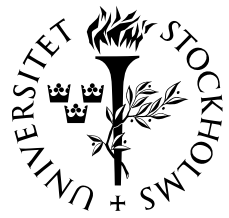



# SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET


## Kvadratisk reciprocitet och två bevis


av

**Love Huldt**



2019 - No K9

# Kvadratisk reciprocitet och två bevis

Love Huldt

---

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Torbjörn Tambour

2019

# Kvadratisk reciprocitet och två bevis

Love Huldt

Vårterminen 2019

**Sammanfattning**

Den här texten behandlar Gauss sats om kvadratisk reciprocitet och presenterar två bevis av satsen. Det första beviset bygger på kongruensekvationer och moduloräkning. Det andra beviset använder den komplexa exponentialfunktionen.

## Tack till

Jag vill tacka min handledare Torbjörn Tambour för hans stora tålamod och kunnande som jag blivit hjälpt av; utan honom denna text hade sett väldigt annorlunda ut. Jag vill också ge ett stort tack till min granskare Håkan Granath för hans väldigt kärnfulla kritik, samt till andra som korrekturläst vissa stycken av texten under skrivandeprocessen.

# Innehållsförteckning

# 1 Inledning

Denna uppsats handlar i huvudsak om den modulära aritmetikens kvadratiska reciprocitetssats, närmare bestämt dess formulering och två bevis, samt de satser på vilka den vilar. Innehållet är indelat i avsnitt med varsitt övergripande ämne; efter inledningen ligger ett avsnitt om för sammanhanget grundläggande talteori, följt av ett avsnitt om själva reciprocitetssatsen och sedan ett avsnitt med det första beviset. Efter det kommer en förberedelse för det andra beviset, som använder den komplexa exponentialfunktionen. Texten avslutas med det andra beviset av reciprocitetssatsen, några exempel på hur den används, samt några personliga reflektioner. Vissa delar av innehållet följs av exempel på hur beräkningar görs med hjälp av den nyss genomgångna teorin; dessa är tydligt märkta med rubriken exempel.

# 2 Talteoretisk grund

Detta avsnitt inleds med några grundläggande fenomen och förklaringar, för att sedan övergå till mer specifika satser och bevis. Hela uppsatsen vilar på moduloräkning, och använder därför enbart heltal för beräkningar.

## 2.1 Heltalsaritmetik

I allmänhet utförs alla beräkningar här inom ramarna för mängden $\mathbb{Z}_p$ som består av heltalen $0,\ 1,\ 2, \ldots,\ p-1$, som är alla rester vid division av något heltal med $p$, där $p$ är ett udda primtal. Varje element i $\mathbb{Z}_p$ kan betraktas som distinkta restklasser som då är på formen $a + qp$, där $q$ är något heltal och $a$ är ett heltal mindre än $p$. Alla tal större än $p$ kan reduceras till något av elementen i $\mathbb{Z}_p$, och alla positiva tal mindre än $p$ är redan element i mängden. Om två tal lämnar samma rest vid division med $p$ är de alltså identiska i $\mathbb{Z}_p$. Låt $A = a + qp$ och $B = b + rp$. Att $A \equiv B \mod p$ innebär alltså att $a \equiv b \mod p$, eftersom alla produkter där $p$ är en faktor är noll i $\mathbb{Z}_p$. Vidare är varje element i $\mathbb{Z}_p$ inverterbart utom 0, och just talet 0 kommer ofta vara oviktigt för sammanhanget och därför utelämnas, vilket vi kommer dra nytta av i senare resonemang och beräkningar.

## 2.2 Kvadratisk rest

Låt $p$ vara ett udda primtal som inte delar $a$. Då är $a$ en kvadratisk rest modulo $p$ om $x^2 \equiv a \mod p$ för något $x$. I fortsättningen behandlas bara kvadratiska rester mod $p$ om inget annat anges, och när ett tal sägs vara en rest eller en icke-rest menas generellt att talet är en kvadratisk rest eller en kvadratisk icke-rest.

## 2.3 Exempel på kvadratiska rester och kvadratiska icke-rester

**Exempel 1.** Vi undersöker vilka rester som finns modulo 19. Det vi behöver undersöka är alltså vilka av alla möjliga rester modulo 19 som är resultatet av att en kvadratisk term $x^2$ har reducerats mod 19, det vill säga alla $a$ sådana att $x^2 \equiv a \mod 19$. Alla intressanta rester mod 19 är 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18. De fullständiga beräkningarna utelämnas, men det är alltså var och en av dessa arton möjliga rester som kvadreras och sedan reduceras mod 19:

$$\begin{array}{llllllll} 1^2 & \equiv 1, & 2^2 & \equiv 4, & 3^2 & \equiv 9, \\ 4^2 & \equiv 16, & 5^2 & \equiv 6, & 6^2 & \equiv 17, \\ 7^2 & \equiv 11, & 8^2 & \equiv 7, & 9^2 & \equiv 5, \\ 10^2 & \equiv 5, & 11^2 & \equiv 7, & 12^2 & \equiv 11, \\ 13^2 & \equiv 17, & 14^2 & \equiv 6, & 15^2 & \equiv 16, \\ 16^2 & \equiv 9, & 17^2 & \equiv 4, & 18^2 & \equiv 1. \end{array}$$

De kvadratiska resterna mod 19 är alltså 1, 4, 5, 6, 7, 9, 11, 16, 17, och de kvadratiska icke-resterna är 2, 3, 8, 10, 12, 13, 14, 15, 18. Detta är för att ett godtyckligt kvadratiskt tal som är större än och inte delbart med 19, reduceras till något av dessa tal i kvadrat.

## 2.4 Antalet kvadratiska rester och icke-rester

Det här avsnittet handlar om antalet rester vi har i någon godtycklig primtalsmodul, vilket vi behöver veta senare för att bevisa flera satser. Vi definierar avbildningen $f : \mathbb{Z}_p \mapsto \mathbb{Z}_p$ genom $f(x) = x^2$. Bilden av $f$ är då mängden av alla kvadratiska rester modulo $p$, och här bortser vi från talet 0. Då gäller att om $a$ är en kvadratisk rest, finns det precis två olika element $x$ i $\mathbb{Z}_p$ sådana att $f(x) = a$. Om den ena av dessa är $b$, är den andra $-b$, och de är olika, för annars vore $2b \equiv 0 \mod p$, det vill säga att $b = 0$, eftersom $p$ är udda. Dessutom, undantaget 0 är varje element i $\mathbb{Z}_p$ inverterbart, eftersom varje element i $\mathbb{Z}_p$ och $p$ är relativt prima. Alltså kan $x^2 = a$ inte ha fler än två lösningar per kvadratisk rest $a$. Alltså är antalet element i bilden av $f$ hälften så många som elementen i $\mathbb{Z}_p$; de är alltså $\frac{1}{2}(p-1)$ stycken. Eftersom ett givet element i $\mathbb{Z}_p$ måste vara antingen en kvadratisk rest eller icke-rest är resterande $\frac{p-1}{2}$ stycken element icke-rester. Alltså är antalet rester och icke-rester lika stort.

## 2.5 Produkter av rester och icke-rester

Vi ska visa att produkten av två rester är en rest, att produkten av en icke-rest och en rest är en icke-rest, och att produkten av två icke-rester är en rest. Modulen är inte viktig att precisera utöver att den är ett udda primtal $p$, så den skrivs inte ut i beräkningarna nedan.

Vi börjar med produkten av två rester: Om $a$ och $b$ är två rester kan vi skriva att $a \equiv x^2$, $b \equiv y^2$. Då är produkten av $a$ och $b$: $ab \equiv x^2y^2$, som kan skrivas

$(xy)^2$. Eftersom $ab$ är kongruent med en kvadratisk term är $ab$ en kvadratisk rest.

Produkten av en rest och en icke-rest: Låt $a$ vara en rest, där $a \equiv x^2$ och låt $b$ vara en icke-rest. Antag då att $ab$ är en kvadratisk rest, så att $ab \equiv c^2 \bmod p$ för något något $c$ i $\mathbb{Z}_p$. Då har vi $c^2 \equiv ab \equiv x^2 b \bmod p$. Eftersom $p$ inte delar $a \equiv x^2 \bmod p$, är inte $p$ en delare till $x$. Alltså har $x$ en invers, som vi kallar $x^{-1}$, sådan att $x^{-1}x \equiv 1 \bmod p$. Nu multiplicerar vi $c^2$ med $(x^{-1})^2$, och vi får $(x^{-1})^2 c^2 \equiv (x^{-1})^2 ab \equiv (x^{-1}x)^2 b \equiv b \bmod p$. Då är $b \equiv (x^{-1}c)^2$ en kvadratisk rest, vilket är en motsägelse. Alltså är produkten av en rest och en icke-rest en icke-rest.

Produkten av två icke-rester: Eftersom antalet rester är samma som antalet icke-rester, kan vi skriva resterna som $R_1$, $R_2$, ..., $R_q$ och icke-resterna som $N_1$, $N_2$, ..., $N_q$, där $q = \frac{1}{2}(p-1)$. Produkten av en godtycklig icke-rest $N$ och varje $R_i$ är då $NR_1$, $NR_2$, ..., $NR_q$, som utgör $q$ stycken icke-rester. Då är produkten av en godtycklig icke-rest och varje icke-rest $NN_1$, $NN_2$, ..., $NN_q$, det vill säga $q$ stycken rester. Inga av dessa $NR_j$ och $NN_i$ är lika, eftersom antalet rester och icke-rester då vore mindre än $p-1$, vilket går emot en av de mest fundamentala egenskaperna hos moduloräkning som denna text vilar på. Eftersom antalet rester och antalet icke-rester är lika många, och tillsammans är de $p - 1 = 2q$ stycken, är dessa $NN_i$ därför en omordning av resterna i $\mathbb{Z}_p$, där varje element endast kan vara en rest eller en icke-rest.

