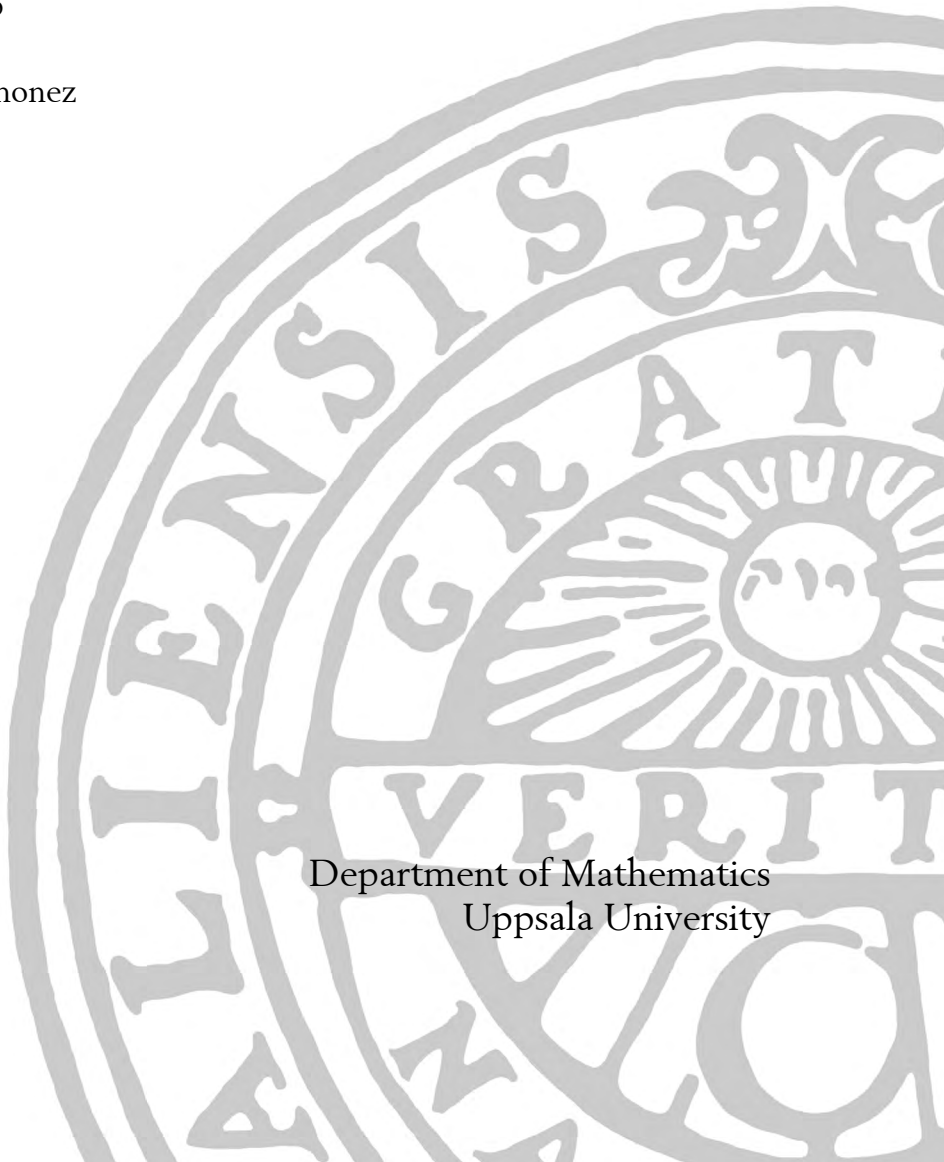
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2019:27

Kvadratiska rester

Elisa Pitkälä

Examensarbete i matematik, 15 hp
Handledare: Gunnar Berg
Examinator: Veronica Crispin Quinonez
Juni 2019



Department of Mathematics
Uppsala University

Abstract

This is an introduction to quadratic residues which are about whether the congruence $x^2 \equiv a \pmod{p}$ is solvable. In addition to being a Degree Project, is this an independent introduction to quadratic residues and therefore is a background about divisibility of numbers and congruence being given. Divisibility is the fundamental concept concerning congruence, and in that part for instance the division algorithm is mentioned. Regarding to congruence, calculation rules, residue classes and theorems like Euler's theorem and Fermat's little theorem are introduced. Then we define quadratic residues and quadratic nonresidues and examples of them modulo the first four primes are given. The reason, for why a congruence equation has exactly two solutions if it is solvable, will be given, and also why the number of quadratic residues is equal to the number of quadratic nonresidues modulo any odd prime. Legendre's symbol is then being defined, which is used to determine, whether or not a given number a is a quadratic residue modulo a prime p. That leads to Euler's criterion and subsequent theorems which, together with the multiplication rules for quadratic residues and nonresidues and Gauss lemma are useful in applications of The Law of Quadratic Reciprocity, that this essay culminates in. It gives the relation between when p is a quadratic residue modulo q and q is a quadratic residue modulo p for primes p and q.

Innehåll

Inledning **1**

1 Bakgrund **2**

1.1 Delbarhet 2

1.2 Kongruens 6

1.2.1 Räkneregler vid kongruensräkning 8

1.2.2 Restklasser 9

2 Kvadratiska rester **14**

2.1 Tabeller med kvadrater modulo 5, 7, 11 och 13 16

2.2 Antal kvadratiska rester och kvadratiska ickerester 18

2.3 Legendresymbolen 19

2.4 Multiplikationsregler 23

2.5 Gauss lemma 25

2.6 Kvadratisk reciprocitet 28

Avslutning **33**

Referenser **34**

Inledning

Låt p vara ett primtal, och a ett heltal som inte delar p. a kallas för en kvadratisk rest modulo p om ekvationen $x^2 \equiv a \pmod{p}$ är lösbar. Om ekvationen saknar lösning, kallas a för en kvadratisk ickerest. Föregående definition är grunden för detta arbete. Här kommer du att få svar på frågor som

- för vilka primtal p kongruensen $x^2 \equiv 2 \pmod{p}$ har lösningar, och
- hur man kan avgöra om ett heltal är en kvadrat modulo ett primtal.

