vara ett udda primtal. Då finns det exakt $(p-1)/2$ inkongruenta kvadratiska rester modulo p och exakt $(p-1)/2$ icke-kvadratiska rester modulo p.*

Bevis Vi vet att om p är ett primtal, så bildar alla elementen i $\mathbb{Z}_p^*$ en cyklisk grupp. (För bevis, se [7]). Låt s vara en generator i $\mathbb{Z}_p^*$. Då kan alla elementen skrivas som s^k för $0 \leq k \leq p-1$. De kvadratiska resterna är precis de jämna potenserna av s. De icke-kvadratiska resterna är exakt de udda potenserna. Beviset är klart. $\square$

Vi ger också ett annat bevis, som inte använder sig av begreppet cyklisk grupp och därför blir lite mer tekniskt.

Bevis Det räcker att konstatera att elementen $\pm 1, \pm 2, ..., \pm(p-1)/2$ representerar alla möjliga restklasser modulo p. Tag nu kvadraten på elementen ovan, vilket ger elementen $1^2, 2^2, ..., ((p-1)/2)^2$ och vi skall visa att dessa utgör $(p-1)/2$ inkongruenta kvadratiska rester. Nämligen, låt a, b vara heltal sådana att $1 \leq a, b \leq (p-1)/2$ och $a^2 \equiv b^2 \pmod{p}$. Då gäller att $a \equiv \pm b \pmod{p}$ det vill säga, antingen $a \equiv b \pmod{p}$ eller $a + b \equiv 0 \pmod{p}$. I första fallet har vi att $a = b$ eftersom $1 \leq a, b \leq (p-1)/2$ och i det andra fallet gäller att $p \mid a + b$, men vi har $1 \leq a, b \leq (p-1)/2$ så $p \nmid a + b$. Vi har fått en motsägelse. Alltså har vi exakt $(p-1)/2$ inkongruenta kvadratiska rester och därmed också $(p-1)/2$ inkongruenta icke-kvadratiska rester. $\square$

Nu skall vi undersöka för vilka udda primtal p, ett givet primtal q är en kvadratisk rest. Tack vare kvadratisk reciprocitet kan vi reducera frågan till en konkret ändlig beräkning. Nämligen så räcker det i samtliga fall att bestämma alla kvadratiska rester modulo $4q$. I vissa fall räcker det att bestämma de kvadratiska resterna modulo q. Detta var faktiskt hur kvadratisk reciprocitet upptäcktes av Leonard Euler en gång i tiden, men detta utgör också en av de viktiga konsekvenserna av lagen om kvadratisk reciprocitet. I nästa kapitel presenteras några exempel samtidigt som vi ger en historisk tillbakablick.

3 Euler, Gauss och Legendre

Det var Euler som upptäckte och formulerade kvadratisk reciprocitet, och Legendre som införde en modern beteckning, vilken i första hand förenklar handhavandet av kvadratisk reciprocitet, men ännu väsentligare visar sig möjliggöra generaliseringar i olika algebraiska talkroppar för högre grads reciprocitetslagar. Men det var alltså Gauss som först lyckades ge ett fullständigt bevis för satsen. Han gav inte bara ett bevis, utan faktiskt så många som 7 stycken helt olika bevis. Anledningen var att han sökte generalisera lagen från kvadratisk reciprocitet till reciprocitet i andra kroppsutvidgningar, i första hand till bikvadratisk reciprocitet. Han studerade därför de aritmetiska egenskaperna i ringen $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, vilken liksom $\mathbb{Z}$ är en Euklidisk ring och därför har unik faktorisering.

Gauss hittade alltså det första fullständiga beviset av lagen om kvadratisk reciprocitet, men dessförinnan hade Euler formulerat satsen och "nästan" bevisat den. Hans försök till bevis från år 1785/1788 bygger bland annat på antagandet av giltigheten av en annan stor sats, nämligen satsen om att varje aritmetisk följd $a + bm$, med a och b relativt prima heltal och $m = 1, 2, 3, \ldots$, innehåller oändligt många primtal. Denna sats bevisades senare av Dirichlet med analytiska metoder, men eftersom satsen på Eulers tid ännu inte var bevisad anses hans bevis av kvadratisk reciprocitet, som beror på det som numera kallas Dirichlets sats, inte fullständigt. På sidorna 16-18 i [2] finns en modern beskrivning av Eulers "bevis". (För övrigt kan kvadratisk reciprocitet med framgång användas för att bevisa specialfall av Dirichlets sats, se till exempel [4] på sidan 52 och 53.) Vi skall snart se att Gauss och många av de efterföljande bevismakarna använde sig av andra metoder, där ofta ett lemma av Gauss har en viktig roll i bevisföringen. Även Gaussummor, kvadratiska former, cyclokotomiska kroppar, kvadratiska kroppar eller permutationer och många andra metoder ger bevis. Här ger vi nu fyra ekvivalenta formuleringar av lagen, men först definieras Legendresymbolen:

Definition 3.1 *Betrakta heltalen a och p varav p är ett primtal. Legendresymbolen $\left(\frac{a}{p}\right)$ definieras som*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a, \\ 1 & a \text{ är en kvadratisk rest modulo } p, \\ -1 & a \text{ är en icke-kvadratisk rest modulo } p. \end{cases}$$

Reciprocitetslagen *Låt p och q vara olika udda primtal, då har vi fyra ekvivalenta formuleringar av reciprocitetslagen:*

(i) *p är en kvadratisk rest modulo q om och endast om q är en kvadratisk rest modulo p, förutom om $p \equiv q \equiv 3 \pmod 4$, då p är en kvadratisk rest modulo q om och endast om q är en icke-kvadratisk rest modulo p.*

(ii) *Legendresymbolen är som i* Definition 3.1. *Nu har vi:*

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

vilket ibland formuleras som

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right),$$

där $p^* := (-1)^{(p-1)/2}p$.

(iii) *Legendresymbolen är som i* Definition 3.1. *Det gäller:*

$$\left(\frac{q}{p}\right) = 1 \Leftrightarrow p \equiv \pm\beta^2 \pmod{4q},$$

för något udda heltal β.

(iv) *Antag $(a,p) = (a,q) = 1$, där a är ett positivt heltal. Om $q \equiv p \pmod{4a}$ eller $q \equiv -p \pmod{4a}$, då är $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$.*

Vi bevisar de ekvivalenta formuleringarna av reciprocitetslagen i Kapitel 6 och 7, utom ekvivalensen av **(ii)** och **(iii)** vilken bevisas här:

Bevis (ii) $\Leftrightarrow$ (iii). Likheten $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$ är ekvivalent med

$$\left(\frac{q}{p}\right) = 1 \quad\Leftrightarrow\quad \left(\frac{p^*}{q}\right) = 1.$$

Nu visar vi att $\left(\frac{p^*}{q}\right) = 1 \Leftrightarrow p \equiv \pm\beta^2 \pmod{4q}$ med β udda:

"$\Leftarrow$" β udda ger $\beta^2 \equiv 1 \pmod 4$. Om $p \equiv 1 \pmod 4$ så $p \equiv \beta^2 \pmod q$ dvs $\left(\frac{p^*}{q}\right) = 1$. Om $p \equiv 3 \pmod 4$ så $p \equiv -\beta^2 \pmod q$ dvs $\left(\frac{p^*}{q}\right) = 1$.

"$\Rightarrow$" $\left(\frac{p^*}{q}\right) = 1$ ger att $p^* \equiv \beta^2 \pmod q$. Det är klart att β är udda ty p^* är udda. Alltså är $\beta^2 \equiv 1 \pmod 4$. Om $p \equiv 1 \pmod 4$ så är $4 \mid p - \beta^2$ dvs

$p \equiv \beta^2 \pmod{4q}$. Om $p \equiv 3 \pmod 4$ så är $4 \mid p+\beta^2$ dvs $p \equiv -\beta^2 \pmod{4q}$. $\square$

När Euler upptäckte Reciprocitetslagen, formulerad som i **(iii)**, på 1700-talet, hade han undersökt flera specialfall av kvadratisk reciprocitet. Här är några av Eulers resultat:

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pmod{12},$$
$$\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 11 \pmod{20},$$
$$\left(\frac{7}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 3, \pm 9 \pmod{28},$$

Det gemensamma mönstret ser vi enklast genom att skriva om de tre leden enligt följande:

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{12},$$
$$\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 9 \pmod{20},$$
$$\left(\frac{7}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 25, \pm 9 \pmod{28}.$$

Nu ser vi att $\pm p$ måste vara kongruent med en kvadrat. Men innan vi drar slutsatser från resultaten ovan, så kan en annan av Eulers påståenden vara värt en begrundan:

$$\left(\frac{6}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pm 5 \pmod{24}.$$

Det kan kontrolleras att ± 5 inte är kvadrater modulo 24, (för alla kvadraterna ges av $1, 4, 9, 16, 25 \equiv 1, 36 \equiv 12, 49 \equiv 1, 64 \equiv 16, 81 \equiv 9, 100 \equiv 4, 121 \equiv 1$). Samma sak händer för $(10/p)$ och $(14/p)$, men $3, 5, 7$ är primtal, medan $6, 10$ och 14 är sammansatta. Därav kan Eulers hypotes, (iii) i reciprocitetslagen, sidan 11, kännas motiverad.

Det var en närbesläktad fråga som ledde Euler mot lagen om kvadratisk reciprocitet. Han sökte nämligen alla representationer av primtal p på formen

x^2+ny^2, där n är ett positivt heltal. Den enklaste ekvationen på denna form är ju givetvis $p = x^2+y^2$. Det var Fermat som först påstod att denna ekvation är ekvivalent med att $p \equiv 1 \pmod 4$. På liknande sätt hävdade Fermat att $p = x^2 + 2y^2 \Leftrightarrow p \equiv 1$ eller $3 \pmod 8$ och att $p = x^2 + 3y^2 \Leftrightarrow p = 3$ eller $p \equiv 1 \pmod 3$. Fermat lämnade inga bevis.