Vi går genast igenom några exempel på beräkningar med kvadratiska rester och icke-rester.

## 2.6 Exempel

Vi tar 97 som modul i alla tre fallen.

**Exempel 2.** Två kvadratiska rester mod 97 är 66 och 70, eftersom $39^2$ samt $58^2 \equiv 66$ och $19^2$ samt $78^2 \equiv 70 \bmod 97$. Då tar vi produkten av dessa rester, och reducerar den mod 97: $66 \cdot 70 = 4620 \equiv 61$. Vi ska nu hitta kvadratrötter till 66 och 70 modulo 97, och visa att produkterna av dessa i sin tur är kvadratrötter till 61 modulo 97.

Vi ska alltså lösa kongruensekvationerna $x^2 \equiv 66$ samt $y^2 \equiv 70 \bmod 97$. Vi har ingen allmän metod för att bestämma kvadratrötter i fall som detta, så genom att vi prövade oss fram fann vi att $x_1 = 39$, $x_2 = 58$, $y_1 = 19$, och $y_2 = 78$, som alla är kvadratiska icke-rester mod 97. Nu går vi igenom de olika produkterna $x_i y_j$, där först ut är $x_1 y_1 = 741 \equiv 62$, som är en kvadratisk rest och en kvadratrot till 61 mod 97, eftersom $62 \cdot 62 \equiv 61 \bmod 97$. Den andra beräkningen gäller $x_1 y_2$, där $x_1 y_2 = 3042 \equiv 35 \bmod 97$, som också är en kvadratisk rest och en kvadratrot till 61 mod 97, eftersom $35 \cdot 35 \equiv 61 \bmod 97$. De andra produkterna $x_2 y_1$ samt $x_2 y_2$ är 35 respektive 62 mod 97, som vi redan visat är kvadratrötter till 61. Varje produkt $x_i y_j$ är alltså $\pm 35$, som vi också kan uttrycka som 35 och 62, för att hålla oss inom mängden $\mathbb{Z}_{97}$.

**Exempel 3** (Produkten av två icke-rester)**.** Nu ska vi undersöka kongruensekvationen $x^2 \equiv 65 \bmod 97$. Genom att återigen undersöka alla rester mod 97,

det vill säga talen 1, 2, ..., 96, fann vi att kvadraträtterna till 65 mod 97 är 29 och 68. När vi försöker hitta lösningar till kongruensekvationerna $x^2 \equiv 29$ och $y^2 \equiv 68 \mod 97$ visar det sig att de saknas, så 29 och 68 är kvadratiska icke-rester mod 97.

**Exempel 4** (Produkten av en rest och en icke-rest)**.** En kvadratisk rest mod 97 är 3, och en kvadratisk icke-rest är 38. Då är beräkningen $3 \cdot 38 = 114 \equiv 17$, som är en kvadratisk icke-rest. I det här fallet har vi dock ännu inget enkelt sätt att visa att 17 är en icke-rest, utan skulle behöva beräkna alla rester mod 97 och undersöka vilka tal i $\mathbb{Z}_{97}$ som inte dyker upp, vilket vi gjorde tidigare för en mindre modul.

Tidigare beräknade vi kvadraterna av alla tal i $\mathbb{Z}_{19}$ för att bestämma vilka tal som var kvadratiska rester och icke-rester. Senare avgör vi om ett givet tal är en kvadratisk rest mod $p$ med hjälp av exempelvis Eulers kriterium, vilket behandlas senare i texten.

## 2.7 Fermats lilla sats

Fermats lilla sats formulerades så tidigt som 1600-talets senare hälft, men fick vänta på sitt bevis i ett antal decennier, då Leibniz publicerade sitt bevis för satsen på 1700-talet. Beviset som används här formulerades först av James Ivory, och publicerades senare även av Dirichlet (Wikipedia, FLT). Fermats lilla sats visade sig vara väldigt viktig i framställandet av en metod för att skicka kodade meddelanden (Rosenthal, Rosenthal, & Rosenthal, 2014).

**Sats 1** (Fermats lilla sats)**.** *Låt $a$ vara ett heltal som inte är delbart med $p$, och $p$ är ett udda primtal. Då gäller att*

$$a^{p-1} \equiv 1 \mod p.$$

*Bevis.* Antag att $a$ inte är delbart med $p$. Vi har att de nollskilda elementen i $\mathbb{Z}_p$ är $\{1,\ 2,\ \ldots,\ p-1\}$ och att dessa tal är olika modulo $p$. Vi betraktar talen $1 \cdot a,\ 2 \cdot a,\ \ldots,\ (p-1) \cdot a$ och reducerar dem modulo $p$. De utgör en omordning av talen $1,\ 2,\ \ldots,\ p-1$, eftersom de alla är olika. För antag att två av dessa är lika, det vill säga att $i \cdot a \equiv j \cdot a \mod p$, vilket är ekvivalent med att $i \cdot a - j \cdot a \equiv 0 \mod p$. Då skulle gälla att $p \mid i \cdot a - j \cdot a = (i-j) \cdot a$, och enligt förutsättningen att $a$ och $p$ är relativt prima, innebär detta att $p \mid i - j$, vilket kräver att $i = j$, som är en motsägelse, eftersom de valdes för att vara olika. Vi multiplicerar talen i den nyss nämnda omordnade talmängden med varandra och får att produkten av dessa tal är kongruent med produkten $a \cdot 2a \cdots (p-1)a$. Detta skriver vi som $a \cdot 2a \cdots (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$. Vi samlar ihop faktorerna och får kongruensekvationen $a^{p-1}(p-1)! \equiv (p-1)! \mod p$. Eftersom $p$ är ett primtal är alla element i $\mathbb{Z}_p$ inverterbara utom 0, och $(p-1)!$ är en produkt vars alla faktorer är relativt prima med $p$, så $(p-1)!$ reduceras till något av elementen i $\mathbb{Z}_p$. Vi multiplicerar både höger- och vänsterled med inversen till $(p-1)!$, vilket ger att $a^{p-1} \equiv 1 \mod p$. □

## 2.8 Legendresymbolen

För att avgöra huruvida något tal $a$ är en kvadratisk rest modulo $p$ eller inte har vi tidigare helt enkelt beräknat de kvadratiska resterna eller hänvisat till att vi *vet* några rester och icke-rester. Nu introducerar vi en ny metod för att avgöra huruvida ett givet tal är en kvadratisk rest eller icke-rest.

**Definition 1.** Låt $p$ vara ett udda primtal och låt $a$ vara ett heltal som inte är delbart med $p$. Då definieras Legendresymbolen för $a$ modulo $p$ som

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

Följande sats kommer vara fundamental i fortsättningen:

**Sats 2** (Eulers kriterium)**.** *Låt $p$ vara ett udda primtal och $a$ vara ett heltal koprimt med $p$. Då gäller att*

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

Denna lämpar sig dock mest för beräkningar med något mindre primtal än vad som ofta kan vara intressant. I denna text utelämnas generellt fallet då $a = 0$, men Legendresymbolen brukar då sägas vara lika med noll, och särskilt är $a^{\frac{1}{2}(p-1)}$ noll då $a$ är noll, eftersom $p - 1 \neq 0$.

*Bevis.* Vi vet sedan tidigare att det finns lika många rester och icke-rester i $\mathbb{Z}_p$, eftersom vi bortser från nollan, samt att dessa tillsammans är $p - 1$ stycken. Eftersom $p$ är ett primtal ger Fermats lilla sats att

$$a^{p-1} \equiv 1 \mod p,$$

som kan skrivas som

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p.$$

Här är det viktigt att $p$ är udda, så att $\frac{1}{2}(p-1)$ är ett heltal.

Om $a$ är en kvadratisk rest mod $p$, det vill säga om $a \equiv x^2 \mod p$ är $a^{\frac{1}{2}(p-1)} \equiv (x^2)^{\frac{1}{2}(p-1)} \equiv x^{2\cdot\frac{1}{2}(p-1)} \equiv x^{p-1} \equiv 1 \bmod p$ enligt Fermats lilla sats, vilket gör att den första faktorn är noll, varför hela uttrycket är lika med noll. Vi anmärker nu att det bara finns $\frac{1}{2}(p-1)$ olika tal som gör den första faktorn till noll, och dessa tal är då alla kvadratiska rester till $a$. De andra $\frac{1}{2}(p-1)$ talen är då alla icke-rester till $a$ som gör den andra faktorn till noll, eftersom det finns $\frac{1}{2}(p-1)$ rester respektive icke-rester och ett givet element i $\mathbb{Z}_p$ kan inte vara både en rest och en icke-rest. Vidare har en kvadratisk kongruens två lösningar när modulen är ett primtal. Alltså är $a^{\frac{1}{2}(p-1)} \equiv -1 \bmod p$ i det fallet $a$ är en kvadratisk icke-rest. Detta visar Eulers kriterium. □

Räkneregler för Legendresymbolen är

$$a \equiv b \mod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \tag{1}$$

och

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \tag{2}$$

Räkneregel (1) ges av att om $a$ och $b$ är kongruenta med varandra mod $p$, måste den ena vara en kvadratisk rest mod $p$ om den andra är det. Det vill säga att om $a \equiv b$ mod $p$ innebär detta att $a = b + n \cdot p$, där $n$ är något heltal. Om $p$ delar $a$, delar $p$ även $a - n \cdot p$ och därmed delas även $b$ av $p$. Däremot, om $p$ inte delar $a$, och $a$ är en kvadratisk rest mod $p$, gäller att $x^2 \equiv a \equiv b$ mod $p$, varför också $b$ är en kvadratisk rest. Med samma sorts resonemang kan det visas att om $a$ inte är en kvadratisk rest mod $p$ kan inte heller $b$ vara det. Det centrala här är egentligen att vi i $\left(\frac{a}{p}\right)$ kan reducera $a$ mod $p$ så att $a < p$, och om $a \neq b$ men $a \equiv b$ är Legendresymbolernas värde för $a$ och $b$ samma.