Förutom att vara ett examensarbete, avses innehållet i detta arbete att vara en självständig introduktion till kvadratiska rester, och därför ges först en bakgrund bestående av bevis för mycket grundläggande påståenden om tals delbarhet samt kongruens. Därefter introduceras Legendresymbolen, vars betydelse tillsammans med notationen kvadratisk rest leder till flera viktiga satser inom talteorin, däribland den kvadratiska reciprocitetssatsen som detta arbete kulminerar i. Reciprocitetssatsen bevisades av Gauss år 1796, och sedan dess har över hundra bevis getts för satsen. Här presenteras ett bevis som bygger på kongruensekvationer och moduloräkning. Satsen går ut på att om vi vet att p är en kvadratisk rest respektive kvadratisk ickerest modulo q, vet vi också om q är en kvadratisk rest eller ickerest modulo p.

1 Bakgrund

För att kunna studera kvadratiska rester, krävs kunskap om tals delbarhet och kongruens. Eftersom detta, utöver att vara ett examensarbete, avses att vara en självständig introduktion till kvadratiska rester, ges i bakgrunden inledningsvis bevis för mycket grundläggande påståenden. Läsare, som har kunskaper motsvarande ett års matematikstudier på universitetsnivå om delbarhet och kongruens, kan börja läsa direkt från avsnitt 1.2.1.

1.1 Delbarhet

Definition 1.1. Om det, givet två heltal a och b, finns ett heltal x sådant att $a = bx$, sägs det att heltalet a är delbart med heltalet b (eller att b är en delare i a) vilket skrivs $b \mid a$. På motsvarande sätt betecknar $b \nmid a$ att b inte delar a, det vill säga b kan inte skrivas som en produkt av a med något annat heltal.

Om $b \nmid a$ går inte divisionen $\frac{a}{b}$ jämnt upp utan ger en rest, och det visar sig att det alltid, för heltal a och $b > 0$, går att skriva $a = bq + r$ där $0 \leqslant r < b$. q kallas för kvot, och r för (huvud)rest vid division av a med b. Detta följer ur divisionsalgoritmen, som går ut på att från a subtraheras så många multipler av b som möjligt utan att resultatet blir negativt. Antalet multipler av b som subtraherats är då kvoten q, och r det minsta talet som blir kvar.
Innan divisionsalgoritmen bevisas, införs beteckningen $[x]$, som kallas för heltalsdelen av x. $[x]$ står för det största heltal, som är $\leqslant x$. Exempelvis är $[3,7] = 3$, $[\frac{7}{4}] = 1$ och $[-4,9] = -5$. För heltalsdelen gäller allmänt att $x - 1 < [x] \leqslant x$.

Sats 1.1 (Divisionsalgoritmen)**.** Om a och b är hela tal med $b > 0$, finns det entydigt bestämda heltal q och r sådana att $a = bq + r$ och $0 \leqslant r < b$.

Bevis. Först bevisas existensen av kvoten q och resten r, och därefter bevisas att de är entydiga. Låt $q = \left[\frac{a}{b}\right]$, och $r = a - b\left[\frac{a}{b}\right]$. Då är $a = bq + r$. Med heltalsdelen av x, $[x]$, kan det skrivas som $\left(\frac{a}{b}\right) - 1 < \left[\frac{a}{b}\right] \leqslant \frac{a}{b}$. Om alla led multipliceras med b, fås $a - b < b\left[\frac{a}{b}\right] \leqslant a$, och om de därefter multipliceras med -1, fås $-a \leqslant -b\left[\frac{a}{b}\right] < b - a$. Om alla led slutligen adderas med a, fås $0 \leqslant a - b\left[\frac{a}{b}\right] = a - bq < b$, det vill säga $0 \leqslant r < b$. Detta bevisar existensen av en kvot q och en rest r sådana att $a = bq + r$ och $0 \leqslant r < b$. Kvarstår att bevisa att de är entydiga. Antag därför att vi också har q' och r' sådana att $a = bq' + r'$ och $0 \leqslant r' < b$. Genom subtraktion fås $r - r' = a - bq - (a - bq') = b(q' - q)$ och $-b < r - r' < b$. Det ger oss olikheten $-b < b(q' - q) < b$, och division med b (där $b > 0$ enligt antagandet) ger $-1 < q' - q < 1$. Eftersom q' och q båda är heltal måste också deras differens vara ett helt tal, och kan därför inte vara annat än 0 eftersom det ska vara ett heltal större än -1 men mindre än 1. Alltså fås $q' - q = 0$, det vill säga $q' = q$ vilket medför att $r = b - aq = b - aq' = r'$.[1] □

I följande sats visas några egenskaper gällande tals delbarhet:

Sats 1.2. Låt a, b och c vara heltal.

(a) Om $a \mid b$ och $a \mid c$, då gäller att $a \mid (b + c)$.

(b) Om $a \mid b$ och $b \mid c$, då gäller att $a \mid c$.

(c) Om $a \mid b$, då gäller att $a \mid bc$ för alla heltal c.

Bevis. (a). Om $a \mid b$ och $a \mid c$, då gäller att $b = ad$ och $c = ae$. $b + c = ad + ae = a(d + e)$. Talet $f = d + e$ är också ett heltal eftersom d och e är heltal, och därför kan vi skriva $b + c = af$ vilket innebär att $a \mid (b + c)$.
(b). $a \mid b \Leftrightarrow b = ad$ och $b \mid c \Leftrightarrow c = be$. Då blir $c = be = ade = a(de)$,

[1] Lars-Åke Lindahl, *Elementär talteori*, Uppsala, 2012, s. 2.

d.v.s. talet $g = de$ är ett heltal eftersom de är ett heltal, då blir $c = ag$ vilket betyder att $a \mid c$.
(c). Att $a \mid b$ innebär att det finns ett heltal d sådant att $b = ad$. Då är $bc = adc = a(dc)$. Låt $e = dc$. Då är $bc = ae$ vilket innebär att $a \mid bc$. □

Ett heltal a som är delare i två andra heltal b och c (d.v.s. $a \mid b$ och $a \mid c$) kallas för en gemensam delare till b och c. Eftersom varje heltal x ($\neq 0$) är delbar med $\pm x$ och ± 1, är talen 1 och -1 gemensamma delare till alla tal, och det finns därför minst en gemensam delare och således en största gemensam delare till b och c.