Generaliseringen av ovanstående uttryck ledde Euler till hypotesen att ekvationen $p = x^2 + ny^2$ är lösbar då och endast då p lämnar specifika rester vid division med n eller $4n$. Följande lemma ger en del av lösningen:

Lemma 3.1 *Låt n vara ett nollskilt heltal, och låt p vara ett udda primtal som inte delar n. Då gäller $p \mid x^2+ny^2$, $sgd(x, y) = 1 \Leftrightarrow -n$ är en kvadratisk rest modulo p.*

Om vi väljer $n = -q$ där q är ett primtal, så är $p \mid x^2 - qy^2$ ekvivalent med $p \equiv \pm\beta^2 \pmod{4q}$, (se [2], sidan 13) och detta är ju som sagt ekvivalent med reciprocitetslagen.

Anledningen till att Euler inte gav bevis av reciprocitetslagen, var enligt A. Weil, se [2] sidan 16–19, att Euler var mest intresserad av att karakterisera de kvadratiska resterna modulo varje *naturligt* tal. Mera i detalj hur Euler gick till väga beskriver [2].

4 Från Eulers Kriterium till Gauss Lemma

Nu först till två viktiga exempel, där vi bestämmer värdet på Legendresymbolen $(\frac{a}{p})$ då $a \equiv -1 \pmod p$, respektive $a \equiv 2 \pmod p$. Dessa två fall brukar kallas de supplementära lagarna. Det enda vi behöver för att bevisa de supplementära lagarna är Eulers kriterium, som är en följd av Fermats lilla sats.

Fermats lilla sats *Antag att p är primtal och a är ett heltal med $(a,p) = 1$. Då gäller att $a^{p-1} \equiv 1 \pmod p$.*

Bevis Fermats lilla sats följer direkt om man noterar att $\mathbb{Z}_p^*$ är en grupp av ordning $p-1$ så att $a^{p-1} = 1$ för varje $a \in \mathbb{Z}_p^*$. □

Det finns bevis som bygger på ren talteori också, se [1] eller [5] till exempel. Kongruensen $a^{n-1} \equiv 1 \pmod n$ ger ett nödvändigt villkor för att ett tal n skall vara ett primtal, men inte ett tillräckligt villkor. Om ett tal n uppfyller kongruensen, men inte är ett primtal, så kallas det för ett pseudoprimtal.

Låt nu p vara ett udda primtal och K vara mängden av alla kvadratiska rester i $\mathbb{Z}_p$. Man vet att $K \subset \mathbb{Z}_p$ bildar en cyklisk delgrupp till $\mathbb{Z}_p^*$. Därför hittar vi alla kvadratiska rester i $\mathbb{Z}_p$ om vi vet en generator till K. Problemet är att vi i allmänhet inte har någon bra metod att hitta ett element som genererar K. Vad vi däremot vet är att eftersom K är en cyklisk delgrupp till $\mathbb{Z}_p^*$, så *finns* det alltid en generator till K, och detta faktum använder vi bland annat i beviset av Eulers kriterium. Eulers kriterium ger en effektiv metod att hitta kvadratiska rester i $\mathbb{Z}_p$, när p är ett primtal.

Eulers Kriterium $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, *där a och p är relativt prima, p är ett udda primtal och $\left(\frac{a}{p}\right)$ är Legendresymbolen.*

Bevis Välj en generator s i $\mathbb{Z}_p^*$. Sätt $s^n \equiv a$, där a är ett heltal och $(a,p) = 1$ enligt förutsättningar i satsen. Vi har att $a^{p-1} \equiv 1 \pmod p$ och därför $(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \pmod p$. Eftersom för jämna $n = 2m$ gäller att $\left(\frac{a}{p}\right) = 1$ har vi $s^{n(p-1)/2} = (s^{p-1})^m \equiv 1 \pmod p$ och alltså $a^{(p-1)/2} \equiv 1 \pmod p$. Vidare gäller att $p-1$ är det minsta talet sådant att $s^{p-1} \equiv 1 \pmod p$. Därför om $n = 2m+1$ är udda, det vill säga om $\left(\frac{a}{p}\right) = -1$, har vi att $a^{(p-1)/2} \equiv s^{m(p-1)} s^{(p-1)/2} \equiv -1 \pmod p$. □

4.1 Supplementära lagarna

När är -1 en kvadratisk rest modulo p? Vi ser direkt att för $p = 5$ gäller att $-1 \equiv 4 \pmod 5$ och 4 är en kvadrat modulo 5. Men däremot för $p = 7$ har vi att $-1 \equiv 6 \pmod 7$ inte är en kvadratisk rest eftersom 1,2,4 är de enda kvadratiska resterna modulo 7. För $p = 11$ respektive för $p = 13$ gäller att 1,3,4,5,9 respektive 1,3,4,9,10,12 är kvadratiska rester och enligt lemma 2.7 ovan finns det inga fler kvadratiska rester modulo 11 respektive modulo 13. Det börjar synas ett mönster att när $p = 5, 13 \equiv 1 \pmod 4$ så är -1 en kvadratisk rest, men när $p = 7, 11 \equiv 3 \pmod 4$, så är -1 en icke-kvadratisk rest. Följande sats brukar kallas den **första supplementära lagen** (till lagen om kvadratisk reciprocitet).

Sats 4.1 *-1 är en kvadratisk rest modulo ett udda primtal p omm $p \equiv 1 \pmod 4$.*

Bevis Eulers kriterium säger att $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, där a och p är relativt prima, varav p är ett primtal. Nu har vi att $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$, vilket direkt ger att $\left(\frac{-1}{p}\right) \equiv 1 \pmod p$ omm $p \equiv 1 \pmod 4$ eftersom för ett heltal m gäller att $p \equiv 1 \pmod 4$ omm $p = 4m + 1$ omm $(-1)^{(p-1)/2} = 1$. □

Den **andra supplementära lagen** lyder som följer:

Sats 4.2 *Låt p vara ett primtal. $\left(\frac{2}{p}\right) = 1$ omm $p \equiv \pm 1 \pmod 8$, $\left(\frac{2}{p}\right) = -1$ omm $p \equiv \pm 3 \pmod 8$, dvs $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.*

Bevis Vi har två fall att beakta:

(i) När $p \equiv 1$ eller $5 \pmod 8$, så är $\left(\frac{2}{p}\right) = (-1)^{(p-1)/4}$ eftersom

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)! = 2 \cdot 4 \cdot 6 \cdots (p-1) \equiv$$

$$2 \cdot 4 \cdot 6 \cdots \left(\frac{p-1}{2}\right) \cdot \left(-\frac{p-3}{2}\right) \cdots (-5)(-3)(-1) \equiv$$

$$(-1)^{(p-1)/4}\left(\frac{p-1}{2}\right)! \pmod p.$$

När vi nu dividerar med $\left(\frac{p-1}{2}\right)!$ får vi resultatet ovan med hjälp av Eulers kriterium. Därför har vi att $p \equiv 1 \pmod 8$ ger $\left(\frac{2}{p}\right) = +1$ och $p \equiv 5 \pmod 8$ ger $\left(\frac{2}{p}\right) = -1$.

(ii) När $p \equiv 3$ eller $7 \pmod 8$, så är $\left(\frac{2}{p}\right) = (-1)^{(p+1)/4}$. Vi har att

$$
\begin{aligned}
2^{(p-1)/2}\left(\frac{p-1}{2}\right)! &= 2\cdot 4\cdot 6\cdots(p-1) \\
&\equiv 2\cdot 4\cdot 6\cdots\left(\frac{p-3}{2}\right)\cdot\left(-\frac{p-1}{2}\right)\cdots(-5)(-3)(-1) \\
&\equiv (-1)^{(p+1)/4}\left(\frac{p-1}{2}\right)! \pmod p.
\end{aligned}
$$

Eulers kriterium ger nu att $\left(\frac{2}{p}\right) = (-1)^{(p+1)/4}$ så att för $p \equiv 3 \pmod 8$ gäller $\left(\frac{2}{p}\right) = -1$ och för $p \equiv 7 \pmod 8$ gäller $\left(\frac{2}{p}\right) = +1$. De två fallen kan sammanfattas som $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. □

4.2 Ett berömt lemma

Många bevis av lagen om kvadratisk reciprocitet bygger på lemmat nedan, som har fått dela namnet med många andra resultat upptäckta av talteoretikernas lärofader Gauss. Ett par beteckningar behövs. De kommer att användas i ett par bevis framöver:

Med de minsta resterna modulo p menas $-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, \frac{p-1}{2}$. Den **negativa halvklassen** modulo p är $\{-\frac{p-1}{2}, \ldots, -2, -1\}$ och den **positiva halvklassen** modulo p är $\{1, 2, \ldots, \frac{p-1}{2}\}$.

Låt a vara ett heltal och låt N beteckna de minsta rester modulo p som lämnas av $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ och som ligger i den negativa restklassen. Låt P beteckna mängden av de minsta rester modulo p som lämnas av samma element och inte ligger i N. Beteckna med μ antalet element i N. Då har vi:

Gauss lemma *Om $(a, p) = 1$, där a är ett heltal och p är ett primtal, så gäller*

$$\left(\frac{a}{p}\right) \equiv (-1)^{\mu}.$$

Bevis För $1 \leq i \leq (p-1)/2$ låt $[ia]$ beteckna den minsta rest modulo p som lämnas av respektive $a, 2a, 3a, \cdots, \frac{p-1}{2}a$. Då har vi $\{1, \ldots, \frac{p-1}{2}\} = \{-[ia] \mid [ia] \in N\} \cup P$. Om man antar motsatsen, så måste gälla att för några heltal i och j i intervallet $1 \leq i, j \leq (p-1)/2$ är $ia \equiv ja \pmod p$. Därför $a(i-j) \equiv 0 \pmod p$. Men $p \nmid a$ medför att $i \equiv j \pmod p$ och $1 \leq i, j \leq (p-1)/2$ ger nu att $i = j$.