Räkneregel (2) följer av räknereglerna för potenser som låter oss skriva produkten av två Legendresymboler som Legendresymbolen av produkten:

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

Denna omskrivning går att göra åt båda hållen, och låter oss därmed reducera ett större tal till dess primtalsfaktorer, vilket underlättar beräkning med Legendresymbolen. Jämför även med avsnitt 2.4 om produkter av rester och icke-rester, eftersom vi med Legendresymbolen väldigt enkelt kan beräkna sådana produkter.

## 2.9 Fallet $a = -1$

Något som ofta ges särskild uppmärksamhet är Legendresymbolen med $-1$ och $p$. Eulers kriterium $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)}$ med $a = -1$ ger direkt att $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$.

## 2.10 Exempel

Nu går vi igenom några exempel på beräkningar med hjälp av Legendresymbolen. Vi tar även upp de tre exemplen från avsnittet om produkter av rester och icke-rester.

**Exempel 5.** Nu undersöker vi om 5 är en kvadratisk rest mod 11 med hjälp av Legendresymbolen och Eulers kriterium, vilket avslöjar om $x^2 \equiv 5$ mod 11 har en lösning eller inte. Tack vare Legendresymbolen och Eulers kriterium är beräkningen mycket mer kortfattad än tidigare:

$$\left(\frac{5}{11}\right) \equiv 5^{\frac{10}{2}} = 5^5 = 5^2 \cdot 5^2 \cdot 5 \equiv 3 \cdot 3 \cdot 5 = 45 \equiv 1 \mod 11.$$

Alltså är 5 en kvadratisk rest mod 11.

**Exempel 6.** Vi tar ett exempel på hur räkneregel (1) kan användas. Låt $a = 237$, $b = 43$ och $p = 67$. Då har vi enligt räkneregel (1) att

$$237 \equiv 43 \mod 67 \implies \left(\frac{237}{67}\right) = \left(\frac{43}{67}\right) \mod 67,$$

vilket uppenbarligen stämmer. Med $p = 67$ är alla möjliga rester $x = \{1, 2, \ldots, 66\}$. Legendresymbolen vars värde vi behöver beräkna är alltså $\left(\frac{43}{67}\right)$ för både $a$ och $b$. Då ska vi nu bestämma vad $43^{33}$ mod 97 är kongruent med. Vi använder Eulers kriterium och vissa räkneregler för potenser för att avgöra detta. $43^{33} = (43^3)^{11} \equiv (-22)^{11} = (-22)^2(-22)^8(-22) \equiv 15(15)^4(-22) = 15^5(-22) \equiv 64(-22) \equiv (-3)(-22) = 66 \equiv -1 \mod 67$. Alltså är både $a$ och $b$ icke-rester mod 67.

**Exempel 7.** Nu går vi igenom hur räkneregel (2) ser ut med ett konkret exempel. Låt nu $a = 47$, $b = 7$ och $p = 113$. Då använder vi räkneregel (2) för att skriva

$$\left(\frac{47 \cdot 7}{113}\right) = \left(\frac{47}{113}\right)\left(\frac{7}{113}\right).$$

Detta kontrollerar vi med Eulers kriterium och räknereglerna för potenser:

$$\left(\frac{47}{113}\right)\left(\frac{7}{113}\right) \equiv 47^{\frac{113-1}{2}} 7^{\frac{113-1}{2}} \equiv (47 \cdot 7)^{\frac{113-1}{2}} \equiv \left(\frac{47 \cdot 7}{113}\right).$$

Med formeln för Eulers kriterium är beräkningen: $47^{56} = (47^2)^{28} \equiv 62^{28} = (62^2)^{14} \equiv 2^{14} = (2^7)^2 \equiv 15^2 = 225 \equiv -1 \mod 113$. På samma sätt beräknar vi den värdet av den andra faktorn: $7^{56} = 7^{54} \cdot 7^2 = (7^3)^{18} \cdot 7^2 \equiv 4^{18} \cdot 7^2 = (4^4)^4 \cdot 4^2 \cdot 7^2 \equiv 30^4 \cdot 4^2 \cdot 7^2 = (30^2)^2 \cdot 4^2 \cdot 7^2 \equiv (-4)^2 \cdot 4^2 \cdot 7^2 = 16 \cdot 4^2 \cdot 7^2 = 4^4 \cdot 7^2 \equiv 30 \cdot 7^2 = 3 \cdot 10 \cdot 49 = 3 \cdot (10 \cdot 49) \equiv 3 \cdot 38 = 114 \equiv 1 \mod 113$, och produkten av dessa modulo 113 är $-1 \cdot 1 = -1$. Resultatet är att produkten av en rest och en icke-rest är en icke-rest, som bevisats tidigare.

Nu använder vi helt enkelt Eulers kriterium för att undersöka talen från avsnittet om restprodukter. Vi börjar med produkten av två rester.

**Exempel 8.** Uttryckt med Legendresymbolen skrivs det första exemplet

$$\left(\frac{61}{97}\right) \equiv 61^{\frac{97-1}{2}}.$$

Enligt Eulers kriterium behöver vi alltså beräkna $61^{48}$ mod 97. Det kan göras enligt följande. $61^{48} = 61^{24} \cdot 61^{24}$, och vi undersöker bara en av dessa faktorer, eftersom de är identiska. Uppmärksamma hur likhetstecken och kongruenstecken används. $61^{24} = (61^2)^{12} \equiv (35)^{12} = (5 \cdot 7)^{12} = 5^{12} \cdot 7^{12} = (5^6)^2 \cdot (7^6)^2 \equiv 8^2 \cdot (-12)^2 = 64 \cdot 144 = 2^6 \cdot 3^2 \cdot 2^4 = 2^{10} \cdot 3^2 = (512) \cdot 2 \cdot 3^2 \equiv 27 \cdot 2 \cdot 3^2 = 3^4 \cdot 3 \cdot 2 = 81 \cdot 3 \cdot 2 \equiv (-16) \cdot 3 \cdot 2 = -96 \equiv 1 \mod 97$. Alltså är $61^{24} \equiv 1 \mod 97$, varför $61^{48} \equiv 1 \cdot 1 = 1 \mod 97$.

Vi fortsätter med produkten av en rest och en icke-rest.

**Exempel 9.** Nu undersöker vi $3 \cdot 38 = 114 \equiv 17 \bmod 97$ med Legendresymbolen och Eulers kriterium:

$$\left(\frac{17}{97}\right) \equiv 17^{48} \bmod 97.$$

På samma sätt som tidigare försöker vi göra $17^{48}$ mer hanterligt genom kongruensräkning. $17^{48} = (17^2)^{24} \equiv (-2)^{24} = 4^{12} = (4^6)^2 = 4096^2 \equiv 22^2 = 484 \equiv -1 \bmod 97$. Därmed är produkten av 3 och 38, det vill säga produkten av en rest och en icke-rest, en icke-rest.

Vi avslutar dessa exempel med att beräkna den produkt av två icke-rester som vi mötte tidigare.

**Exempel 10.** Vi inleder exemplet med att skriva Legendresymbolen och Eulers kriterium för 65 mod 97, för att sedan beräkna det med hjälp av en av räknereglerna för Legendresymbolen. Alltså skriver vi följande.

$$\left(\frac{65}{97}\right) = \left(\frac{5 \cdot 13}{97}\right) = \left(\frac{5}{97}\right)\left(\frac{13}{97}\right) \equiv 5^{48} \cdot 13^{48}$$

Vi börjar nu med att beräkna $5^{48} \bmod 97$. $5^{48} = (5^3)^{16} = 125^{16} \equiv 28^{16} = (28^2)^8 \equiv 8^8 \equiv (8^4)^2 = 4096^2 \equiv 22^2 = 484 \equiv -1$. Alltså är $5^{48} \equiv -1 \bmod 97$. Nu tar vi oss an $13^{48}$ på samma sätt. $13^{48} = (13^2)^{16} = 169^{16} \equiv 72^{24} = (72^2)^{12} = 5184^2 \equiv 43^12 = (43^2)^6 = 1849^6 \equiv 6^6 = (6^3)2 = 216^2 \equiv 22^2 \equiv -1 \bmod 97$. Nu ska vi alltså undersöka värdet av Legendresymbolen för $(-1)^2$ som uppenbarligen är 1. Alltså är produkten av de ursprungliga icke-resterna 84 och 92 en rest, vilket vi ville ge ett exempel på här.