Definition 1.2. Den *största gemensamma delaren* till två tal a och b, varav minst en är nollskild, kallas $\text{sgd}(a, b)$. Om talet 1 är den enda gemensamma delaren, sägs talen vara *relativt prima*, vilket skrivs $\text{sgd}(a, b) = 1$.[2]

Definitionen av största gemensamma delare gäller även fler än två tal: för n heltal $a_1, a_2, \ldots, a_n$ är största gemensamma delaren det största heltal som delar alla n givna talen, förutsatt att de alla inte är lika med noll. Talen $a_1, a_2, \ldots, a_n$ kallas *relativt prima* om $\text{sgd}(a_1, a_2, \ldots, a_n) = 1$, och *parvis relativt prima* om varje par av talen är relativt prima.

Sats 1.3. Till varje par av heltal a och b finns heltal m och n sådana att

$$ma + nb = \text{sgd}(a, b).$$

Bevis. Tag två heltal a och b och bilda $M = \{ma + nb \mid m, n \in \mathbb{Z}\}$ samt låt α vara det minsta positiva talet i M. Då vet vi att $\alpha = ma + nb$ för heltal m och n, och $N\alpha \in M$ för alla heltal N. Antag att $\beta \in M$ och använd divisionsalgoritmen på α och β: $\beta = k\alpha + r$, $0 \leqslant r < \alpha$. Då gäller att $r \in M$ men eftersom α är det minsta positiva heltal i M och $r < \alpha$ måste vi ha

[2]Lindahl, s. 1.

$r = 0$ så $\beta = k \cdot \alpha$. Då kan följande slutsats dras: alla tal i M har formen $k \cdot \alpha$ där $k \in \mathbb{Z}$. Eftersom $\alpha = ma + nb$, gäller att om $\gamma \mid a$ och $\gamma \mid b$, så måste $\gamma \mid \alpha$ enligt sats 1.2. Vidare är $a = n\alpha$ och $b = m\alpha$ för m, n i $\mathbb{Z}$ så α är en gemensam delare till a och b. Men varje gemensam delare till a och b delar α, och därför dras slutsatsen att $\alpha = ma + nb = \text{sgd}(a, b)$. □

Korollarium 1.3.1. Om $\text{sgd}(a, b) = 1$ och $a \mid bc$ så måste $a \mid c$.

Bevis. $\text{sgd}(a, b) = 1$ ger med sats 1.3 att det finns m och n sådana att $ma + nb = 1$. Multiplikation med c ger: $mac + nbc = c$.

$$a \mid mac \text{ och } a \mid bc \Rightarrow a \mid (mac + nbc) \Rightarrow a \mid c. \qquad \square$$

Korollarium 1.3.2 (Euklides lemma)**.** Om a och b är heltal, p ett primtal och $p \mid ab$ så gäller att $p \mid a$ eller $p \mid b$.

Bevis. Eftersom p är ett primtal så uppstår två fall: $\text{sgd}(p, a) = p$ eller $\text{sgd}(p, a) = 1$. I första fallet gäller att $p \mid a$. I andra fallet gäller enligt korollarium 1.3.1 att $p \mid b$. □

I följande sats visas några egenskaper hos största gemensamma delaren:

Sats 1.4. Låt a, b och k vara heltal. Då gäller:[3]

(a) $d = \text{sgd}(a, b) \Rightarrow \text{sgd}(a/d, b/d) = 1$

(b) $\text{sgd}(a, b) = \text{sgd}(a + kb, b)$

(c) för alla icke-negativa heltal c är $\text{sgd}(ca, cb) = c \cdot \text{sgd}(a, b)$.

Bevis. (a). Sätt $m = \frac{a}{d}$, $n = \frac{b}{d}$. Om $\text{sgd}(m, n) \neq 1$, så skulle m och n ha en gemensam delare $d' > 1$. Då vore $m = m'd'$ och $n = n'd'$ där m' och n' är

[3]Boris Sjöberg, *Grundkurs i talteori*, Åbo: Sigma vid Åbo Akademi, 1992, s. 13.

heltal. Då vore $a = m'd'd$ och $b = n'd'd$, vilket skulle innebära att a och b skulle ha en gemensam delare $d'd > d$. Men det blir en motsägelse på grund av d:s definition. Därför är $\text{sgd}(m, n) = 1$.

(b). Varje gemensam delare till a och b är också gemensam delare till $a+kb$ och b. Omvänt gäller att varje gemensam delare till $a + kb$ och b är en gemensam delare till a och b på grund av att a kan skrivas som $a = (a + kb) - kb$. Talen a och b har alltså samma gemensamma divisorer som $a + kb$ och b. Därmed är (b) bevisad.

(c). Sätt $d = \text{sgd}(a, b)$. Enligt sats 1.3 gäller att $d = ax + by$ för heltal x, y. Eftersom $cax + cby = c \cdot (ax + by)$, leder det till att $cd = cax + cby$. Men det gäller också, att $\text{sgd}(ca, cb) = cax + cby$, och eftersom x och y är entydigt bestämda, dras slutsatsen att $\text{sgd}(ca, cb) = cd = c \cdot \text{sgd}(a, b)$. □

Sats 1.5. Om $\text{sgd}(a, b) = \text{sgd}(a, c) = 1$, så är $\text{sgd}(a, bc) = 1$.

Bevis. Antag att $\text{sgd}(a, b) = \text{sgd}(a, c) = 1$, då finns det med anledning av sats 1.3 heltal x, y och z, sådana att $ax + by = 1$ och $az + cw = 1$. Det betyder att

$$by \cdot cw = (1 - ax)(1 - az) = 1 - az - ax + a^2xz = 1 - an,$$

där $n = x + z - axz$ är ett heltal. Då fås likheten $an + bc \cdot yw = 1$ där n och yw är heltal och som medför att $\text{sgd}(a, bc) = 1$.[4] □

1.2 Kongruens

Kongruens är ett begrepp inom talteorin som infördes av Gauss i verket *Disquisitiones arithmeticae* år 1801.[5]

[4] Lindahl, s. 7.