Eftersom μ är antalet element i N har vi följande kongruenser, (där den sista följer av Eulers kriterium):

$$(-1)^{\mu} \left(\frac{p-1}{2}\right)! \equiv a \cdot 2a \cdot 3a \cdots \frac{p-1}{2} a \pmod p$$

och

$$a \cdot 2a \cdot 3a \cdots \frac{p-1}{2} a = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right) \left(\frac{p-1}{2}\right)! \pmod p.$$

Dividera med $\left(\frac{p-1}{2}\right)!$ och vi har att $(-1)^{\mu} \equiv \left(\frac{a}{p}\right) \pmod p$, vilket medför $(-1)^{\mu} = \left(\frac{a}{p}\right)$. $\square$

Nu använder vi Gauss lemma för att en gång till beräkna värdet av Legendresymbolen $\left(\frac{2}{p}\right)$. Det räcker att bestämma pariteten på antalet element i N modulo p, där N definieras som ovan för $a = 2$.

Bevis 2 av andra supplementära lagen Elementen $x \in N$ uppfyller $(p+1)/2 \leq x \leq p-1$, där x är ett jämnt heltal. Vi har två fall att beakta:

(i) Om $p = 4k+1$ så har vi $2k+1 \leq x \leq 4k$, det vill säga $k + 1/2 \leq x/2 \leq 2k$ och vi har att $k+1 \leq x/2 \leq 2k$. x antar alltså k jämna heltalsvärden i den negativa halvklassen, vilket, enligt Gauss lemma $\left(\frac{2}{p}\right) = (-1)^k$ betyder att 2 är en kvadratisk rest när k är jämnt och en icke-kvadratisk rest när k är udda. Alltså gäller:

$$p \equiv 1 \pmod 8 \Rightarrow 2 \text{ är kvadratisk rest modulo } p$$

$$p \equiv -3 \pmod 8 \Rightarrow 2 \text{ är icke-kvadratisk rest modulo } p.$$

(ii) Om $p = 4k+3$ så är $(4k+4)/2 \leq x \leq 4k+2$. När vi förkortar med 2 får vi, $k+1 \leq x/2 \leq 2k+1$ och vi har att x antar $k+1$ jämna heltalsvärden i negativa halvklassen. Enligt Gauss lemma är $\left(\frac{2}{p}\right) = (-1)^{k+1}$. Därför gäller i det här fallet att 2 är en kvadratisk rest om och endast om k är udda. Vi har:

$$p \equiv -1 \pmod 8 \Rightarrow 2 \text{ är kvadratisk rest modulo } p$$

$$p \equiv 3 \pmod 8 \;\Rightarrow\; 2 \text{ är en icke-kvadratisk rest modulo } p.$$

$\square$

5 Legendresymbolen och Jacobisymbolen

Nu tittar vi på några av Legendresymbolens egenskaper, för att sedan definiera och förklara Jacobisymbolen utifrån Legendresymbolen. I ett senare avsnitt kommer vi att beröra den allmänna teorin för karaktärer, där Legendresymbolen är ett specialfall.

Lemma 5.1 *Antag att p är ett udda primtal, Då gäller:*

(i) $a \equiv b \pmod p$ *medför* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(iii) $\left(\frac{a^2}{p}\right) = 1$ *om* $(a,p) = 1$;

(iv) $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$ *om* $(a,p) = 1$.

Alla påståenden ovan följer direkt ur definitionen av Legendresymbolen, eller från Eulers kriterium. (ii) verifieras på följande sätt:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}}(b)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p.$$

Säg att vi vill beräkna Legendresymbolen för riktigt stora tal. För att kunna använda reciprocitetslagen effektivt krävs att vi kan primtalsfaktorisera dessa stora tal. Det finns till dags dato inga snabba sätt att göra detta på. Hur som helst finns en metod som inte kräver faktorisering, förutom att bryta ut potenser av 2, vilket är mycket enkelt. Nu behöver vi Jacobisymbolen. Den definieras här som produkten av Legendresymboler enligt följande:

Definition 5.1 *Låt a vara ett heltal, och låt $n > 1$ vara ett udda heltal. Låt $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ vara primfaktoriseringen av n. Då definierar vi Jacobisymbolen $\left(\frac{a}{n}\right)$ som produkten av Legendresymboler:*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Vi behöver vara försiktiga här, för det innebär inte alls med säkerhet att a är en kvadratisk rest om Jacobisymbolen $\left(\frac{a}{n}\right) = 1$. När n är ett primtal, så sammanfaller Jacobisymbolen med Legendresymbolen och vi kan dra slutsatsen att a är en kvadratisk rest, men om n kan faktoriseras, säg $n = pq$, så kan ju $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 1$ innebära att a varken är en kvadratisk rest modulo p eller modulo q och inte heller modulo n. Till exempel finns ingen heltalslösning till ekvationen $x^2 \equiv 2 \pmod{15}$, fastän att $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$.

Nu vill vi veta hur reciprocitetslagens generalisering till Jacobisymbolen ser ut. Först en beskrivning av andra supplementära lagen för Jacobisymbolen:

Sats 5.2 *För ett udda heltal $n > 1$ har vi att* $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

Bevis Låt $f(n) = (-1)^{(n^2-1)/8}$. Om $n = n_1 n_2$ ser vi genom att granska alla fallen för n_1 och n_2 modulo 8 att:

$$f(n) = f(n_1)f(n_2) = \begin{cases} 1 & \text{om } |n_1| \equiv |n_2| \equiv 1 \pmod{8}, \\ 1 & \text{om } |n_1| \equiv |n_2| \equiv 3 \pmod{8}, \\ -1 & \text{om } |n_1| \not\equiv |n_2| \pmod{8}. \end{cases}$$

Till exempel, om $n_1 \equiv 3 \pmod{8}$ och $n_2 \equiv 5 \pmod{8}$ får vi att $f(3)f(5) = (-1)^{(3^2-1)/8}(-1)^{(5^2-1)/8} = 1$. Dessutom är givetvis $3 \cdot 5 = 15 \equiv -1 \pmod{8}$ och $f(-1) = (-1)^{((-1)^2-1)/8} = 1$. Alltså om $n = n_1 n_2$, gäller $f(n) = f(n_1)f(n_2)$. Det följer sedan från Definition 5.1, samt andra supplementära lagen för Legendresymbolen, att när $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, så är

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right)^{\alpha_1} \cdots \left(\frac{2}{p_r}\right)^{\alpha_r} = f(p_1)^{\alpha_1} \cdots f(p_r)^{\alpha_r} = f(n).$$

□

Reciprocitetslagen för Jacobisymbolen *För två udda heltal $n > 1$ och $m > 1$ har vi att*

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4} \left(\frac{n}{m}\right).$$

Bevis Först noterar vi att om m och n har en gemensam faktor, så följer det från definitionen av Legendre- och Jacobisymbolen att båda sidorna är noll. Antag därför att $(m,n) = 1$. Därefter skriver vi m respektive n, som en produkt av primtal: $n = p_1 p_2 \cdots p_r$ och $m = q_1 q_2 \cdots q_s$ (här tillåts upprepningar av samma primfaktorer, dvs m eller n får innehålla en kvadratfaktor). När vi konverterar från $\left(\frac{n}{m}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right)$ till $\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{q_j}{p_i}\right)$ måste vi tillämpa kvadratiska reciprocitetslagen rs antal gånger. När både p_i och q_j $\equiv 3 \pmod 4$ så är $\left(\frac{q_j}{p_i}\right) = -\left(\frac{p_i}{q_j}\right)$. Vi ser nu att för udda heltaltal som m och n att endast när ett udda antal primfaktorer är kongruenta med 3 modulo 4 för både m och n, så är $\left(\frac{m}{n}\right) \equiv -\left(\frac{n}{m}\right)$. Dessutom är $m \equiv 3 \pmod 4$ omm $q_j \equiv 3 \pmod 4$ för ett udda antal j. Motsvarande gäller givetvis för n och p_i. När antalet q_j eller $p_i \equiv 3 \pmod 4$ är jämnt har vi att $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)$. Satsen följer härmed. □

Exempel 5.1 Om vi nu vill beräkna Legendresymbolen från exemplet i inledningen, som visar att 7411 är en icke-kvadratisk rest modulo 9283, utan att behöva faktorisera 1872, mer än att bryta ut största potensen av 2, så använder vi reciprocitetslagen för Jacobisybolen på följande sätt:

$$\left(\frac{1872}{7411}\right) = \left(\frac{16}{7411}\right)\left(\frac{117}{7411}\right) = \left(\frac{7411}{117}\right) = \left(\frac{40}{117}\right) =$$

$$\left(\frac{2}{117}\right)\left(\frac{5}{117}\right) = -\left(\frac{117}{5}\right) = -\left(\frac{2}{5}\right) = 1.$$

Jacobisymbolen har många tillämpningar. Till exempel kan med hjälp av Jacobisymbolen visas att för ett godtyckligt udda heltal a finns det oändligt många primtal för vilka a är en icke-kvadratisk rest (se [5]).