# 3 Gauss lemma och minsta rest

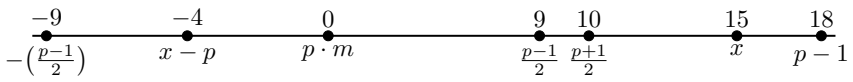
Tidigare i texten när vi avgjorde om vissa tal var kvadratiska rester eller icke-rester gjordes detta rest för rest, sedan introducerades Legendresymbolen för att förenkla det arbetet. Nu ska vi gå igenom Gauss lemma, som är ännu ett sätt att avgöra om ett tal är en kvadratisk rest eller inte. Precis som Legendresymbolen bygger lemmat på Eulers kriterium. Lemmat behövs längre fram för att bevisa den kvadratiska reciprocitetssatsen.

## 3.1 Minsta rest

För att formulera Gauss lemma behöver vi begreppen minsta positiv rest och absolut minsta rest modulo $p$, där $p$ är ett udda primtal. För ett godtyckligt heltal $n$ som inte delas av $p$ finns det enligt divisionsalgoritmen entydigt bestämda tal $q$ och $r$ sådana att $n = qp + r$ och $0 < r \leq p - 1$. Talet $r$ kallas den minsta positiva resten.

**Definition 2.** Vi definierar talet $x$ genom $x = r$ om $1 \leq r \leq \frac{p-1}{2}$ och $x = r - p$ om $\frac{p+1}{2} \leq r \leq p - 1$. Då gäller att $|x| < \frac{p}{2}$ och $n \equiv x \bmod p$. Talet $x$ är det tal med minst absolutbelopp som är kongruent med $n$ modulo $p$ och kallas den absolut minsta resten.

**Exempel 11.** Om exempelvis $p = 19$ och $x = 205$, vet vi att att $205 \equiv 15 \equiv -4$ mod 19. Då är den minsta positiva resten 15, medan den absolut minsta resten är $-4$, och produkten av något godtyckligt heltal $m$ och $p$ är kongruent med noll. Se nedanstående tallinje.




Det är viktigt att skilja mellan absolut minsta rest och minsta positiva rest. Absolut minsta rest kan vara negativ eller positiv, medan minsta positiva rest aldrig är negativ.

## 3.2 Gauss lemma

Nu har vi kommit till själva lemmat.

**Sats 3** (Gauss lemma)**.** *Låt $p$ vara ett udda primtal, $m$ ett heltal som inte är delbart med $p$, samt låt $\mu$ vara antalet element i mängden av talen $m$, $2m$, …, $\frac{1}{2}(p-1)m$ vars minsta positiva rester modulo $p$ är större än $\frac{1}{2}p$. Då gäller att*

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

*Bevis.* Vi ska betrakta de minsta positiva resterna $r$ modulo $p$ av talen $km$, där $k = 1, 2, \ldots, \frac{1}{2}(p-1)$. De rester som ligger i intervallet $1 \leq r \leq \frac{1}{2}(p-1)$ betecknar vi $u_1, u_2, \ldots, u_\lambda$ och de som ligger i intervallet $\frac{1}{2}(p-1) < r \leq p-1$ med $v_1, v_2, \ldots, v_\mu$. Vi har alltså att $\lambda + \mu = \frac{1}{2}(p-1)$ och $1 \leq p - v_i \leq \frac{1}{2}(p-1)$.

Alla tal $u_i$ och $p - v_i$ är olika. För antag att $u_i = u_j$. Vi vet att $a \neq b$ och att $am \equiv u_i$ samt $bm \equiv u_j$ för några $a$ och $b$. Då gäller att eftersom $u_i = u_j$ är $am \equiv bm \bmod p$, vilket ger att $a = b$ eftersom $m$ och $p$ är relativt prima, vilket är en motsägelse. På liknande sätt kan vi se att alla $p - v_i$ är olika. Antag att $u_i = p - v_j$. Vi skriver om detta till $u_i + v_j = p$ samt låter $am \equiv u_i$ och $bm \equiv v_j$. Vi får då att $am + bm \equiv p \equiv 0 \bmod p$, som eftersom $m$ och $p$ är relativt prima kan reduceras mod $p$ till $a + b \equiv 0 \bmod p$. Men eftersom $1 \leq a,\ b \leq \frac{1}{2}(p-1)$ gäller att $2 \leq a + b \leq 2 \cdot \frac{1}{2}(p-1) = p - 1$, vilket visar att $p$ inte delar summan $a + b$, eftersom $p > a + b$.

Talen $u_i$ $p - v_i$ är alltså omordningar av talen 1, 2, …, $\frac{1}{2}(p-1)$. Vi tar produkten av dem, så att vi får

$$\left(\frac{p-1}{2}\right)! = u_1 \cdot u_2 \cdots u_\lambda \cdot (p - v_1) \cdots (p - v_\mu),$$

som vi reducerar mod $p$ och sen faktoriserar vi ut $-1$ från alla $\mu$ stycken $v_i$, och

gör följande omskrivningar:

$$\begin{aligned}\left(\tfrac{p-1}{2}\right)! &\equiv u_1 \cdots u_\lambda \cdot (-v_1) \cdots (-v_\mu) \mod p \\ &\equiv (-1)^\mu u_1 \cdots u_\lambda \cdot v_1 \cdots v_\mu \\ &\equiv (-1)^\mu (1 \cdot m)(2 \cdot m) \cdots \left(\tfrac{p-1}{2} \cdot m\right) \mod p \\ &\equiv (-1)^\mu \left(\tfrac{p-1}{2}\right)! \, m^{\frac{1}{2}(p-1)} \mod p.\end{aligned}$$

Nu multiplicerar vi båda led med inversen till $\frac{1}{2}(p-1)!$, och har då att

$$1 \equiv (-1)^\mu \, m^{\frac{1}{2}(p-1)} \mod p.$$

Nu påpekar vi att $(-1)^\mu$ är sin egen invers, eftersom $\frac{1}{(-1)^\mu} = (-1)^\mu$, så nu vet vi också att

$$1 \equiv (-1)^\mu m^{\frac{1}{2}(p-1)} \iff (-1)^\mu \equiv m^{\frac{1}{2}(p-1)} \mod p.$$

Slutligen har vi då att eftersom $\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}}$ gäller enligt Eulers kriterium också att $\left(\frac{m}{p}\right) = (-1)^\mu$, vilket skulle visas. □

Gauss lemma har stor teoretisk betydelse i många bevis av den kvadratiska reciprocitetssatsen, av vilka två tas upp senare i texten. Lemmat är generellt inte behjälpligt rent beräkningsmässigt, men vi tar ändå ett exempel på hur beräkningar med hjälp av Gauss lemma kan se ut.

**Exempel 12.** Låt $m = 11$ och $p = 13$. Då är talen $m$, $2m$, …, $\frac{1}{2}(p-1)m$ lika med 11, 22, 33, 44, 55, 66, som reduceras till 11, 9, 7, 5, 3, 1 modulo 13. Av dessa är endast 7, 9 och 11 större än $\frac{1}{2}p = \frac{13}{2}$, alltså är $\mu = 3$. Då säger Gauss lemma att $\left(\frac{11}{13}\right) \equiv (-1)^3 = -1$, det vill säga att 11 är en kvadratisk icke-rest modulo 13, vilket Eulers kriterium också ger oss: $11^{\frac{13-1}{2}} = 11^6 = 11^2 \cdot 11^2 \cdot 11^2$, och eftersom $11^2 = 121 \equiv 4 \mod 13$, gäller att $11^{\frac{13-1}{2}} = 11^6 = 11^2 \cdot 11^2 \cdot 11^2 \equiv 4 \cdot 4 \cdot 4$, där $4^2 = 16 \equiv 3 \mod 13$, så $4^2 \cdot 4 \equiv 3 \cdot 4 = 12 \equiv -1 \mod 13$.

# 4 Ett specialfall av Gauss lemma

Nu är det dags att behandla $\left(\frac{2}{p}\right)$ samt hur $\lambda$ och $\mu$ ser ut då $m = 2$. Här introducerar vi beteckningen $[x]$ för heltalsdelen av $x$; det största heltalet mindre än eller lika med $x$.

## 4.1 Talen $\lambda$ och $\mu$ då $m = 2$

Vi börjar med att påminna om att $\lambda + \mu = \frac{1}{2}(p-1)$. Då $m = 2$ i Gauss lemma gäller att $\lambda$ är antalet jämna positiva heltal som är mindre än eller lika stora som $\frac{p}{2}$. Om vi betecknar dessa tal med $2k$, där $k = 1, 2, \ldots, \frac{1}{2}(p-1)$, så får vi $2k \leq \frac{p}{2}$, alltså är $k \leq \frac{p}{4}$. Eftersom $k$ är heltal, är det största värdet $k = [\frac{p}{4}]$ och antalet olika $k$ är $[\frac{p}{4}]$.

Nu ska vi visa att $\mu = \left[\frac{1}{4}(p+1)\right]$ genom att visa att $\mu = \frac{1}{2}(p-1) - [\frac{1}{4}p]$. I fallet då $p = 4n+1$ gäller att $\mu = \frac{4n+1-1}{2} - \frac{4n+1-1}{4} = 2n - n = n$, som är $\left[\frac{1}{4}(p+1)\right]$. Då $p = 4n+3$ gäller att $\mu = \frac{1}{2}(4n+3-1) - \frac{1}{4}(4n+3-3)$ $= \frac{1}{2}(4n+2) - \frac{1}{4}(4n) = 2n+1-n = n+1$, som är $\left[\frac{1}{p}(p+1)\right]$ då $p = 4n+3$. Alltså gäller att $\mu = \left[\frac{1}{4}(p+1)\right]$ och $\lambda = \left[\frac{1}{4}p\right]$. Vi går nu igenom två exempel på beräkningar av $\lambda$ och $\mu$ med olika former av $p$.