[5] Sjöberg, s. 36.

Definition 1.3 (Kongruens)**.** Talen a och b är kongruenta modulo m om $m \mid (a-b)$. Detta skrivs som $a \equiv b \,(\mathrm{mod}\ m)$. Det är ekvivalent med att $a = qm + b$ för något heltal q, och innebär att mängden av alla tal b som är kongruenta med a modulo m är lika med mängden av alla rester som fås när a divideras med modulen m. Om $m \nmid (a-b)$, är a inte kongruent med b modulo m och det skrivs som $a \not\equiv b \,(\mathrm{mod}\ m)$.[6]

Ur ovanstående definition följer att $m \mid (a-b) \Leftrightarrow a - b = qm$ för något heltal q, vilket betyder att kongruenser kan förvandlas till likheter. Detta åskådliggörs genom följande exempel:

Exempel 1. $14 \equiv 6 \,(\mathrm{mod}\ 8)$ eftersom $14 = 8 \cdot 1 + 6$, $2 \equiv 2 \,(\mathrm{mod}\ 5)$ eftersom $2 = 5 \cdot 0 + 2$, $-7 \equiv 1 \,(\mathrm{mod}\ 4)$ eftersom $-7 = 4 \cdot (-2) + 1$ och $11 \not\equiv 4 \,(\mathrm{mod}\ 3)$ eftersom det inte finns något heltal q som uppfyller $11 = 3q + 4$.

Sats 1.6. Kongruensrelationen är en ekvivalensrelation[7], vilket innebär att

(a) $a \equiv a \,(\mathrm{mod}\ m)$,

(b) $a \equiv b \,(\mathrm{mod}\ m) \Rightarrow b \equiv a \,(\mathrm{mod}\ m)$,

(c) $a \equiv b \,(\mathrm{mod}\ m) \wedge b \equiv c \,(\mathrm{mod}\ m) \Rightarrow a \equiv c \,(\mathrm{mod}\ m)$.

Bevis. Eftersom $a - a = 0$ är delbart med m, gäller (a). Om $a - b$ är delbart med m, är även $b - a = -(a-b)$ delbart med m, därför gäller även (b). Slutligen gäller också (c) eftersom om m delar både $a-b$ och $b-c$, delar den även $(a-b) + (b-c) = a - c$. □

[6] Lindahl, s. 19.

[7] Sjöberg, s. 36.

1.2.1 Räkneregler vid kongruensräkning

Kongruenser liknar vanliga ekvationer i det avseendet att det går att utföra addition, subtraktion och multiplikation på dem:[8]

Sats 1.7. Låt a, b, c och d vara heltal.

(a) Om $a \equiv b \pmod{m}$ och $c \equiv d \pmod{m}$, så är $a \pm c \equiv b \pm d \pmod{m}$,

(b) Om $a \equiv b \pmod{m}$ och $c \equiv d \pmod{m}$, så är $ac \equiv bd \pmod{m}$.

Bevis. (a). Om $m \mid (a-b)$ och $m \mid (c-d)$, då gäller enligt sats 1.2 (b) att $m \mid \{(a-b) \pm (c-d)\}$.
(b). Om $a \equiv b \pmod{m}$ och $c \equiv d \pmod{m}$, så är $a = b + mh$ och $c = d + mk$ för heltal h och k. Då är $ac = (b+mh)(d+mk) = bd + m(bk + dh + mhk)$, vilket bevisar att $ac \equiv bd \pmod{m}$. □

Eftersom $c \equiv c \pmod{m}$, följer av ovanstående sats:

Korollarium 1.7.1. Om $a \equiv b \pmod{m}$, då är

(a) $a \pm c \equiv b \pm c \pmod{m}$,

(b) $ac \equiv bc \pmod{m}$.

Korollariet visar att båda leden i en kongruens kan ökas, minskas eller multipliceras med samma konstant utan att kongruensen förlorar sin giltighet.

Exempel 2. $14 \equiv 6 \pmod{8} \Leftrightarrow 11 \equiv 3 \pmod{8}$ och $6 \equiv 1 \pmod{5} \Leftrightarrow 24 \equiv 4 \pmod{5}$.

Det är dock inte möjligt att dividera båda leden med en konstant utan att kongruensen upphör att gälla, vilket följande exempel visar:

[8]Komaravolu Chandrasekharan, *Introduction to analytic number theory* (Vol 148), Springer Science & Business Media, 2012, s. 11.

Exempel 3. $45 \equiv 21 \pmod{24}$, men $15 \not\equiv 7 \pmod{24}$ där båda leden har dividerats med $\text{sgd}(45, 21) = 3$. Det gäller dock att $15 \equiv 7 \pmod{8}$.

Även modulen måste alltså ändras för att kongruensen inte ska upphöra att gälla. Division för kongruenser framgår av följande sats:

Sats 1.8. Om $ac \equiv bc \pmod{m}$, då är $a \equiv b \pmod{m/d}$, där $d = (c, m)$.

Bevis. Ur definition 1.3 följer att det finns ett heltal k sådant att $ac - bc = c(a-b) = km$. Division med d ger $(c/d)(a-b) = k(m/d)$. Vänsterledet, det vill säga $(c/d)(a-b)$, är alltså delbart med m/d. Enligt sats 1.4 är $(c/d, m/d) = 1$. Därför måste talet $a-b$ vara delbart med m/d (enligt korollarium 1.3.1). Det innebär att $a \equiv b \pmod{m/d}$.[9] □

I exempel 3 var $d = \text{sgd}(3, 24) = 3$ och därför blir modulen $m/d = 24/3 = 8$.