6 Några bevis av lagen om kvadratisk reciprocitet

Med hjälp av Gauss Lemma kunde vi bestämma alla primtal p för vilka 2 är en kvadratisk rest. Det vore naturligtvis möjligt att byta ut 2 mot ett annat heltal $a > 2$ och i varje enskilt fall med hjälp av Gauss lemma, bestämma för vilka primtal som a är en kvadratisk rest (till exempel för $(\frac{7}{p})$ behöver vi i sådana fall räkna antalet element i den negativa halvklassen bland $7j \pmod{28}$ då $1 \leq j \leq (p-1)/2$). Detta är en smula omständligt, för med hjälp av kvadratiska reciprocitetslagen, som vi bevisar för alla primtalspar p, q, blir frågan om att bestämma alla primtal för vilka ett heltal a är en kvadratisk rest en rutinberäkning. Nu beskriver vi några bevis av reciprocitetslagen.

6.1 Ett vanligt förekommande bevis av lagen om kvadratisk reciprocitet

Beviset nedan är snarlikt Gauss tredje bevis från år 1808, se vidare sektion 6.3. Det har en enkel geometrisk tolkning, men kan tyvärr inte generaliseras till andra kroppsutvidgningar eller högre graders reciprocitetslagar.

Låt p, q vara primtal. Låt $(\frac{q}{p}) = (-1)^{\mu}$ respektive $\left(\frac{p}{q}\right) = (-1)^{\nu}$, där μ och ν definieras som innan Gauss lemma på sidan 16. Vi skall använda oss av en väldigt enkel idè i vårt första bevis av reciprocitetslagen. När μ summeras med ν får vi samma resultat modulo 2 som när vi räknar antalet heltalskombinationer (x, y) för $0 < x < \frac{p}{2}$ och $0 < y < \frac{q}{2}$. Dessa är givetvis $(p-1)(q-1)/4$ till antalet. Gauss lemma medför därför att $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\mu+\nu} = (-1)^{(p-1)(q-1)/4}$, vilket stämmer överens med formulering (ii) i reciprocitetslagen på sidan 11.

Bevis av kvadratiska reciprocitetslagen. Låt x, y, p, q vara heltal, varav p, q är primtal. För alla x med $0 < x < p/2$ och egenskapen att qx tillhör den negativa halvklassen modulo p, gäller att olikheten

$$-p/2 < \ qx - py < \ 0 \tag{8}$$

har en heltalig lösning y. Detta y är ett av talen $1, \dots, (q-1)/2$ eftersom å ena sidan kan vi välja y större än noll, men å andra sidan gäller

$$py < \; qx + p/2 < \; qp/2 + p/2 = \; p(q+1)/2,$$

så att

$$0 < \; y < \; (q+1)/2. \tag{9}$$

Låt μ beteckna antalet heltalskombinationer (x, y), som uppfyller villkoren (8) och (9) samt $0 < x < p/2$.

På motsvarande sätt beräknas enkelt, för alla y med $0 < y < q/2$ och med egenskapen att py tillhör den negativa halvklassen modulo q, att

$$-q/2 < \; py - qx < \; 0 \tag{10}$$

har en heltalig lösning x, där även

$$0 < \; x < \; (p+1)/2. \tag{11}$$

Låt ν beteckna antalet heltalskombinationer (x, y) som uppfyller villkoren (10) och (11) samt $0 < y < q/2$.

Betrakta nu avbildningen

$$(x, y) \mapsto \; (x', y'),$$

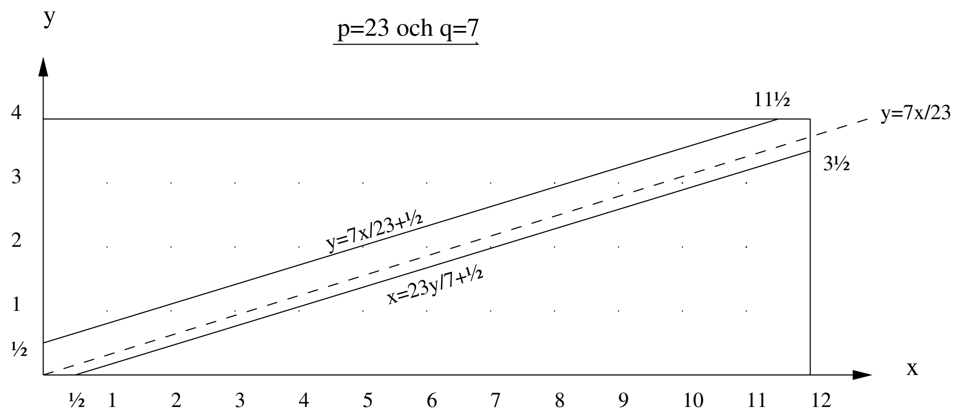
som ges av

$$(x', y') = \; \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y \right). \tag{12}$$

Denna avbildning gör att alla par (x, y) flyttas symmetriskt runt punkten $(k, l) = (\frac{p+1}{4}, \frac{q+1}{4})$ och detta visar att vi alltid har ett jämnt antal gitterpunkter i områdena utanför mittremsan $M = \; \{x, y \mid \; x, y \in \mathbb{Z}, \; \frac{q}{p}(x - \frac{1}{2}) <$

$y < \frac{q}{p}x + \frac{1}{2}\}$, men fortfarande inne i kvadraten $K = \{x, y \mid x, y \in \mathbb{Z},\ 0 < x < (p+1)/2,\ 0 < y < (q+1)/2\}$. Men antalet gitterpunkter i mittremsan M är, enligt vår konstruktion, lika med värdet av $\mu + \nu$. Vi har därför att $\mu + \nu$ är udda om och endast om $\frac{p-1}{2} \cdot \frac{q-1}{2}$ är udda. Gauss lemma applicerat på både $\left(\frac{p}{q}\right)$ och $\left(\frac{q}{p}\right)$ medför lagen om kvadratisk reciprocitet, eftersom $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu}(-1)^{\nu} = (-1)^{\mu+\nu} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. $\square$

Anmärkning Vi kan se med hjälp av vår avbildning (12) att $\mu+\nu$ antar ett udda värde om och endast om mittpunkten (k, l) i rektangeln är en gitterpunkt, det vill säga om och endast om k och l är heltal. Men $k = (p+1)/4$ och $l = (q+1)/4$ är heltal omm $p \equiv 3 \pmod 4$ och $q \equiv 3 \pmod 4$. Alltså $\left(\frac{p}{q}\right) \neq \left(\frac{q}{p}\right)$ omm $p \equiv q \equiv 3 \pmod 4$. Detta är formulering (i) av reciprocitetslagen på sidan 11.



Figur 1 Låt $p = 23$ och $q = 7$. Diagrammet visar alla gitterpunkter (x, y) inuti rektangeln som begränsas av $0 < y < (q+1)/2$ och $0 < x < (p+1)/2$. Vi har att inga gitterpunkter ligger på någon av linjerna $y = qx/p$, $-p/2 = qx - py$, $qx - py = q/2$, eftersom p och q är relativt prima. Området mellan $y = qx/p$ och $y = qx/p + 1/2$ innehåller alla gitterpunkter (x, y), för vilka qx tillhör negativa halvklassen modulo p, och området mellan $y = qx/p$ och $x = py/q + 1/2$ innehåller på motsvarande sätt alla gitterpunkter för vilka py tillhör negativa halvklassen modulo q.

6.2 En variation på temat

Den följande satsen är ekvivalent med den moderna formuleringen av lagen om kvadratisk reciprocitet. Enligt [1] var det Euler som först formulerade den efter att ha granskat flera specialfall av kvadratisk reciprocitet, se Kapitel 3. Satsen säger att för ett heltal a och ett udda primtal p beror värdet av Legendresymbolen $\left(\frac{a}{p}\right)$ endast på resten när p delas med $4a$. Mera precist gäller följande:

Sats 6.1 *Låt p och q vara distinkta udda primtal och antag att $(a,p) = (a,q) = 1$, där a är ett positivt heltal. Om $q \equiv p \pmod{4a}$ eller $q \equiv -p \pmod{4a}$, då är $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$.*

Bevis Låt $S = \{a, 2a, 3a, \dots, \frac{p-1}{2}a\}$. Beteckna med μ antalet element ur S som ligger i den negativa halvklassen modulo p. Då är μ antalet element ur S i intervallen:

$$\left(\frac{p}{2}, p\right), \left(\frac{3p}{2}, 2p\right), \left(\frac{5p}{2}, 3p\right), \dots, \left(\frac{2c-1}{2}p, cp\right),$$

där $c = a/2$ om a är jämnt och $c = (a-1)/2$ om a udda. Om vi delar ut med a alla element i intervallen ovan, så får vi följande intervall:

$$\left(\frac{p}{2a}, \frac{p}{a}\right), \left(\frac{3p}{2a}, \frac{2p}{a}\right), \dots, \left(\frac{2c-1}{2a}p, \frac{cp}{a}\right). \tag{13}$$

μ är antalet *heltal* i alla dessa intervall.

De element ur S som tillhör negativa halvklassen modulo q, kan på liknande sätt beskrivas som mängden heltal i intervallserien:

$$\left(\frac{q}{2a}, \frac{q}{a}\right), \left(\frac{3q}{2a}, \frac{2q}{a}\right), \left(\frac{5q}{2a}, \frac{3q}{a}\right), \dots, \left(\frac{2c-1}{2a}q, \frac{cq}{a}\right). \tag{14}$$

Låt m vara ett heltal. Vi skall nu visa att pariteten av antalet element i (14) är densamma som pariteten av μ, både för $q = 4am+p$ och för $q = 4am-p$.

När $q = 4am+p$ får vi genom insättning i den senaste intervalluppsättningen,

$$\left(2m + \frac{p}{2a},\ 4m + \frac{p}{a}\right), \left(6m + \frac{3p}{2a},\ 8m + \frac{2p}{a}\right), \dots,$$

$$\left(2(2c-1)m + \frac{2c-1}{2a}p,\ 4cm + \frac{cp}{a}\right). \tag{15}$$

Eftersom en förflyttning med ett jämnt heltal från vilket som helst av intervallgränserna inte kommer att påverka pariteten av antalet heltal i intervallet, så inses att intervallen i (13) och (15) innehåller lika många heltal modulo 2. Därför följer satsen ur Gauss lemma i fallet $q = 4am + p$.