**Exempel 13** ($p = 4n+1$)**.** Vi väljer $p = 29$, där vi behöver betrakta talen 2, 4, 6, ..., 28. Då $\lambda$ är antalet rester som är mindre än eller lika stora som $\frac{1}{2}(p-1)$, det vill säga alla positiva jämna heltal mindre eller lika med 14, och $\mu$ är antalet jämna heltal från och med 15 till och med 28, eftersom vi för $\mu$ tittar på antalet rester från och med $\frac{1}{2}(p+1)$ till och med $p-1$. Det finns sju av vardera sort, eftersom antalet jämna tal från 1 till 14 är $\frac{14}{2} = 7$ och det är lika många jämna tal mellan 15 och 28.

**Exempel 14** ($p = 4n+3$)**.** Nu tar vi $p = 31$. Talen att betrakta är då 2, 4, ..., 30. $\frac{1}{2}(p-1) = 15$, och $\frac{1}{2}(p+1) = 16$, och det finns inget heltal mellan dessa två. Antalet jämna heltal större än 1 men mindre eller lika med 15 är 7, alltså är $\lambda = \left[\frac{1}{4}p\right]$. Antalet jämna heltal mellan $\frac{1}{2}(p-1)$ och $p-1$ är 8, eftersom att $\mu = \frac{1}{2}(p-1) - \lambda$ innebär att $\mu = \frac{30}{2} - 7$, som förenklas så att vi ser att $\mu = 15 - 7 = 8$. Alltså kan vi uttrycka det som att $\mu = \frac{1}{2}(p-1) - \frac{1}{4}(p-3) = \frac{1}{4}(p+1) = \left[\frac{1}{4}(p+1)\right]$.

I den här texten bestämmer vi bara explicita uttryck för $\mu$ och $\lambda$ då $m = 2$. Det finns några fler fall utöver de som här nämns, men de ligger utanför vidden av denna text och de tas således inte upp. Det är dock intressant att ta upp en formulering av exponenten i Gauss lemma då $m = 2$ som inte behöver delas upp i olika fall, vilket kan åstadkommas enligt följande resonemang.

Vi säger att två heltal har samma paritet om de är kongruenta mod 2, det vill säga om båda är jämna eller båda är udda. Lägg märke till att om $a$ är udda, så har $ab$ samma paritet som $b$. Om $p = 4n+1$, är $\frac{1}{2}(p+1)$ udda och $\mu \cdot \frac{1}{2}(p+1) = \frac{1}{8}(p^2-1)$ har således samma paritet som $\mu$. Om $p = 4n+3$, så är $\frac{1}{2}(p-1)$ udda och $\mu \cdot \frac{1}{2}(p-1) = \frac{1}{8}(p^2-1)$ har således samma paritet som $\mu$. I båda fallen har vi tydligen att $\mu \equiv \frac{1}{8}(p^2-1) \bmod 2$, varför $\left(\frac{2}{p}\right) \equiv (-1)^{\mu} \equiv (-1)^{\frac{1}{8}(p^2-1)}$.

För ett bevis senare i texten är det viktigt att här poängtera att $\frac{1}{8}(p^2-1)$ är delbar med 8, eftersom de olika $p$ vi arbetar med här är antingen på formen $p = 4n+1$ eller $p = 4n+3$, så vi har att

$$p = 4n+1 \implies \frac{p^2-1}{8} = \frac{16n^2+8n}{8} = 4n^2+n, \text{ och}$$

$$p = 4n+3 \implies \frac{p^2-1}{8} = \frac{16n^2+24n+8}{8} = 2n^2+3n+1.$$

Då $m = 2$ gäller att $\mu = \frac{1}{2}(p-1) - \left[\frac{1}{4}(p+1)\right] = \left[\frac{1}{4}(p+1)\right]$. Alltså har vi att $\left(\frac{2}{p}\right) \equiv 2^{\frac{1}{2}(p-1)} \equiv (-1)^{\left[\frac{1}{4}(p+1)\right]} \bmod p$, det vill säga $\left(\frac{2}{p}\right) \equiv 1$ om $p = 8n \pm 1$, $\left(\frac{2}{p}\right) \equiv -1$ om $p = 8n \pm 3$. Om $p = 8n \pm 1$ är $\frac{1}{8}(p^2-1)$ jämnt, och då $p = 8n \pm 3$

är $\frac{1}{8}(p^2-1)$ udda. Därför gäller att $(-1)^{\left[\frac{1}{4}(p+1)\right]} \equiv (-1)^{\frac{1}{8}(p^2-1)} \bmod p$. Nu har vi visat två viktiga samband, som vi sammanfattar som en sats.

**Sats 4.**

$$\left(\frac{2}{p}\right) \equiv (-1)^{\left[\frac{p+1}{4}\right]} \equiv (-1)^{\frac{p^2-1}{8}} \mod p.$$

# 5 Den kvadratiska reciprocitetssatsen

Den kvadratiska reciprocitetssatsen formulerades först av Euler och bevisades senare av Gauss; den var en milstolpe inom talteorin, och Gauss själv var helt begeistrad av sambandet. Han formulerade av egen kraft åtta olika bevis av satsen, vilken han dessutom kallade för det gyllene teoremet (Wikipedia, QR).

Satsen om kvadratisk reciprocitet låter oss avgöra huruvida kvadratiska kongruensekvationer av typen $x^2 \equiv a \mod p$ är lösbara eller ej, men avslöjar ingenting om själva lösningen utöver dess existens. Vi går genast till formuleringen av satsen.

**Sats 5** (Den kvadratiska reciprocitetssatsen)**.** *Låt $p$ och $q$ vara olika udda primtal. Då är*

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

*där $p' = \frac{1}{2}(p-1)$ och $q' = \frac{1}{2}(q-1)$, det vill säga*

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

Det finns två viktiga omformuleringar av satsen som vi också ska nämna, när primtalen $p$ och $q$ är av särskild typ. Det viktiga här är att då både $p$ och $q$ är på formen $4n_i + 3$ är produkten $p'q'$ udda, och annars är den jämn. Det visas på följande sätt.

Då $p = 4n_1+1$ och $q = 4n_2+3$ är $p' = \frac{1}{2}(4n_1+1-1)$ och $q' = \frac{1}{2}(4n_2+3-1)$, där $n_i$ är olika godtyckliga positiva heltal. Därför är $p'q' = \frac{1}{4}(16n_1n_2 + 8n_1) = 4n_1n_2 + 2n_1$, alltså ett jämnt heltal. Nu undersöker vi produkten $p'q'$ när både $p$ och $q$ är på formen $4n_i + 1$. Då är $p'q' = \frac{1}{4}(4n_1 + 1 - 1)(4n_2 + 1 - 1) = \frac{1}{4}(4n_1)(4n_2) = \frac{1}{4}(16n_1n_2) = 4n_1n_2$. Detta ger oss sambandet

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right), \tag{3}$$

Om både $p$ och $q$ är på formen $4n_i+3$, gäller att $p'q' = \frac{1}{4}(4n_1+3-1)(4n_2+3-1) = \frac{1}{4}(16n_1n_2 + 8n_1 + 8n_2 + 4) = 4n_1n_2 + 2n_1 + 2n_2 + 1$. Alltså är då $p'q'$ udda, vilket ger oss

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

Här visar (3) att när som mest ett av primtalen $p$ och $q$ är kongruenta med 3 mod 4 är $p$ en kvadratisk rest till $q$ om och endast om $q$ är en kvadratisk rest

till $p$, och (4) ger att när både $p$ och $q$ är kongruenta med 3 mod 4 är $p$ en kvadratisk rest till $q$ om och endast om $q$ är en kvadratisk icke-rest till $p$.

Nu följer två bevis av reciprocitetssatsen.

# 6 Det första beviset

Det här är ett bevis av reciprocitetssatsen hämtat från Nagell (1951), som vilar på flitigt summerande på olika sätt. Vi drar slutsatser baserade på pariteten hos summorna, vilket framgår i bevisföringen. I början använder vi ett heltal $m$ som inte delas av primtalet $p$, och längre fram i beviset övergår vi från $m$ till ett annat udda primtal $q$.