1.2.2 Restklasser

Följande beskrivning av restklasser kommer från Sjöbergs *Grundkurs i talteori*: Låt m vara ett heltal. Enligt sats 1.6 är kongruensrelationen en ekvivalensrelation, vilket medför att varje kongruens modulo m delar in mängden av hela tal, $\mathbb{Z}$, i ekvivalensklasser. Ekvivalensklasserna karaktäriseras av vilken rest som fås när a divideras med m, och därför kallas ekvivalensklasserna för restklasser när det gäller kongruens. Tal inom samma restklass är inbördes kongruenta modulo m, men inkongruenta med tal ur alla andra restklasser. För att bestämma restklasserna modulo m, tas ett godtyckligt heltal a och applicerar divisionsalgoritmen på a och m. Då fås $a = mq+r$, där $0 \leqslant r < m$, och därför är $a \equiv r \pmod{m}$. Enligt definitionen för resten r kan den endast anta värden $< m$, och de värdena är inbördes kongruenta modulo m. Det innebär att varje heltal a är kongruent med endast ett av talen $0, 1, 2, \ldots, m-1$.

[9] Sjöberg, s. 37.

En restklass modulo m består alltså av alla heltal på formen $mq + r$, där q går igenom alla heltal och r är ett fixt heltal mellan $0 \leqslant r \leqslant m - 1$. Det finns således $0, 1, 2, \ldots, m-1 = m$ stycken restklasser modulo m, en för varje möjlig rest.[10]

Definition 1.4. Om $\text{sgd}(a, m) = 1$, är en restklass relativt prima mot sin modul m.[11]

Definition 1.5. Med ett *fullständigt restsystem* modulo m menas de m heltalen $x_1, x_2, \ldots, x_m$ tillhörande olika restklasser modulo m. Exempel på ett fullständigt restsystem modulo m är mängden $\{0, 1, 2, \ldots, m - 1\}$.

Exempel 4. Antag att $m = 7$. Då fås sju restklasser $K_r = 7q + r$, där r går igenom ett fullständigt restsystem modulo 7:

$K_0 = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$

$K_1 = \{\ldots, -13, -6, 1, 8, 15, \ldots\}$

$K_2 = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$

$K_3 = \{\ldots, -11, -4, 3, 10, 17, \ldots\}$

$K_4 = \{\ldots, -10, -3, 4, 11, 18, \ldots\}$

$K_5 = \{\ldots, -9, -2, 5, 12, 19, \ldots\}$

$K_6 = \{\ldots, -8, -1, 6, 13, 20, \ldots\}$

Genom att ta ett tal ur varje restklass K_r, fås ett fullständigt restsystem modulo 7. Exempel på ett sådant är: $\{7, -6, 2, 17, -10, 5, 13\}$.

Från ett fullständigt restsystem kan ett annat fullständigt restsystem bildas. Följande sats visar hur det går till:

[10] Sjöberg, s. 38.

[11] Lindahl, s. 22.

Sats 1.9. Om $\{r_1, r_2, \ldots, r_m\}$ är ett fullständigt restsystem modulo m, så bildar talen $ar_1 + b, ar_2 + b, \ldots, ar_m + b$ ytterligare ett fullständigt restsystem modulo m, där a, b och m är heltal med $m > 0$, och $\text{sgd}(a, m) = 1$.

Bevis. Det gäller att visa att talen $ar_1 + b, ar_2 + b, \ldots, ar_m + b$ är parvis inkongruenta modulo m. Motsatsen antas, det vill säga att $ar_h + b \equiv ar_k + b \pmod{m}$ för något indexpar (h, k). Enligt sats 1.7 gäller att kongruensen kan förenklas till $ar_h \equiv ar_k \pmod{m}$ och eftersom $\text{sgd}(a, m) = 1$ kan kongruensen divideras med a enligt sats 1.8. Resultatet skulle då bli $r_h \equiv r_k \pmod{m}$ vilket inte kan stämma eftersom $r_1, r_2, \ldots, r_m$ bildar ett fullständigt restsystem modulo m (det vill säga de är inbördes inkongruenta). Motsatsen gäller alltså inte, och därför utgör talen $ar_1 + b, ar_2 + b, \ldots, ar_m + b$ ett fullständigt restsystem modulo m.[12] □

Sats 1.10. Om $a_1, a_2, \ldots, a_m$ är ett fullständigt restsystem modulo m, och h ett heltal relativt prima mot m, då bildar även $ha_1, ha_2, \ldots, ha_m$ ett fullständigt restsystem modulo m.

Bevis. För att bevisa satsen, räcker det att kontrollera att alla elementen i följden $ha_1, ha_2, \ldots, ha_m$ är parvis inkongruenta modulo m, d.v.s. valda från olika restklasser. Enligt sats 1.8 medför $ha_i \equiv ha_j \pmod{m}$ att $a_i \equiv a_j \pmod{m}$ eftersom $\text{sgd}(h, m) = 1$ enligt antagandet. Det betyder att $i = j$, vilket bevisar att elementen är parvis inkongruenta.[13] □

Liknande sats gäller för ett reducerat restsystem, men innan den bevisas följer några definitioner:

Definition 1.6. Ett *reducerat restsystem* modulo m är en mängd bestående av ett tal ur varje restklass som är relativt prima mot modulen m.

[12] Sjöberg, s. 39.

[13] Chandrasekharan, s. 13.

Definition 1.7 (Eulers ϕ-funktion)**.** Antalet restklasser som är relativt prima mot sin modul m betecknas $\phi(m)$.[14]

Exempel 5. I intervallet $[0, 11]$ $(= [0, 12-1])$ är talen 1, 5, 7 och 11 relativt prima mot modulen 12. Därför är $\phi(12) = 4$, och $\{1, 5, 7, 11\}$ ett reducerat restsystem modulo 12.