När $q = 4am - p$ kan vi skriva (14) som följande intervallserie:

$$\left(2m - \frac{p}{2a}, 4m - \frac{p}{a}\right),\ \left(6m - \frac{3p}{2a},\ 8m - \frac{2p}{a}\right), \ldots,$$

$$\left(2(2c-1)m - \frac{2c-1}{2a}p,\ 4cm - \frac{cp}{a}\right). \tag{16}$$

Det är inte riktigt lika självklart att pariteten på antalet heltal i dessa intervall är densamma som för (13). Det krävs en viss försiktighet i manipuleringen av intervallgränserna. Låt $n(u, v)$ beteckna antalet heltal i intervallet (u, v). Subtrahera bort $2m$ från båda intervallgränserna av det första intervallet i (16) och spegla sedan i punkten 0. Då har vi att $n(2m - p/2a, 4m - p/a) = n(p/a - 2m, p/2a)$. Låt nu $A = (p/2a, p/a), B = (p/a - 2m, p/2a), C = (p/a - 2m, p/a)$ då har vi att $nA + nB = nC$, eftersom punkten $p/2a$ inte kan vara ett heltal, men $nC = 2m$ så $nA \equiv nB \pmod 2$. Samma argument håller för vilket som helst intervall i (13) och motsvarande intervall i (16). Alltså har antalet heltal i intervall (16) samma paritet som i intervall (13) och Gauss lemma ger att $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$. $\square$

Nu visar vi att Sats 6.1 är ekvivalent med reciprocitetslagen. Det följer av räknereglerna för Legendresymbolen, samt av värdet av $\left(\frac{-1}{q}\right)$.

Bevis av reciprocitetslagen. Om $q = p + 4m$ så gäller,

$$\left(\frac{q}{p}\right) = \left(\frac{p+4m}{p}\right) = \left(\frac{4m}{p}\right) = \left(\frac{m}{p}\right),$$

och

$$\left(\frac{p}{q}\right) = \left(\frac{q-4m}{q}\right) = \left(\frac{-4m}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{m}{q}\right).$$

Föregående sats är ekvivalent med reciprocitetslagen i det här fallet eftersom $\left(\frac{-1}{q}\right) = -1$ omm $p \equiv q \equiv 3 \pmod 4$. När $q = -p + 4m$, det vill säga när $p \not\equiv q \pmod 4$, har vi att

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4m}{q}\right) = \left(\frac{4m}{q}\right) = \left(\frac{m}{q}\right) = \left(\frac{m}{p}\right) = \left(\frac{-p+4m}{p}\right) = \left(\frac{q}{p}\right),$$

vilket även här medför att Sats 6.1 är ekvivalent med reciprocitetslagen. □

6.3 Golvfunktionen och Gauss tredje bevis.

Ideérna i beviset nedan är ur Gauss tredje bevis av Reciprocitetslagen, men år 1844 publicerade den då 21-årige Eisenstein förenklingar av beviset.

Låt oss använda följande standard-beteckning för golvfunktionen, $\lfloor\cdot\rfloor$, det största heltalet mindre än eller lika med ett givet reellt tal.

Betrakta primtalen q, p. Vi definierar

$$M = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor,$$

och

$$L = \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor.$$

Vi skall visa att $M \equiv \mu \pmod 2$ där μ definieras som på sidan 16, innan Gauss lemma, här med $a = q$. Sedan räcker det att visa,

$$M+L=\sum_{x=1}^{(p-1)/2}\left\lfloor\frac{qx}{p}\right\rfloor+\sum_{y=1}^{(q-1)/2}\left\lfloor\frac{py}{q}\right\rfloor=(q-1)(p-1)/4,$$

vilket med ens medför lagen om kvadratisk reciprocitet.

Bevis Låt $x\in\{1,\dots,(p-1)/2\}$. Dela qx med p. Divisionsalgoritmen ger att det finns heltal m_x och t_x med $0\le t_x\le p-1$, sådana att $qx=pm_x+t_x$. Eftersom $t_x\ne 0$ är minsta rest för qx modulo p ser vi att $m_x=\lfloor\frac{qx}{p}\rfloor$. Därför $qx=p\lfloor\frac{qx}{p}\rfloor+t_x$, och om vi summerar från $x=1$ till $x=(p-1)/2$ på båda sidorna har vi

$$\sum_{x=1}^{(p-1)/2}qx=\sum_{x=1}^{(p-1)/2}p\left\lfloor\frac{qx}{p}\right\rfloor+\sum_{x=1}^{(p-1)/2}t_x.$$

En enkel beräkning ger att $\sum_{x=1}^{(p-1)/2}x=(p^2-1)/8$.

Skriv nu $\sum_{x=1}^{(p-1)/2}t_x=\sum_{x=1}^{\mu}(p+a_x)+\sum_{x=1}^{p-\mu}b_x=p\mu+A+B$, där $a_x\in N$ och $b_x\in P$ med beteckningar från innan Gauss lemma på sidan 16, och dessutom med $A:=\sum_{x=1}^{\mu}a_x,\ B:=\sum_{x=1}^{p-\mu}b_x$.

Nu ser vi att det å ena sidan gäller,

$$q\frac{p^2-1}{8}=p\sum_{x=1}^{(p-1)/2}\left\lfloor\frac{qx}{p}\right\rfloor+\sum_{x=1}^{(p-1)/2}t_x=pM+p\mu+A+B,\tag{17}$$

men å andra sidan medför $\{1,\dots,(p-1)/2\}=\{-a_x\}_{x=1}^{\mu}\cup\{b_x\}_{x=1}^{p-\mu}$ att

$$\frac{p^2-1}{8}=\sum_{x=1}^{\mu}(-a_x)+\sum_{x=1}^{p-\mu}b_x=-A+B.\tag{18}$$

Om vi nu subtraherar (18) från (17) får vi

$$(q-1)(p^2-1)/8=p(M+\mu)+2A.$$

Vi har här ett jämnt heltal i vänsterledet, eftersom q, p är udda primtal och $8 \mid (p^2 - 1)$ för alla udda heltal p, men i högerledet har vi ett jämnt heltal om och endast om $M \equiv \mu \pmod 2$.

Den första delen av beviset är nu klar, men det återstår att visa att $M + L = (q-1)(p-1)/4$. Först noterar vi därför att det finns exakt $(q-1)(p-1)/4$ gitterpunkter strikt inne i rektangeln med hörn i punkterna

$$(0,0),\ (0,q/2),\ (p/2,0),\ (p/2,q/2).$$

Drag nu diagonalen $y = px/q$. Notera att vi inte kan ha några gitterpunkter på $y = px/q$ eftersom $(q,p) = 1$. Låt oss beteckna området i rektangeln under diagonalen för U. Om d är ett heltal med $0 < d < p/2$ så har vi $\left\lfloor \frac{qd}{p} \right\rfloor$ heltalsvärden rakt ovanför d i U. Alltså är antalet gitterpunkter i U lika med $M = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor$.

Beteckna området i rektangeln ovanför diagonalen för O. Vi ser på motsvarande sätt att antalet gitterpunkter i O är $L = \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor$. Nämligen om vi låter c vara ett heltal med $0 < c < q/2$, så har vi $\left\lfloor \frac{pc}{q} \right\rfloor$ heltalsvärden rakt till höger om c i O. Nu ser vi att $M + L = (q-1)(p-1)/4$ och beviset är klart. $\square$

6.4 Eisensteins analytiska bevis

Eisensteins bevis av lagen om kvadratisk reciprocitet använder sig av sinusfunktionens periodicitet och bygger på en omformulering av Gauss lemma. Vad vi behöver här är en funktion $f : \mathbb{Q} \to \mathbb{C}$ med tre egenskaper:

(1) Heltalsperiodicitet, det vill säga, för $z \in \mathbb{Q}$, med $n \in \mathbb{Z}$, gäller $f(z) = f(z+n)$,
(2) $f(z)$ skall vara en udda funktion, det vill säga $f(-z) = -f(z)$ och
(3) $f(nz) = \prod_l f(z + \frac{l}{n})$, där l löper över ett godtyckligt representantsystem för alla rester modulo n.