*Bevis.* Låt $m$ vara något heltal som inte är delbart med $p$. Vi betecknar då resterna av $m$, $2m$, $\ldots$, $\frac{1}{2}(p-1)m$ mod $p$ med $u_i$ och $v_i$, precis som i beviset av Gauss lemma. Alltså gäller att $0 < u_i \leq p'$ och $0 < p - v_i \leq p'$, där $p' < v_i \leq p-1$ och antalet termer $p - v_i$ är $\mu$ stycken. Tidigare visades att $u_i$ och $p - v_i$ är två omordningar av talen 1, 2, $\ldots$, $p'$, så att vi kan skriva

$$\sum u_i + \sum (p - v_i) = \sum_{k=1}^{p'} k = \frac{1}{2}p'(p'+1) = \frac{1}{8}(p^2-1),$$

enligt formeln för aritmetisk summa. Som tidigare, i samband med beviset av Gauss lemma, definierar vi här $\mu$ som antalet minsta positiva rester av $m$, $2m$, $\ldots$, $\frac{1}{2}(p-1)m$ som är större än $p'$, vilket medför att

$$\mu p + \sum u_i - \sum v_i = \frac{1}{8}(p^2-1). \tag{5}$$

Eftersom $c - d \equiv c + d \bmod 2$, det vill säga att för två heltal $c$ och $d$ gäller att pariteten hos summan $c + d$ är samma som för skillnaden $c - d$, så undersöker vi istället summan

$$\sum u_i + \sum v_i$$

som är summan av alla resterna då talen $km$ divideras med $p$, där $m$ och $k$ är några heltal som inte är delbara med $p$. Vi har

$$km = p\left[\frac{km}{p}\right] + r_k,$$

så summan av alla resterna är

$$\sum_{k=1}^{p'} r_k = \sum_{k=1}^{p'} \left( km - p\left[\frac{km}{p}\right]\right),$$

som förenklas till

$$m\sum_{k=1}^{p'} k - p\sum_{k=1}^{p'}\left[\frac{km}{p}\right] = \frac{1}{8}m(p^2-1) - pS(m,p),$$

där

$$S(m,p) = \sum_{k=1}^{p'} \left[ \frac{km}{p} \right].$$

Alltså är $\sum r_k$, summan av alla rester, lika med

$$\sum u_i + \sum v_i = \frac{1}{8} m(p^2-1) - pS(m,p). \tag{6}$$

Då vi subtraherar (6) från (5) ledvis, får vi

$$\mu p - 2\sum v_i = \frac{1}{8}(p^2-1) - \frac{1}{8}m(p^2-1) + pS(m,p),$$

vilket vi för att samla summorna i ena ledet skriver som

$$pS(m,p) - \mu p + 2\sum v_i = \frac{1}{8}(m-1)(p^2-1). \tag{7}$$

Vi antar nu att $m$ är udda, så att $m-1$ är jämnt. Eftersom $p^2-1$ är delbart med 8, är högerledet i (7) jämnt och vi ser att $pS(m,p) - \mu p$ är jämnt. Då $p$ är udda måste $S(m,p) - \mu$ vara jämnt, det vill säga $S(m,p) - \mu \equiv 0 \bmod 2$, av vilket följer att

$$\mu \equiv S(m,p) \mod 2.$$

Gauss lemma ger nu

$$\left(\frac{m}{p}\right) = (-1)^{S(m,p)}$$

och om vi ersätter $m$ med ett udda primtal $q \neq p$, så får vi

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)}.$$

För att visa reciprocitetssatsen behöver vi nu visa att $S(p,q) + S(q,p) \equiv p'q' \bmod 2$.

Betrakta talen $qx - py$, där $x$ och $y$ är heltal och $1 \leq x \leq p'$, $1 \leq y \leq q'$. Antalet sådana tal är ju $p'q'$. De är alla skilda från 0, för antag att $qx = py$. Eftersom $p$ och $q$ är olika primtal, måste $p$ dela $x$, det vill säga att $x = tp$ för något heltal $t$. Men eftersom $1 \leq x \leq p'$, är den enda möjligheten $t = 0$, och vi får $x = 0$, vilket är en motsägelse. Alltså är inga av dessa tal lika med 0.

Vi ska räkna antalet positiva respektive antalet negativa tal $qx - py$. Observera att $qx - py < 0$ om och endast om $y < \frac{qx}{p}$. Antalet $y$ sådana att $qx - py > 0$ för ett fixt $x$ är alltså $\left[\frac{qx}{p}\right]$. Antalet positiva tal $qx - py$ får vi genom att summera detta då $x$ går från 1 till $p'$, vilket är

$$\sum_{x=1}^{p'} \left[ \frac{qx}{p} \right] = S(q,p).$$

På samma sätt ser vi att antalet negativa tal $qx - py$ är lika med $S(p,q)$ och det följer nu att det totala antalet tal $qx - py$ är $S(p,q) + S(q,p)$ eftersom $qx - py \neq 0$ för alla $x$ och $y$. Således är $S(p,q) + S(q,p) = p'q'$, och framförallt är pariteten samma, i både högerled och vänsterled. Därmed är satsen bevisad. □

# 7 Den komplexa exponentialfunktionen

I nästa avsnitt följer ett bevis först författat av Gotthold Eisensten (Ireland & Rosen, 2010). Beviset använder den komplexa exponentialfunktionen, egenskaper hos enhetsrötter samt upprepade produkter, vilket påminner om hur vi använde summor i det första beviset av reciprocitetssatsen. I det här avsnittet presenteras några fundamentala förhållanden och likheter vi behöver för att genomföra beviset.

## 7.1 Den komplexa exponentialfunktionen och dess rötter

Vi börjar med några definitioner.

**Definition 3.** När $t$ är reellt, definierar vi den komplexa exponentialfunktionen som

$$e^{it} = \cos t + i \sin t.$$

En lösning $z_k$ till ekvationen $z^n = 1$ kallas ofta för en $n$:te enhetsrot. Vi kan beräkna enhetsrötter genom att skriva $z_k = e^{\frac{2\pi ki}{n}}$ där $k$ är ett heltal och sedan lösa ekvationen $e^{2\pi ki} = 1$, så att rötterna är

$$z_k = e^{\frac{2\pi ki}{n}}, \quad k \in \mathbb{Z}.$$

För dessa enhetsrötter gäller att

$$z_{k+n} = e^{\frac{2\pi i(k+n)}{n}} = e^{\frac{2\pi ki}{n} + \frac{2\pi in}{n}} = e^{\frac{2\pi ki}{n}} \cdot e^{2\pi i} = e^{\frac{2\pi ki}{n}} = z_k.$$

Alltså räcker det att ta $k = 0, 1, 2, ..., n-1$. Dessutom är talen $z_k$ olika. För om $z_k = z_m$, skulle

$$e^{\frac{2\pi ki}{n}} = e^{\frac{2\pi mi}{n}} \text{ och alltså } \ e^{\frac{2\pi i(m-k)}{n}} = 1.$$

Då måste $m-k$ delas av $n$, vilket ger $k = m$. Alltså utgör $z_k = e^{\frac{2\pi ki}{n}}$, då $k = 0, 1, ..., n-1$, samtliga $n$:te enhetsrötter. Vidare gäller enligt räknereglerna för potenser att

$$z_k = e^{\frac{2\pi ki}{n}} = (e^{\frac{2\pi i}{n}})^k = (z_1)^k.$$

## 7.2 Polynom, produkter och två lemman

Om $p(z) = z^n + a_1 z^{n-1} + \cdots + a_n$ är ett polynom med nollställen $z_1, \ldots, z_n$, gäller enligt faktorsatsen att

$$p(z) = (z - z_1)(z - z_2) \cdots (z - z_n).$$

Talen $z_k = e^{\frac{2\pi ki}{n}}$ är som bekant nollställena till $p(z) = z^n - 1$, varför

$$z^n - 1 = (z - z_0)(z - z_1) \cdots (z - z_{n-1}) = \prod_{k=0}^{n-1} (z - z_k) = \prod_{k=0}^{n-1} (z - e^{\frac{2\pi ki}{n}}).$$

Detta kommer leda till ett viktigt resultat. Vi börjar med att sätta $z = \frac{x}{y}$:

$$\Big(\frac{x}{y}\Big)^n - 1 = \Big(\frac{x}{y} - z_0\Big)\Big(\frac{x}{y} - z_1\Big)\cdots\Big(\frac{x}{y} - z_{n-1}\Big).$$

Nu multiplicerar vi denna senaste ekvation med $y^n$, så att vi i vänsterledet får

$$y^n\Big(\Big(\frac{x}{y}\Big)^n - 1\Big) = y^n \cdot \frac{x^n}{y^n} - y^n = x^n - y^n,$$

och i högerledet får vi

$$\begin{aligned} & y^n\Big(\tfrac{x}{y} - z_0\Big)\Big(\tfrac{x}{y} - z_1\Big)\cdots\Big(\tfrac{x}{y} - z_{n-1}\Big) \\ = \;& y\Big(\tfrac{x}{y} - z_0\Big)\cdot y\Big(\tfrac{x}{y} - z_1\Big)\cdots y\Big(\tfrac{x}{y} - z_{n-1}\Big) \\ = \;& (x - z_0y)(x - z_1y)\cdots(x - z_{n-1}y), \end{aligned}$$

som alltså är faktorformen av polynomet $x^n - y^n$. Detta sammanfattar vi som ett lemma.

**Lemma 1.**

$$\begin{aligned} x^n - y^n &= (x - z_0y)(x - z_1y)\cdots(x - z_{n-1}y) \\ &= \prod_{k=0}^{n-1}(x - z_ky) \\ &= \prod_{k=0}^{n-1}(x - e^{\frac{2\pi ki}{n}}y). \end{aligned}$$

Vi tar direkt upp ett besläktat lemma.

**Lemma 2.** *När $n$ är udda, kan vi skriva*

$$x^n - y^n = \prod_{k=0}^{n-1}(x - e^{\frac{2\pi i(-2k)}{n}}y),$$

eftersom då $k = 0, 1, \ldots, n-1$, gäller att värdemängderna till $e^{\frac{2\pi ki}{n}}$ och $e^{\frac{2\pi i(-2k)}{n}}$ är två olika omordningar av $n$:te enhetsrötter. Vi har tidigare visat att $e^{\frac{2k\pi i}{n}}$ genomlöper alla $n$:te enhetsrötter då $k = 0, 1, \ldots, n-1$. Det återstår att visa att detta gäller även för $e^{\frac{2\pi i(-2k)}{n}}$, vilket görs genom på följande sätt.