Sats 1.11. Om $r_1, r_2, \ldots, r_{\phi(m)}$ är ett reducerat restsystem modulo m, och om a och m är relativt prima, då formar också heltalen $ar_1, ar_2, \ldots, ar_{\phi(m)}$ ett reducerat restsystem modulo m. Därför gäller att

$$r_1 r_2 \cdots r_{\phi(m)} \equiv ar_1 \cdot ar_2 \cdots ar_{\phi(m)} \,(\mathrm{mod}\ m)$$

eller

$$(a^{\phi(m)} - 1) r_1 r_2 \cdots r_{\phi(m)} \equiv 0 \,(\mathrm{mod}\ m).$$

Bevis. Eftersom $\mathrm{sgd}(r_i, m) = 1$ och $\mathrm{sgd}(a, m) = 1$ är $\mathrm{sgd}(ar_i, m) = 1$ för $i = 1, 2, \ldots, \phi(m)$ enligt sats 1.5. Talen $ar_1, ar_2, \ldots, ar_{\phi(m)}$ tillhör därför restklasser som är relativt prima mot modulen m, och tillhör olika restklasser enligt samma orsak som bevisades i sats 1.10. Eftersom de dessutom är $\phi(m)$ stycken, bildar de ett reducerat restsystem modulo m.[15] □

Sats 1.12 (Eulers sats)**.** Om a är ett heltal och m ett positivt heltal, som är relativt prima mot a, då gäller:

$$a^{\phi(m)} \equiv 1 \,(\mathrm{mod}\ m).$$

Bevis. Låt $r_1, r_2, \ldots, r_{\phi(m)}$ vara ett reducerat restsystem modulo m. Då gäller enligt sats 1.11 att även $ar_1, ar_2, \ldots, ar_{\phi(m)}$ bildar ett reducerat restsystem

[14] Lindahl s. 22.

[15] Chandrasekharan, s. 13.

modulo m. Det innebär att talen i det första systemet är kongruenta med talen i det andra systemet i någon ordning, och om kongruenserna multipliceras med varandra, fås med användning av sats 1.7 (b):

$$r_1 r_2 \cdots r_{\phi(m)} \equiv a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Eftersom $\text{sgd}(r_i, m) = 1$, kan sats 1.8 användas för att dividera bort talen r_i från båda leden. Efter $\phi(m)$ divisioner fås $a^{\phi(m)} \equiv 1 \pmod{m}$, och Eulers sats är bevisad.[16] □

Nästa sats följer som korollarium av Eulers sats, men med m som ett primtal p, i vilket fall $\phi(p) = p - 1$.

Sats 1.13 (Fermats lilla sats)**.** Om p är ett primtal och $p \nmid a$, så är

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

Därför är $a^p \equiv a \pmod{p}$ för varje heltal a.

Bevis. Om $p \nmid a$, så är $\text{sgd}(a, p) = 1$. Talen $1, 2, \ldots, p-1$ är alla relativt primiska till p eftersom p är ett primtal, och det följer att $\phi(p) = p - 1$. Därför följer $a^{p-1} \equiv 1 \pmod{p}$ av Eulers sats. Om kongruensen multipliceras med a, fås $a \cdot a^{p-1} = a^p \equiv 1 \cdot a = a$, d.v.s. $a^p \equiv a \pmod{p}$. □

En speciell kongruens, som används för att testa om n är ett primtal, är följande:

Sats 1.14 (Wilsons sats)**.** Om p är ett primtal, så är $(p-1)! \equiv -1 \pmod{p}$.[17]

[16] Sjöberg, s. 60.

[17] Sjöberg, s. 55.

Bevis. För kroppen $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ modulo p har varje element $\neq 0$ en multiplikativ invers tillhörande mängden $\{1, 2, \ldots, p-1\}$. Om sedan talen $\{1, 2, \ldots, p-1\}$ multipliceras med varandra, och ordnas så att varje tal står bredvid sin invers, kommer produkten av dessa par, med anledning av sats 1.7, att vara $\equiv 1 \pmod{p}$. Talen 1 och $p-1$ återstår eftersom de har sig själva till invers. För dessa gäller att: $1 \equiv 1$ och $p-1 \equiv -1 \pmod{p}$. Därför gäller:

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}. \qquad \square$$

2 Kvadratiska rester

Kvadratiska rester härrör från lösning av kvadratiska kongruensekvationer av formen $x^2 \equiv a \pmod{p}$, där p är ett primtal och a ett heltal, som inte är delbart med p.[18] Vi börjar med att studera ett exempel.

Exempel 6. Beräkna x^2 och reducera modulo $m = 7$ för $x = 0, \ldots, 6$.

$0^2 = 0 \equiv 0 \pmod{7}$

$1^2 = 1 \equiv 1 \pmod{7}$

$2^2 = 4 \equiv 4 \pmod{7}$

$3^2 = 9 \equiv 2 \pmod{7}$

$4^2 = 16 \equiv 2 \pmod{7}$

$5^2 = 25 \equiv 4 \pmod{7}$

$6^2 = 36 \equiv 1 \pmod{7}$

Beräkningarna ovan visar, att värdena av x^2 modulo 7 endast kan vara 1, 2 eller 4. Det innebär att ekvationer som $x^2 \equiv a \pmod{7}$ där $a = 1, 2$ eller 4 är lösbara. Exempelvis ekvationen $x^2 \equiv 2 \pmod{7}$ är lösbar, med lösningarna $x = 3$ och $x = 4$. Å andra sidan har ekvationer av formen $x^2 \equiv a \pmod{7}$ inga lösningar när $a = 3, 5$ eller 6.

[18] Lindahl, s. 47.

Det visar sig, att kongruensekvationen $x^2 \equiv a \pmod{p}$ har exakt två rötter när talet a är relativt primiskt till modulen p.

Lemma 2.1. Låt p vara ett udda primtal, och a ett heltal som inte är delbart med p. Då har ekvationen $x^2 \equiv a \pmod{p}$ antingen inga lösningar alls, eller exakt två rötter.