Gauss använde sig av funktionen $z \mapsto (-1)^{\lfloor z \rfloor}$ i ett av sina bevis, men här använder vi oss alltså av Eisensteins förslag. Kandidaten är

$$F : z \mapsto 2i \sin 2\pi z.$$

Lemmermeyer skriver i sin bok [6] att denna ide "...knappast kan överskattas: slutligen ledde den Eisenstein till upptäckten av de enklaste bevis av kubisk och kvadratisk reciprocitet som man kan föreställa sig." I [4] har man inkluderat Eisensteins bevis av kvadratisk reciprocitet för att man anser det vara "ingenious", men på andra ställen har man sagt att det är en smart vidareutveckling av Gauss ideer, som tydde på Eisenstens genialitet, men att hans bevis går tyvärr inte att vidareutveckla på samma sätt som Gausssummorna, vilka har generaliseringar till allmännare reciprocitetslagar. Det råder visst en delad mening här. Lemmermeyer skriver i [6] att det troligtvis är möjligt att generalisera det analytiska beviset bortom kubisk och kvadratisk reciprocitet, men att det ännu inte är någon som tagit sig för uppgiften. För generaliseringen till bikvadratisk reciprocitet, se [6] sidan 251, krävs teorin om elliptiska kurvor. Hur som helst, presenterar vi nu Eisensteins bevis av kvadratisk reciprocitet som utnyttjar sinusfunktionens egenskaper på ett smart sätt. Vi följer huvudsakligen ett bevis av David R. Hayes, nerladdat från internet, sidan:
www.umastr1.math.umass.edu/~holden/Math471/qrl-rev/

Proposition 6.2 (Gauss lemma enligt Eisenstein.) *Låt* $A = \{\alpha \in \mathbb{Z} \mid 0 < \alpha < (p+1)/2\}$ *vara en halvklass modulo ett udda primtal* p. *Då gäller:*

$$\left(\frac{a}{p}\right) = \prod_{\alpha \in A} \frac{\sin\left(\frac{2\pi}{p} a\alpha\right)}{\sin\left(\frac{2\pi}{p}\alpha\right)}.$$

Bevis Titta på högerledet. Där finns inget μ (= antalet representanter av $a\alpha$ i den negativa halvklassen), som vi är vana vid från Gauss lemma. Men vi skall visa att uttrycket är lika med $(-1)^{\mu}$. Låt oss beteckna, med N mängden av alla element $a\alpha \equiv u$ som ligger i den negativa halvklassen, och med P motsvarande mängd av element $a\alpha \equiv v$ som ligger i den positiva halvklassen. Nu ser vi att μ är antalet $u \in N$. Sätt:

$$E = \prod_{\alpha \in A} \frac{\sin\left(\frac{2\pi}{p} a\alpha\right)}{\sin\left(\frac{2\pi}{p}\alpha\right)} = \frac{\prod_{\alpha \in A} \sin\left(\frac{2\pi}{p} a\alpha\right)}{\prod_{\alpha \in A} \sin\left(\frac{2\pi}{p}\alpha\right)}.$$

Nu uttnyttjar vi att $\sin(\frac{2\pi}{p}\alpha)$ är periodisk med period p, det vill säga att för $c \equiv d \pmod p$ har vi $\sin(\frac{2\pi}{p}c) = \sin(\frac{2\pi}{p}d)$.

$$E = \frac{\prod_{v \in N} \sin\left(\frac{2\pi}{p} v\right) \prod_{u \in P} \sin\left(\frac{2\pi}{p} u\right)}{\prod_{\alpha \in A} \sin\left(\frac{2\pi}{p}\alpha\right)}.$$

Här utnyttjar vi att sinus är en udda funktion:

$$E = \frac{\prod_{v \in N} - \sin\left(\frac{2\pi}{p}(-v)\right) \prod_{u \in P} \sin\left(\frac{2\pi}{p} u\right)}{\prod_{\alpha \in A} \sin\left(\frac{2\pi}{p}\alpha\right)}$$

Nu ser vi att:

$$E = (-1)^{\mu} \frac{\prod_{v \in N} \sin\left(\frac{2\pi}{p}(-v)\right) \prod_{u \in P} \sin\left(\frac{2\pi}{p} u\right)}{\prod_{\alpha \in A} \sin\left(\frac{2\pi}{p}\alpha\right)} =$$

$$(-1)^{\mu}\frac{\prod_{\alpha\in A}\sin\left(\frac{2\pi}{p}\alpha\right)}{\prod_{\alpha\in A}\sin\left(\frac{2\pi}{p}\alpha\right)}=(-1)^{\mu},$$

där vi liksom i beviset av Gauss lemma, sidan 16, använt oss av att eftersom a och p är relativt prima så är $\{-v \mid v\in N\}\cup\{u\mid u\in P\}=A$.

För beviset av reciprocitetslagen behöver vi den trigonometriska identiteten:

$$\sin(nx)=2^{n-1}\prod_{r=0}^{n-1}\sin\left(x+\frac{r\pi}{n}\right), \tag{19}$$

För bevis av identiteten, se [4], Lemma på sidan 59.

Om i denna likhet n är udda så gäller:

$$\prod_{l=1}^{n-1}\sin\left(x+\frac{2l\pi}{n}\right)=(-1)^{(n-1)/2}\prod_{r=1}^{n-1}\sin\left(x+\frac{r\pi}{n}\right). \tag{20}$$

För att bevisa (20) låt $2l:=r_l+nt_l$, där r_l är den minsta positiva resten modulo n. Nu har vi,

$$\prod_{l=1}^{n-1}\sin\left(x+\frac{2l\pi}{n}\right)=\prod_{l=1}^{n-1}\sin\left(x+\frac{r_l\pi}{n}+t_l\pi\right)=\prod_{l=1}^{n-1}\sin\left(x+\frac{r_l\pi}{n}\right)\cdot(-1)^{t_l}$$

$$(-1)^{(n-1)/2}\prod_{l=1}^{n-1}\sin\left(x+\frac{r_l\pi}{n}\right)=(-1)^{(n-1)/2}\prod_{r=1}^{n-1}\sin\left(x+\frac{r\pi}{n}\right),$$

eftersom exakt hälften av talen t_l är udda (=1). När n är udda kan vi nu skriva om (20) som

$$F(nx)=\prod_{l=0}^{n-1}F\left(x+\frac{l}{n}\right), \tag{21}$$

där $F(x) = 2i\sin(2\pi x)$.

Enligt Proposition 6.2 följer att Legendresymbolen kan skrivas som

$$\left(\frac{q}{p}\right) = \prod_{a=1}^{(p-1)/2} \frac{F(aq/p)}{F(a/p)}.$$

Låt nu $x = a/p$ och $n = q$. Då l löper över alla rester mellan $-q/2$ och $q/2$ i (21) får vi (eftersom l kan löpa över ett godtyckligt representantsystem modulo p):

$$\frac{F(aq/p)}{F(a/p)} = \frac{\prod_{l=-(q-1)/2}^{(q-1)/2} F\left(\frac{a}{p}+\frac{l}{q}\right)}{F(a/p)} = \prod_{l=1}^{(q-1)/2} F\left(\frac{a}{p}+\frac{l}{q}\right) F\left(\frac{a}{p}-\frac{l}{q}\right).$$

Alltså är

$$\left(\frac{q}{p}\right) = \prod_{a=1}^{(p-1)/2} \prod_{l=1}^{(q-1)/2} F\left(\frac{a}{p}+\frac{l}{q}\right) F\left(\frac{a}{p}-\frac{l}{q}\right),$$

och eftersom vi på liknande sätt har att

$$\left(\frac{p}{q}\right) = \prod_{a=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} F\left(\frac{a}{q}+\frac{l}{p}\right) F\left(\frac{a}{q}-\frac{l}{p}\right),$$

och $F(\frac{a}{q}-\frac{l}{p}) = -F(\frac{l}{p}-\frac{a}{q})$ så är produkten av $(p-1)(q-1)/4$ minustecken det enda som skiljer uttrycken från varandra. Därför följer nu lagen om kvadratisk reciprocitet:

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

□

7 Gausssummor, ändliga talkroppar och kvadratisk reciprocitet

När Gauss år 1818 publicerade sitt 6:e bevis av kvadratisk reciprocitet under titeln, "Neue Beweise und Erweiterungen des Fundamentalsatzes in der Lehre von den Quadratishe Resten", hade han sökt i många år efter en metod som generaliserar till kubisk och bikvadratisk reciprocitet. Nu hade hans sökande krönts med framgång, skriver han själv i inledningen till denna artikel. "...die unermüdliche Arbeit wurde endlich von glücklige erfolge gekrönt." Han skriver vidare att syftet med att publicera sitt sjätte bevis var att säga farväl till den delen av den "högre aritmetiken" som behandlar kvadratisk reciprocitet. Beviset som vi ger ser lite annorlunda ut än Gauss ursprungliga. Dedekind introducerade begreppen *algebraiska tal* och *algebraiska heltal* först år 1893, men de hade använts långt tidigare av Eisenstein, Jacobi, med flera. Gauss egen version av Gaussumma är polynomet $f_k(x) = \sum_t \chi(t)x^{kt}$, men vi skall använda den modernare varianten, med $x = \zeta_p$, där ζ_p är en primitiv p:te enhetsrot, se Proposition 7.9. Denna observation gjordes bland andra av Eisenstein, en av Gauss mest begåvade elever, som tyvärr dog ung, vid 29 års ålder. Eisenstein lyckades, både med analytiska och algebraiska metoder, bevisa de generaliseringar från kvadratisk reciprocitet till kubisk och bikvadratisk reciprocitet, som Gauss hade sökt så länge, men inte nått riktigt ända fram till.

Generaliseringarna av kvadratisk reciprocitet till kubisk och bikvadratisk reciprocitet (eller för den del även till kvadratisk reciprocitet i andra ringutvidgningar, som till exempel $\mathbb{Z}[i]$ - bevisat av L. Dirichlet cirka 1830), vore en spännande fortsättning av examensarbetet. Den intresserade läsaren hänvisas till [2], [4] och [6].

Definition 7.1 *Ett* algebraiskt tal *är ett komplext tal α som är en rot till en ekvation $\sum_{i=0}^{n} a_i x^{n-i} = 0$, där $a_i \in \mathbb{Q}$ och $a_0 \neq 0$.*
Ett algebraiskt heltal *ω är ett komplext tal, som är en rot till en ekvation $\sum_{i=0}^{n} a_i x^{n-i} = 0$, där $a_i \in \mathbb{Z}$ och $a_0 = 1$.*

Direkt från definitionen följer att varje algebraiskt heltal är ett algebraiskt tal, men omvändningen gäller inte. Nämligen:

Proposition 7.1 *Ett rationellt tal $r \in \mathbb{Q}$ är ett algebraiskt heltal då och endast då $r \in \mathbb{Z}$.*

Det viktiga resultatet i denna sektion är att de algebraiska talen bildar en kropp och de algebraiska heltalen utgör en ring.

Sats 7.2 *Mängden av algebraiska tal är en delkropp av den komplexa kroppen $\mathbb{C}$.*

Sats 7.3 *Mängden av algebraiska heltal bildar en delring till kroppen av de algebraiska talen.*

För bevis av dessa två satser se [7], Kapitel 2.