*Bevis av lemma* 2. Om $e^{\frac{2\pi i(-2k)}{n}} = e^{\frac{2\pi i(-2m)}{n}}$, så är $e^{\frac{2\pi i(2m-2k)}{n}} = 1$, och då måste $n$ dela $2m - 2k$. Eftersom $n$ är udda, måste i så fall $n$ dela $m - k$. Då $0 \leq m,\ k \leq n-1$, måste $m$ vara lika med $k$. Talen $e^{\frac{2\pi i(-2k)}{n}}$ är alltså olika och eftersom de är $n$ stycken, utgör även de alla $n$:te enhetsrötter. □

Om vi faktoriserar ut $e^{\frac{-2\pi ki}{n}}$ ur $x$-termen och faktoriserar samma uttryck ur $y$:s koefficient i argumentet till produkten i lemma 1, ser vi att

$$x - e^{\frac{2\pi i(-2k)}{n}}y = e^{\frac{-2\pi ki}{n}}\big(e^{\frac{2\pi ki}{n}}x - e^{\frac{-2\pi ki}{n}}y\big).$$

Nu kan vi göra en omskrivning av produkten i lemmat, efter att vi gjort faktoriseringen som nyss förklarats. Då gäller att

$$\begin{aligned} x^n - y^n &= \prod_{k=0}^{n-1} e^{\frac{-2\pi ki}{n}} \left(e^{\frac{2\pi ki}{n}} x - e^{\frac{-2\pi ki}{n}} y\right) \\ &= \prod_{k=0}^{n-1} e^{\frac{-2\pi ki}{n}} \prod_{k=0}^{n-1} \left(e^{\frac{2\pi ki}{n}} x - e^{\frac{-2\pi ki}{n}} y\right). \end{aligned}$$

Den första produkten i den andra raden här kan snabbt beräknas:

$$\prod_{k=0}^{n-1} e^{\frac{-2\pi ki}{n}} = e^0 \cdot e^{\frac{-2\pi i}{n}} \cdots e^{\frac{-2\pi i(n-1)}{n}} = e^{\frac{-2\pi i(0+1+\cdots+(n-1))}{n}}.$$

Här har vi att $0 + 1 + 2 + \cdots + (n-1) = \frac{1}{2} \cdot \frac{1}{n}(n(n-1)) = \frac{1}{2}(n-1)$, så att vi ser att då $n$ är udda, är $n-1$ jämnt och $\frac{1}{2}(n-1)$ är ett heltal. Detta ger

$$\prod_{k=0}^{n-1} e^{\frac{-2\pi ki}{n}} = e^{\frac{-2\pi i \cdot \frac{n(n-1)}{2}}{n}} = e^{-2\pi i \cdot \frac{n-1}{2}} = 1,$$

eftersom $-2\pi i \cdot \frac{n-1}{2}$ är $-2\pi i$ multiplicerat med ett heltal, det vill säga att $e^{-2\pi i \cdot a} = \cos(-2\pi a) + i \sin(-2\pi a)$, som är lika med 1 då $a$ är ett heltal.

Alltså gäller

$$x^n - y^n = \prod_{k=0}^{n-1} \left(e^{\frac{2\pi ki}{n}} x - e^{\frac{-2\pi ki}{n}} y\right) \tag{8}$$

för udda $n$.

# 8 Det andra beviset

Nu börjar vi ta oss an det andra beviset av den kvadratiska reciprocitetssatsen. Precis som det första beviset är huvudnumret i bevisföringen att bestämma talet $\mu$ i Gauss lemma, som vi formulerar en gång till, med mer anpassad notation. Vi använder också upprepade produkter på liknande sätt som vi använde summor i det första beviset. Det här beviset är anpassat från Ireland och Rosen (2010).

*Eisensteins bevis.* Vi börjar med att definiera en funktion $f$ genom

**Definition 4.**

$$f(z) = e^{2\pi iz} - e^{-2\pi iz}, \text{ då } z \in \mathbb{C}.$$

Då är $f$ periodisk med perioden 1, det vill säga att $f(z+1) = f(z)$, eftersom

$$e^{2\pi i(z+1)} = e^{2\pi iz + 2\pi i} = e^{2\pi iz} \cdot e^{2\pi i} = e^{2\pi iz} \cdot 1 = e^{2\pi iz},$$

och motsvarande gäller för $e^{-2\pi iz}$.

I ekvation (8) sätter vi nu $x = e^{2\pi iz}$ och $y = e^{-2\pi iz}$, där $z$ är komplext. Vänsterledet blir då

$$e^{2\pi inz} - e^{-2\pi inz} = f(nz).$$

Vi har vidare att

$$\begin{aligned}\left(e^{\frac{2\pi ki}{n}}x - e^{\frac{-2\pi ki}{n}}y\right) &= e^{\frac{2\pi ki}{n}}\cdot e^{2\pi iz} - e^{\frac{-2\pi ki}{n}}\cdot e^{-2\pi iz}\\ &= e^{2\pi i(z+\frac{k}{n})} - e^{-2\pi i(z+\frac{k}{n})}\\ &= f(z+\tfrac{k}{n}),\end{aligned}$$

så högerledet i (8) blir

$$f(nz) = \prod_{k=0}^{n-1} f\Big(z+\frac{k}{n}\Big) = f(z)\prod_{k=1}^{n-1} f\Big(z+\frac{k}{n}\Big).$$

Där vi har faktoriserat ut $f(0) = f(z)$ till utanför produkten och ändrat index från att börja med 0 till att börja med 1, vilket vi kan göra eftersom $f(0) = f\big(z-\frac{0}{n}\big) = f(z)$. Alltså är

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{n-1} f\Big(z+\frac{k}{n}\Big). \tag{9}$$

Vi antog att $n$ udda, så att $n-1$ är jämnt. Produkten i högerledet i (9) kan då delas upp i två delar:

$$\prod_{k=1}^{n-1} f\Big(z+\frac{k}{n}\Big) = \prod_{k=1}^{\frac{n-1}{2}} f\Big(z+\frac{k}{n}\Big)\cdot\prod_{k=\frac{n+1}{2}}^{n-1} f\Big(z+\frac{k}{n}\Big)$$

eftersom $\frac{n+1}{2} = \frac{n-1}{2}+1$. Vi fortsätter med att skriva om produkten ovan. Nu skriver vi

$$f\Big(z+\frac{k}{n}\Big) = f\Big(z+\Big(\frac{k}{n}-1\Big)\Big) = f\Big(z-\frac{n-k}{n}\Big).$$

Vi sätter nu $j = n-k$. När $k = \frac{n+1}{2}, \ldots, n-1$, så är $j = \frac{n-1}{2}, \ldots, 1$, varför $f\big(z+\frac{k}{n}\big) = f\big(z-\frac{j}{n}\big)$ och

$$\prod_{k=\frac{n+1}{2}}^{n-1} f\Big(z+\frac{k}{n}\Big) = \prod_{j=1}^{\frac{n-1}{2}} f\Big(z-\frac{j}{n}\Big).$$

Det spelar ju ingen roll vilken symbol vi har som index, så vi kan byta $j$ mot $k$ i högerledet och får då

$$\prod_{k=\frac{n+1}{2}}^{n-1} f\Big(z+\frac{k}{n}\Big) = \prod_{k=1}^{\frac{n-1}{2}} f\Big(z-\frac{k}{n}\Big).$$

Sammanfattningsvis har vi nu detta samband:

$$\begin{aligned}\frac{f(nz)}{f(z)} &= \prod_{k=1}^{\frac{n-1}{2}} f\Big(z+\frac{k}{n}\Big)\cdot\prod_{k=\frac{n+1}{2}}^{n-1} f\Big(z+\frac{k}{n}\Big)\\ &= \prod_{k=1}^{\frac{n-1}{2}} f\Big(z+\frac{k}{n}\Big)\cdot\prod_{k=1}^{\frac{n-1}{2}} f\Big(z-\frac{k}{n}\Big)\\ &= \prod_{k=1}^{\frac{n-1}{2}} f\Big(z+\frac{k}{n}\Big)\cdot f\Big(z-\frac{k}{n}\Big). \qquad (10)\end{aligned}$$

Nu tar vi upp en lite annorlunda formulering av Gauss lemma jämfört med den vi använde för det första beviset.