Bevis. Om ekvationen $x^2 \equiv a \pmod{p}$ inte har några lösningar alls, är beviset klart. Antag därför, att den har åtminstone en lösning, $x = s$. Då fås $s^2 \equiv a \pmod{p}$. Ur det följer att även $x = -s \equiv p - s \pmod{p}$ är en lösning till ekvationen. Vi påstår sedan, att $x = s$ och $x = p - s$ inte är lika med varandra modulo p. För att bevisa det, antas att $p - s \equiv s \pmod{p}$. Då fås $p \mid (p-2s)$. Eftersom p är ett udda primtal enligt antagandet, gäller att $p \nmid 2$. Därför måste $p \mid s$, vilket medför att $p \mid s^2$. Eftersom $p \mid (s^2 - a)$, innebär det att p måste dela a, vilket leder till en motsägelse eftersom $p \nmid a$ enligt antagande. Därför gäller att $p - s \not\equiv s \pmod{p}$, vilket visar att ekvationen $x^2 \equiv a \pmod{p}$ har minst två lösningar. Det återstår att bevisa, att en lösning till ekvationen $x^2 \equiv a \pmod{p}$ måste vara kongruent med antingen $x = s$ eller $x = p - s$. Antag därför att $t^2 \equiv a \pmod{p}$. Då är $t^2 \equiv s^2 \pmod{p}$. Då måste $p \mid (t + s)(t - s)$. Enligt korollarium 1.3.2 betyder det att p måste dela en av faktorerna, d.v.s. antingen $p \mid (t - s)$ eller $p \mid (t - s)$. $p \mid (t + s) \Rightarrow t \equiv -s \pmod{p}$ och $p \mid (t - s) \Rightarrow t \equiv s \pmod{p}$.[19] □

Definition 2.1. Antag att $\text{sgd}(a, p) = 1$. Talet a sägs vara en *kvadratisk rest* modulo p, om kongruensen $x^2 \equiv a \pmod{p}$ har någon lösning x. Om lösning saknas, kallas a för en *kvadratisk ickerest* till p.

[19]Dan Ma, Solving Quadratic Congruences [Blogginlägg], 2013, hämtad 7 juni 2019 från: https://exploringnumbertheory.wordpress.com/2013/10/15/solving-quadratic-congruences/

Om a är en kvadratisk rest (respektive ickerest) modulo p, så är även varje tal i a:s restklass en kvadratisk rest (respektive ickerest). När vi vill ta reda på vilka kvadratiska rester eller ickerester som finns, behöver vi endast studera sådana tal a, som är inbördes inkongruenta modulo p. Eftersom a dessutom ska vara relativt primiskt till p enligt antagandet, räcker det att kontrollera ett reducerat restsystem modulo p, exempelvis talen $1, 2, \ldots, p-1$. Samma sak gäller för eventuella rötter till kongruensen $x^2 \equiv a \pmod{p}$, eftersom om x är en lösning, så är även varje y med $x \equiv y \pmod{p}$ en lösning. Dessutom måste varje rot x vara relativt primiskt till p, eftersom då $x^2 - a$ är delbart med p, så vore även a delbart med p om $x = kp$ för något heltal k. För att finna möjliga lösningar till kongruensen $x^2 \equiv a \pmod{p}$, räcker det alltså att kontrollera talen $1, 2, \ldots, p-1$.[20]

I exempel 6 studerades fallet $p = 7$, och då kvadrerades talen $1, 2, \ldots, p-1 = 6$. Eftersom 7 är ett primtal, och a därför är relativt primiskt till modulen, räcker det att studera ett reducerat restsystem modulo 7, i detta fall talen $1, \ldots, 6$. Efter att de kvadrerade talen reducerats modulo 7, går det att utläsa vilka tal som är kongruenta med en kvadrat modulo 7. För modulo 7 är de kvadratiska resterna $\{1, 2, 4\}$, och kvadratiska ickeresterna $\{3, 5, 6\}$. 0 är varken en kvadratisk rest eller ickerest, eftersom den är delbar med p.

I följande stycke finns tabeller som visar vilka kvadrater som finns modulo de fyra första primtalen.

2.1 Tabeller med kvadrater modulo 5, 7, 11 och 13

Av bekvämlighetsskäl betecknas kvadratisk rest i fortsättningen med QR (quadratic residue) och kvadratisk ickerest med NR (non-quadratic residue).

[20] Sjöberg, s. 80.

Modulo 5

x	x^2	$\equiv a$
0	0	0
1	1	1
2	4	4
3	9	4
4	16	1

QR: $\{1, 4\}$

NR: $\{2, 3\}$

Modulo 7

x	x^2	$\equiv a$
0	0	0
1	1	1
2	4	4
3	9	2
4	16	2
5	25	4
6	36	1

QR: $\{1, 2, 4\}$

NR: $\{3, 5, 6\}$

Modulo 11

x	x^2	$\equiv a$
0	0	0
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3
6	36	3
7	49	5
8	64	9
9	81	4
10	100	1

QR:

$\{1, 3, 4, 5, 9\}$

NR:

$\{2, 6, 7, 8, 10\}$

Modulo 13

x	x^2	$\equiv a$
0	0	0
1	1	1
2	4	4
3	9	9
4	16	3
5	25	12
6	36	10
7	49	10
8	64	12
9	81	3
10	100	9
11	121	4
12	144	1

QR:

$\{1, 3, 4, 9, 10, 12\}$

NR:

$\{2, 5, 6, 7, 8, 11\}$

Några observationer kan göras:

- Varje kvadratisk rest, d.v.s. varje nollskilt tal som är en kvadrat, verkar uppkomma två gånger. Exempelvis är 9 både 3^2 och 8^2 modulo 11. Dessutom verkar de kvadratiska resterna uppkomma symmetriskt: om varje tabell delas på hälften, uppkommer samma rest både uppe och nere (förutom 0 som varken är QR eller NR). Med andra ord är kvadraten av x samt $p - x$ lika modulo p.

- Det finns lika många kvadratiska rester, som kvadratiska ickerester, modulo ett udda primtal.

Första observationen stöds av att ekvationen $x^2 \equiv a \pmod{p}$ har enligt lemma 2.1 exakt två rötter om den är lösbar. Ekvationen är lösbar för varje kvadratisk rest, och därför uppkommer varje QR två gånger. Symmetrin beror på att $a^2 \equiv p^2 - 2pa + a^2 = (p-a)^2 \pmod{p}$.
Andra observationen bevisas i följande avsnitt.

2.2 Antal kvadratiska rester och kvadratiska ickerester

Exemplen i tabellerna i avsnitt 2.1 visade, att det finns lika många kvadratiska rester som kvadratiska ickerester. Detta gäller allmänt, när modulen är ett udda primtal.

Sats 2.2. Låt p vara ett udda primtal. Då existerar det exakt $(p-1)/2$ inkongruenta kvadratiska rester (respektive kvadratiska ickerester) till p.