Låt nu Ω beteckna ringen av algebraiska heltal. Om $\omega_1, \omega_2, \gamma \in \Omega$, så säger vi att $\omega_1 \equiv \omega_2, \pmod{\gamma}$ närhelst $\omega_1 - \omega_2 = \gamma\alpha$, med $\alpha \in \Omega$. Denna typ av kongruens har samma formella egenskaper som kongruens i $\mathbb{Z}$. Om $a, b, c \in \mathbb{Z}, c \neq 0$, då är $a \equiv b \pmod{c}$ tvetydigt eftersom det betecknar kongruenser både i $\mathbb{Z}$ och i Ω. Men enligt Proposition 7.1 ser vi att om $a - b = c\alpha$ med $\alpha \in \Omega$, då är α både ett rationellt tal och ett algebraiskt heltal, så $\alpha \in \mathbb{Z}$. Följande proposition är en följd av binomialsatsen och faktumet att Ω är en ring.

Proposition 7.4 *Om $\omega_1, \omega_2 \in \Omega$ och $p \in \mathbb{Z}$ är ett primtal, så gäller*

$$(\omega_1 + \omega_2)^p = \omega_1^p + \omega_2^p \pmod{p}.$$

En *enhetsrot* är en lösning till en ekvation på formen $x^n - 1 = 0$. Därför är enhetsrötter algebraiska heltal. (Se även Proposition 7.9.) Detta faktum använder vi i nästa sektion, där vi ger en kortfattad introduktion till teorin om karaktärer. För en mera ingående beskrivning av denna teori, se till exempel [3], Kapitel 5.

7.1 Karaktärer och Gaussummor

Definition 7.2 *En multiplikativ karaktär χ på $\mathbb{F}_p$ är en avbildning*

$$\chi : \quad \mathbb{F}_p^* \mapsto \mathbb{C} \backslash \{0\}$$

som för alla $a, b \in \mathbb{F}_p^*$ uppfyller

$$\chi(ab) = \chi(a)\chi(b).$$

Legendresymbolen $(\frac{a}{p})$ är ett exempel på en sådan karaktär om den betraktas som en funktion från restklassen av a modulo p. Ett annat exempel är den triviala multiplikativa karaktären, definierad genom relationen $\epsilon := \epsilon(a) = 1$ för alla $a \in \mathbb{F}_p^*$. Det är vanligt att, liksom vi har gjort med Legendresymbolen, utvidga definitionsmängden till hela $\mathbb{F}_p$. Om $\chi \neq \epsilon$ är en karaktär definierar vi helt enkelt $\chi(0) := 0$ och $\epsilon(0) := 1$. Multiplikativa karaktärer kallas ofta bara karaktärer.

Definition 7.3 *Låt χ_1 och χ_2 vara karaktärer och $a \in \mathbb{F}_p^*$. Då definierar vi:*
(1) $(\chi_1\chi_2)(a) := \chi_1(a)\chi_2(a)$,
(2) χ^{-1} *är avbildningen* $a \mapsto \chi(a)^{-1}$.

Det är enkelt att verifiera, att med dessa definitioner är χ^{-1} och $\chi_1\chi_2$ karaktärer. Alla karaktärer av $\mathbb{F}_p^*$ bildar en cyklisk grupp av ordning $p-1$, vilket bevisas i [4], Kapitel 8. Om vi med $N(x^n = a)$ betecknar antalet lösningar till ekvationen $x^n = a$, med $a \in \mathbb{F}_p$, så har vi att om $n \mid p-1$:

$$N(x^n = a) = \sum_{\chi^n = \epsilon} \chi(a),$$

där summan löper över alla karaktärer med ordning som delar n. Bevis ges i [4], Kapitel 8. I vårt speciella fall med χ som Legendresymbolen, det vill säga när $n = 2$ och p är ett udda primtal, har vi alltså

$$N(x^2 = a) = 1 + \left(\frac{a}{p}\right),$$

vilket vi känner igen från Kapitel 1, Följdsats 2.3 (eller Proposition 2.6, med $k = 0$ och $r = 1$).

7.2 Beräkning av $G(\chi)^2$

Låt ζ beteckna en p:te primitiv enhetsrot, det vill säga $\zeta = e^{2\pi i/p}$, och låt χ beteckna Legendresymbolen.

Definition 7.4 $G_a = \sum_{t=0}^{p-1} \chi(t)\zeta^{at}$ *kallas den kvadratiska Gaussumman.*

Alla summeringar i fortsättningen kommer att utföras i intervallet från 0 till $p-1$. Det underlättar läsbarheten att inte skriva ut det varje gång.

När $a \equiv 0 \pmod{p}$ gäller att $G_0 = \sum_t \left(\frac{t}{p}\right) \zeta^{0t} = 0$. Detta inses lätt eftersom antalet kvadratiska rester modulo ett primtal är lika många som de icke-kvadratiska resterna.

För $a \not\equiv 0 \pmod{p}$ gäller att at går över en hel restklass modulo p närhelst t gör det. Symbolerna $\left(\frac{x}{p}\right)$ samt ζ^x beror bara på restklassen för $x \pmod{p}$. Låt oss nu verifiera att kvadraten på *den kvadratiska Gaussumman* $G(\chi)^2$ är oberoende av restklassen av a i definition 7.4. Vi bevisar först följande proposition.

Proposition 7.5 $G_a = \left(\frac{a}{p}\right) G_1$

Bevis Om $p \mid a$, så har vi att $\zeta^{at} = 1$ för alla t. Detta ger resultatet $G_0 = 0$. Antag nu att $p \nmid a$. Då har vi:

$$\left(\frac{a}{p}\right) G_a = \sum_t \left(\frac{at}{p}\right) \zeta^{at} = \sum_x \left(\frac{x}{p}\right) \zeta^x = G_1.$$

Multiplicera nu med $\left(\frac{a}{p}\right)$ på bägge sidorna av ekvationen $\left(\frac{a}{p}\right)G_a = G_1$ och resultatet följer eftersom $\left(\frac{a}{p}\right)^2 = 1$. □

Låt G beteckna G_1. Om $a \not\equiv 0 \pmod{p}$ så medför Proposition 7.5 att $G_a^2 = G^2$. Nu kan vi beräkna värdet på $G(\chi)^2$.

Proposition 7.6 $G^2 = (-1)^{(p-1)/2} p$.

Bevis Här beräknar vi summan $\sum_a G_a G_{-a}$ på två olika sätt. Om $a \not\equiv 0 \pmod{p}$, då är $G_a G_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right)G^2 = \left(\frac{-1}{p}\right)G^2$. Detta följer av att $G_a = \left(\frac{a}{p}\right)G$ och vi ser därför att:

$$\sum_a G_a G_{-a} = \left(\frac{-1}{p}\right)(p-1)G^2.$$

Vidare gäller att $G_a G_{-a} = \sum_x \left(\frac{x}{p}\right)\zeta^{xa} \sum_y \left(\frac{y}{p}\right)\zeta^{-ya} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{(x-y)a}$. När vi nu summerar båda sidor över a och utnyttjar $\sum_a \zeta^{(x-y)a} = 0$ när $x \neq y$ och $\sum_a \zeta^{(x-y)a} = p$ när $x = y$ så får vi:

$$\sum_a G_a G_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \sum_a \zeta^{(x-y)a} = \sum_{x=y=1}^{p-1} 1 \cdot p = (p-1)p.$$

När vi nu sätter ihop dessa bägge resultat får vi,

$$\left(\frac{-1}{p}\right)(p-1)G^2 = (p-1)p.$$

Förkortning av $p-1$ och multiplikation med $\left(\frac{-1}{p}\right)$ ger det eftersökta resultatet. $\square$

Gauss 6:e bevis av kvadratisk reciprocitet.

Låt $p^* = (-1)^{(p-1)/2}p$ och låt q vara ett annat udda primtal. Betrakta kongruenser modulo q i ringen av algebraiska heltal:

$$G^{q-1} = (G^2)^{(q-1)/2} = p^{*(q-1)/2} \equiv \left(\frac{p^*}{q}\right) \pmod{q}.$$

Genom att använda egenskaperna, enligt Proposition 7.4, hos de algebraiska heltalen modulo q, ser vi genast att,

$$G^q = \left(\sum \left(\frac{t}{p}\right)\zeta^t\right)^q \equiv \sum \left(\frac{t}{p}\right)^q \zeta^{qt} \equiv G_q \pmod{q}.$$

Nu är vi nästan framme, för det gäller alltså med hjälp av den tidigare observationen $G_a = (a/p)G$, att

$$\left(\frac{p^*}{q}\right) G \equiv G^q \equiv G_q \equiv \left(\frac{q}{p}\right) G \pmod{q}.$$

Multiplikation med G medför ekvivalensen

$$\left(\frac{p^*}{q}\right)p^* \equiv \left(\frac{q}{p}\right)p^* \pmod{q},$$

vilket i sin tur medför

$$\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q}$$

och slutligen

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Med hjälp av Lemma 5.1 och Eulers kriterium kan vi nu skriva om vänsterledet som

$$\left(\frac{(-1)^{(p-1)/2}p}{q}\right) = \left(\frac{(-1)^{(p-1)/2}}{q}\right)\left(\frac{p}{q}\right) = ((-1)^{(p-1)/2})^{(q-1)/2}\left(\frac{p}{q}\right).$$

Därför är

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

□

7.3 Ändliga kropssutvidgningar och kvadratisk reciprocitet.

Teorin om ändliga kroppar är från [5] och där kan man lämpligen studera dess bevis. Beviset av kvadratisk reciprocitet är hämtat från [4], sidan 85.