Låt $p$ vara ett udda primtal. Gauss lemma säger att om $p$ och $m$ är relativt prima, så är

$$\Big(\frac{m}{p}\Big) = (-1)^{\mu},$$

där $\mu$ är antalet tal $lm$, där $1 \le l \le \frac{p-1}{2}$, som har negativ absolut minsta rest vid division med $p$. Låt den absolut minsta resten av $lm$ vara $\pm r_l$, där $r_l > 0$ och det således är minustecken för $\mu$ stycken $l$. Detta innebär att $lm = s_l p \pm r_l$ eller $\frac{lm}{p} = s_l \pm \frac{r_l}{p}$, där $s_l$ är heltal. Då är alltså $s_l$ kvoten och $r_l$ är resten, vid division av $lm$ med $p$. Vi påminner om att eftersom $f$ är periodisk med periodlängden 1, gäller att ett godtyckligt antal hela tal i $f$:s argument inte förändrar någonting i bilden av $f$, varför vi kan göra omskrivningen

$$f\Big(\frac{lm}{p}\Big) = f\Big(s_l \pm \frac{r_l}{p}\Big) = f\Big(\frac{\pm r_l}{p}\Big) = \pm f\Big(\frac{r_l}{p}\Big).$$

Eftersom talen $r_l$, där $1 \le l \le \frac{p-1}{2}$, är en omordning av 1, 2, ..., $\frac{p-1}{2}$ och antalet minustecken är $\mu$, så får vi

$$\prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{lm}{p}\Big) = (-1)^{\mu}\prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{r_l}{p}\Big) = \Big(\frac{m}{p}\Big)\prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{l}{p}\Big), \qquad (11)$$

där vi ser att $\prod f\big(\frac{l}{p}\big)$ i högerledet inte beror på $m$.

Nu använder vi några samband vi visat tidigare. I ekvation (10) sätter vi $z = \frac{l}{p}$ och $n = q$, där $q$ är ett annat udda primtal. Då får vi

$$f\Big(\frac{ql}{p}\Big) = f\Big(\frac{l}{p}\Big)\prod_{k=1}^{\frac{q-1}{2}} f\Big(\frac{l}{p}+\frac{k}{q}\Big)\cdot f\Big(\frac{l}{p}-\frac{k}{q}\Big).$$

Tar vi produkten över $l$ av dessa likheter, får vi

$$\prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{lq}{p}\Big) = \prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{l}{p}\Big)\cdot\prod_{l=1}^{\frac{p-1}{2}}\prod_{k=1}^{\frac{q-1}{2}} f\Big(\frac{l}{p}+\frac{k}{q}\Big)f\Big(\frac{l}{p}-\frac{k}{q}\Big).$$

Nu använder vi likheten i (11), så att vi får

$$\Big(\frac{q}{p}\Big)\prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{l}{p}\Big) = \prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{l}{p}\Big)\cdot\prod_{l=1}^{\frac{p-1}{2}}\prod_{k=1}^{\frac{q-1}{2}} f\Big(\frac{l}{p}+\frac{k}{q}\Big)f\Big(\frac{l}{p}-\frac{k}{q}\Big).$$

Vi vet att $e^{it}\neq 0$, så vi kan dividera med $\prod_{l=1}^{\frac{p-1}{2}} f\big(\frac{l}{p}\big)$, vilket ger

$$\Big(\frac{q}{p}\Big) = \prod_{l=1}^{\frac{p-1}{2}}\prod_{k=1}^{\frac{q-1}{2}} f\Big(\frac{l}{p}+\frac{k}{q}\Big)f\Big(\frac{l}{p}-\frac{k}{q}\Big). \tag{12}$$

Byter vi $p$ och $q$ mot varandra, får vi

$$\Big(\frac{p}{q}\Big) = \prod_{l=1}^{\frac{q-1}{2}}\prod_{k=1}^{\frac{p-1}{2}} f\Big(\frac{l}{q}+\frac{k}{p}\Big)f\Big(\frac{l}{q}-\frac{k}{p}\Big),$$

och om vi också skiftar index får vi

$$\Big(\frac{p}{q}\Big) = \prod_{k=1}^{\frac{q-1}{2}}\prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{k}{q}+\frac{l}{p}\Big)f\Big(\frac{k}{q}-\frac{l}{p}\Big). \tag{13}$$

Det enda som skiljer likheterna (12) och (13) åt, är att det står $f\big(\frac{l}{p}-\frac{k}{q}\big)$ i (12) och $f\big(\frac{k}{q}-\frac{l}{p}\big)$ i (13). Då

$$f\Big(\frac{k}{q}-\frac{l}{p}\Big) = -f\Big(\frac{l}{p}-\frac{k}{q}\Big),$$

så är högerledet i (13) lika med

$$\begin{aligned}&\prod_{k=1}^{\frac{q-1}{2}}\prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{k}{q}+\frac{l}{p}\Big)\Big(-f\Big(\frac{l}{p}-\frac{k}{q}\Big)\Big)\\ =\;& (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\prod_{k=1}^{\frac{q-1}{2}}\prod_{l=1}^{\frac{p-1}{2}} f\Big(\frac{l}{q}+\frac{k}{p}\Big)f\Big(\frac{l}{q}-\frac{k}{p}\Big)\end{aligned}$$

eftersom antalet faktorer är $\frac{p-1}{2}\cdot\frac{q-1}{2}$. Alltså är

$$\Big(\frac{p}{q}\Big) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\Big(\frac{q}{p}\Big)$$

och beviset är klart. □

## 8.1 Exempel

Nu återbesöker vi ett av de exempel vi gick igenom tidigare samt går igenom ett nytt exempel med tresiffriga primtal, och visar hur reciprocitetssatsen förenklar arbetet med att undersöka kvadratiska rester.

**Exempel 15.** Låt $p = 61$, $q = 97$. Då är

$$\Big(\frac{61}{97}\Big)\Big(\frac{97}{61}\Big) = (-1)^{\frac{61-1}{2}\cdot\frac{97-1}{2}},$$

som vi skriver om till

$$\Big(\frac{61}{97}\Big) = (-1)^{30\cdot 48}\Big(\frac{36}{61}\Big).$$

Här har vi reducerat 97 mod 61 till 36, samt multiplicerat med $\big(\frac{36}{61}\big)$. Nu använder vi räkneregel (2) för att skriva om

$$\Big(\frac{36}{61}\Big) = \Big(\frac{6}{61}\Big)\Big(\frac{6}{61}\Big) = \Big(\frac{6}{61}\Big)^2,$$

så att vi ser att $97 \equiv 36$ är en kvadratisk rest mod 61, vilket enligt reciprocitetssatsen ger att 61 är en kvadratisk rest mod 97.

**Exempel 16.** Låt $p = 197$, samt $q = 157$. Nu ska vi undersöka huruvida 157 är en kvadratisk rest modulo 197 med hjälp av reciprocitetssatsen och Legendresymbolen. Då $p$ och $q$ är udda primtal kan vi enligt den kvadratiska reciprocitetssatsen skriva

$$\Big(\frac{157}{197}\Big) = (-1)^{\frac{157-1}{2}\cdot\frac{197-1}{2}}\Big(\frac{197}{157}\Big).$$

Eftersom $\frac{1}{2}(157-1) = 78$, det vill säga att exponenten till $(-1)$ är jämn, så får vi att

$$\Big(\frac{157}{197}\Big) = \Big(\frac{197}{157}\Big),$$

men $197 \equiv 40 = 2^3 \cdot 5 \bmod 157$, så använder vi räknereglerna för Legendresymbolen för att skriva om $\big(\frac{197}{157}\big)$ enligt

$$\Big(\frac{197}{157}\Big) = \Big(\frac{40}{157}\Big) = \Big(\frac{2}{157}\Big)^3\Big(\frac{5}{157}\Big) = \Big(\frac{2}{157}\Big)\Big(\frac{5}{157}\Big),$$

där vi också använt att $(\pm 1)^3 = \pm 1$. Vi har

$$\Big(\frac{2}{157}\Big) = (-1)^{\frac{157^2-1}{8}},$$

men $\frac{1}{8}(157^2-1) = \frac{1}{8}(156\cdot 158) = 39\cdot 79$, vilket är udda, så

$$\Big(\frac{2}{157}\Big) = -1.$$

Till sist är

$$\Big(\frac{5}{157}\Big) = (-1)^{\frac{5-1}{2}\cdot\frac{157-1}{2}}\Big(\frac{157}{5}\Big) = \Big(\frac{2}{5}\Big) = -1,$$

eftersom 2 inte är en kvadratisk rest mod 5, varför

$$\Big(\frac{157}{197}\Big) = \Big(\frac{2}{157}\Big)\Big(\frac{5}{157}\Big) = (-1)\cdot(-1) = 1.$$

Alltså är svaret ja; 157 är en kvadratisk rest mod 197.

Nu har vi gått igenom Gauss kvadratiska reciprocitetssats, vilket var målet med denna text. □

# 9 Personliga reflektioner

Det finns så många olika sätt att bevisa reciprocitetssatsen, att det snäva urval som här har visats inte är i närheten av att vara representativt för alla olika metoder som har använts genom historien. Det är också intressant att reciprocitetssatsen kan bevisas med hjälp av den komplexa exponentialfunktionen såväl som med Dedekindsummor, och även geometriskt genom att räkna gitterpunkter i en särskild rektangel. Det vore intressant att utforska kopplingen mellan dessa, eftersom de kommer från så till synes skilda områden, men ändå alla möts vid reciprocitetssatsen.

# 10 Referenslista


Ireland, K. och Rosen, M.. *A Classical Introduction to Modern Number Theory* (andra upplagan, med rättningar). (2010). New York: Springer-Verlag New York, Inc..

Nagell, T., *Introduction to Number Theory*. (1951). Stockholm: Almqvist & Wiksell.

Rosenthal, D., Rosenthal, D., och Rosenthal, P.. *A Readable Introduction to Real Mathemathics*. (2014). Cham: Springer International Publishing.

Wikipedia, *Fermat's little theorem*. https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_little_theorem Hämtad 2018-11-19.

Wikipedia, *Quadratic reciprocity*. https://en.wikipedia.org/wiki/Quadratic_reciprocity Hämtad 2019-01-15.