Varje ändlig kropp $\mathbb{F}$ består av p^f element, där p är ett primtal och f är ett naturligt tal. Följande proposition visar att det för varje primtalspotens p^f finns en och (upp till isomorfism) endast en ändlig kropp med p^f element.

Proposition 7.7 *Låt $\mathbb{F}$ vara en ändlig kropp. Då uppfyller varje element ekvationen $X^{p^f} - X = 0$ och elementen i $\mathbb{F}$ är precis rötterna till denna ekvation. Omvänt så är, för varje primtalspotens p^f, sönderfallskroppen över $\mathbb{F}_p$ av polynomet $X^{p^f} - X = 0$ en kropp med p^f element.*

Den unika kroppen med p^f element betecknas $\mathbb{F}_{p^f}$. Dess multiplikativa grupp är cyklisk. Ordningen av vilket som helst element i $\mathbb{F}_{p^f}$ delar $p^f - 1$. Nu har vi att en generator, säg g, i $\mathbb{F}^*_{p^f}$ har ordningen $p^f - 1$, så att ett godtyckligt element $a \in \mathbb{F}^*$ kan skrivas som $a = g^j$ för $0 \leq j < p^f - 1$.

Följande lemma behövs i beviset av reciprocitetslagen. *Karakteristiken* av kroppen $\mathbb{F}_{p^f}$ definieras som det minsta heltal p, sådant att $p \cdot 1 = 0$. En kropp med p^f element har karakteristiken p.

Lemma 7.8 *Låt $a, b \in \mathbb{F}_{p^f}$ och låt d vara ett naturligt tal. Då gäller*
(i) $a = a^{p^f}$,
(ii) $(a + b)^{p^d} = a^{p^d} + b^{p^d}$.

Enhetsrötter är lösningar till ekvationen $x^n = 1$ i ändliga kroppar. Hur många n-te enhetsrötter finns det i kroppen $\mathbb{F}_{p^f}$? Följande proposition (för bevis se [5], sidan 41) besvarar den frågan.

Proposition 7.9 *Låt g vara en generator till $\mathbb{F}^*_{p^f}$. Då är g^j en n-te enhetsrot om och endast om $nj \equiv 0 \pmod{p^f - 1}$. Antalet enhetsrötter är $(n, p^f - 1)$. Speciellt, så har $\mathbb{F}_{p^f}$ en primitiv $n-$te enhetsrot omm $n \mid p^f - 1$. Om ξ är en primitiv enhetsrot så är ξ^j också en primitiv n-te enhetsrot omm $(j, n) = 1$.*

En direkt följd av propositionen är:

Följdsats 7.10 *Om $(n, p^f - 1) = 1$, så är 1 den enda n-te enhetsroten i $\mathbb{F}_{p^f}$.*

Vi börjar med ett 'nytt' bevis av den första supplementära lagen med hjälp av teorin om ändliga kroppsutvidgningar.

Lemma 7.11 *Elementet $-1 \in \mathbb{F}_{p^f}$ har en kvadratrot i $\mathbb{F}_{p^f}$ omm $p^f \equiv 1 \pmod 4$.*

Bevis Det är klart att om -1 har en kvadratrot, dvs $-1 = a^2$ för något $a \in \mathbb{F}_{p^f}^*$, så gäller att det finns en 4-de enhetsrot (eftersom $1 = (-1)^2 = a^4$), det vill säga $4|p^f - 1$. Åt andra hållet gäller om $4|p^f - 1$, så innehåller $\mathbb{F}_{p^f}^*$ ett element av ordningen 4. Alltså har vi $x \in \mathbb{F}_{p^f}^*$ sådant att $x^4 = 1$. Då gäller $a = -1$ om $a = x^2$, (ty $a = \pm 1$, men $+1$ är uteslutet eftersom $o(x) = 4$). $\square$

Lemma 7.11 för $f = 1$ visar att $(\frac{-1}{p}) = (-1)^{(p-1)/2}$, det vill säga, den första supplementära lagen. Nu ger vi ett nytt bevis av andra supplementära lagen.

Bevis av andra supplementära lagen. Låt $f(n) = (-1)^{(n^2-1)/8}$ för udda n och $f(n) = 0$ för jämna n. Vi vill visa att $(\frac{2}{p}) = f(p)$. Eftersom $p^2 \equiv 1 \pmod 8$, innehåller kroppen $\mathbb{F}_{p^2}$ en primitiv 8:nde enhetsrot, enligt Proposition 7.9. Låt $\xi \in \mathbb{F}_{p^2}$ beteckna en primitiv 8-nde enhetsrot. Notera att $\xi^4 = -1$. Definiera Gausssumman $G = \sum_{j=0}^{7} f(j)\xi^j$, det vill säga $G = \xi - \xi^3 - \xi^5 + \xi^7 = 2(\xi - \xi^3) \to G^2 = 4(\xi^2 - 2\xi^4 + \xi^6) = 8$. Därför har vi i $\mathbb{F}_{p^2}$,

$$G^p = (G^2)^{(p-1)/2}G = 8^{(p-1)/2}G = \left(\frac{8}{p}\right)G = \left(\frac{2}{p}\right)G,$$

genom Eulers kriterium och Lemma 5.1 (iv). Å andra sidan, från definitionen av G, faktumet att $(a+b)^p = a^p + b^p$ i $\mathbb{F}_{p^2}$, samt den uppenbara observationen att $f(j)^p = f(j)$, har vi $G^p = \sum_{j=0}^{7} f(j)\xi^{pj}$. Notera nu att $f(j) = f(p)f(pj)$, vilket följer av att f är en fullt multiplikativ funktion, dvs $f(nm) = f(n)f(m)$ för alla heltal m, n. Om vi nu gör ett variabelbyte, $j' = pj$ så har vi

$$G^p = \sum_{j=0}^{7} f(p)f(pj)\xi^{pj} = f(p)\sum_{j=0}^{7} f(j')\xi^{j'} = f(p)G.$$

Propositionen följer genom att jämföra de två olika resultaten ovan. $\square$

Slutligen kan vi presentera ett kort och koncist bevis av reciprocitetslagen utifrån ett liknande resonemang.

Bevis av reciprocitetslagen utifrån teorin för ändliga kroppar. Låt p och q vara olika udda primtal. Eftersom $(p,q) = 1$, så finns det ett heltal n, sådant att $q^n \equiv 1 \pmod p$. Låt $\mathbb{F}$ vara en ändlig kropp med dimension n över $\mathbb{Z}/q\mathbb{Z}$. Då är $\mathbb{F}^*$ cyklisk av ordning $q^n - 1$. Låt γ vara en generator av $\mathbb{F}^*$ och sätt $\lambda = \gamma^{(q^n-1)/p}$. λ har ordningen p.

Definiera $\tau_a = \sum_{t=0}^{p-1}(\frac{t}{p})\lambda^{at}$, där $a \in \mathbb{Z}$. Beteckna $\tau_1 = \tau$. Vi har nu en analog situation som i beviset med hjälp av Gaussummor. Här är $\tau_q = (\frac{q}{p})\tau$ och $\tau^2 = (-1)^{(p-1)/2}\overline{p}$, där $\overline{p}$ är restklassen p modulo q.

Låt $p^* = (-1)^{(p-1)/2}p$. Då ser vi att $\tau^2 = \overline{p^*}$ vilket innebär att $\left(\frac{p^*}{q}\right) = 1$ omm $\tau \in \mathbb{Z}/q\mathbb{Z}$. Det är klart att $\tau \in \mathbb{Z}/q\mathbb{Z}$ om och endast om $\tau^q = \tau$, och eftersom

$$\tau^q = \left(\sum\left(\frac{t}{p}\right)\lambda^t\right)^q = \sum\left(\frac{t}{p}\right)^q\lambda^{qt} = \tau_q \ = (\frac{q}{p})\tau,$$

ger relationen $\tau^q = (\frac{q}{p})\tau$ att $\tau \in \mathbb{Z}/q\mathbb{Z}$ då och endast då $(\frac{q}{p}) = 1$. Det följer nu till slut:

$$\left(\frac{p^*}{q}\right) = 1 \ \Leftrightarrow \ \left(\frac{q}{p}\right) = 1.$$

$\square$

Beviset är klart och jag ger inga fler bevis, även om det hade varit kul att fortsätta med några fler, till exempel beviset på sidan 238 i [6] (Third proof), som visar ett snyggt samband mellan vårt bevis med hjälp av kvadratiska Gausssummor på sidan 39 och Eisensteins analytiska bevis i kapitel 6.4.

Det (troligtvis) senaste och 196:e beviset av Gaussiska reciprocitet publicerades av Franz Lemmermeyer år 2000. För en detaljerad lista över alla bevis av kvadratisk reciprocitet och en mycket omfattande referens-samling till böcker och artiklar med olika reciprocitetslagar, se slutet av [6] eller enklare på internet:

www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

Referenser

[1] Andrew Adler, John E. Coury, *The Theory of Numbers*, Jones and Bartlett Publishers. Boston, London, 1995.

[2] David A.Cox, *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, New York Chichester Brisbane Toronto Singapore, 1989.

[3] Helmut Hasse *Number Theory* Springer-verlag, New York, Heidelberg, Berlin, 1980.

[4] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*, Springer-verlag New York Heidelberg Berlin, 1982.

[5] Neal Koblitz, *A course in Number Theory and Cryptography*, Springer-verlag New York Heidelberg Berlin, 1987.

[6] Franz Lemmermeyer, *Reciprocity Laws From Euler to Eisenstein.* Springer-verlag, New York, Heidelberg, Berlin, 2000.

[7] I.N.Stewart and D.O.Tall, *Algebraic Number theory*, Chapman & Hall/CRC. Boca Raton, London, New York, Washington D.C., 1987.

[8] Harry N. Wright, *Theory of Numbers*, John Wiley & Sons, Inc. New York, London, 1939.