Bevis. Alla kvadratiska rester a i intervallet $[1, p-1]$ fås genom att kvadrera talen $1, 2, \ldots, p-1$ och därefter reducera modulo p. För varje a finns det två heltal b och $p-b$ i $[1, p-1]$, eftersom $b^2 \equiv (p-b)^2 = p^2 - 2pb + b^2 \pmod{p}$ för $b = 1, 2, \ldots, (p-1)/2$. Antalet kvadratiska rester blir alltså hälften, det vill säga $(p-1)/2$. Eftersom summan av antalet kvadratiska rester och ickerester är $p-1$, betyder det att det måste finnas lika många, $(p-1)/2$, kvadratiska ickerester modulo p. Ett system av inkongruenta kvadratiska rester modulo p är därför exempelvis talen (när de reduceras modulo p)

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{2.1}$$

De är inkongruenta modulo p eftersom om motsatsen antas, att $h^2 \equiv k^2 \pmod{p}$ för några h, k mellan 1 och $(p-1)/2$, så vore $(h^2 - k^2) = (h-k)(h+k)$

delbart med p, men det är en omöjlighet eftersom $h + k$ ska vara ett tal mindre än p, och $|h - k| < (p - 1)/2$. Talen 2.1 utgör alltså ett fullständigt system av inkongruenta kvadratiska rester modulo p.[21] □

Anmärkning. $p = 2$ är det enda jämna primtalet, och i det fallet blir lösningarna till ekvationen $x^2 \equiv a \pmod 2$ följande: för $x^2 \equiv 0 \pmod 2$ är $x = 0$ den enda lösningen, och för $x^2 \equiv 1 \pmod 2$ är $x = 1$ enda lösningen eftersom det modulo 2 finns endast två restklasser; 0 och 1. För sammansatta moduli kan den kvadratiska ekvationen $x^2 \equiv a \pmod m$ ha fler än två lösningar. Därför studeras i detta arbete endast moduli som är udda primtal.

För att avgöra om ett givet tal a är en kvadratisk rest modulo p, går det att beräkna kvadraterna av alla restklasser modulo p och sedan göra en tabell som i exempel 6. Men vid stora p blir det jobbigt.[22] Därför finns det ett hjälpmedel som kallas för Legendresymbolen som introduceras i följande avsnitt.

2.3 Legendresymbolen

Adrien-Marie Legendre introducerade notationen $\left(\frac{a}{p}\right)$ som kallas för Legendresymbolen.[23] Med hjälp av den går det att, på ett enkelt sätt, uttrycka att ett heltal är en kvadratisk rest eller en kvadratisk ickerest modulo ett udda primtal. Symbolen definieras på följande sätt:

Definition 2.2. Låt p vara ett udda primtal och a ett godtyckligt heltal. Då gäller:

[21] Lindahl, s. 49.

[22] Engblom, Andreas och Sola, Alan, *Talteori*, Stockholm: KTHs Matematiska cirkel, Institutionen för matematik, 2008, s. 47.

[23] Joseph H Silverman, *A friendly introduction to number theory*, Upper Saddle River, NJ: Prentice-Hall, 2001, s. 148.

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

Exempel 7. $(\frac{4}{7}) = 1$ och $(\frac{5}{13}) = -1$ eftersom 4 är kvadratisk rest modulo 7 medan 5 är en kvadratisk icke-rest modulo 13.

Sats 2.3 (Eulers kriterium)**.** Låt p vara ett udda primtal och a ett heltal, som inte är delbart med p. Då gäller:[24]

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

Satsen ger att:

$$a^{(p-1)/2} \equiv 1 \,(\text{mod } p) \text{ om } a \text{ är en kvadratisk rest modulo } p,$$

och

$$a^{(p-1)/2} \equiv -1 \,(\text{mod } p) \text{ om } a \text{ är en kvadratisk ickerest modulo } p.$$

Bevis. Om a är en kvadratisk rest modulo p, då är $\left(\frac{a}{p}\right) = 1$. Enligt definition 2.2 har då kongruensen $x^2 \equiv a \,(\text{mod } p)$ en lösning. Kalla den lösningen x_0. Då gäller att:

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv (x_0^2)^{\frac{p-1}{2}} \equiv x_0^{p-1} \,(\text{mod } p) \\ &\equiv 1 \,(\text{mod } p) \,(\text{enligt Fermats lilla sats (1.13) eftersom } p \nmid x_0) \\ &\equiv \left(\frac{a}{p}\right) \,(\text{mod } p). \end{aligned}$$

Antag sedan att a är en kvadratisk ickerest modulo p. Då är $\left(\frac{a}{p}\right) = -1$. För varje heltal i $(1 \leqslant i \leqslant p-1)$ finns ett entydigt bestämt annat heltal j

[24] Sjöberg, s. 81.

$(1 \leqslant j \leqslant p-1)$ så att $ij \equiv a \pmod{p}$, eftersom de linjära kongruenserna är lösbara. Dessutom är $i \neq j$, eftersom annars vore $ij = i^2 \equiv a \pmod{p}$ och a är en kvadratisk rest modulo p, och då vore $\left(\frac{a}{p}\right) = 1$ vilket blir en motsägelse. Eftersom $i \neq j$, kan heltalen mellan 1 och $p-1$ matchas till $(p-1)/2$ par som alla är kongruenta med a modulo m. Om dessa heltal multipliceras samman, fås:

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p},$$

vilket ger

$$-1 \equiv a^{\frac{p-1}{2}} \pmod{p} \text{ (enligt Wilsons sats 1.14)}$$

och

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

Exempel 8. Vi undersöker om 7 är en kvadratisk rest modulo 13. Eulers kriterium ger:

$$7^{\frac{13-1}{2}} = 7^6 \equiv -1 \pmod{13},$$

det vill säga 7 är en kvadratisk ickerest modulo 13.

Sats 2.4. Låt p vara ett udda primtal. Då gäller:[25]

(a) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,

(b) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$,

(d) om $\text{sgd}(a,p) = 1$, så är $\left(\frac{a^2}{p}\right) = 1$ och $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$,

(e) $\left(\frac{1}{p}\right) = 1$,

(f) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{om } p \equiv 1 \pmod{4}, \\ -1 & \text{om } p \equiv 3 \pmod{4}. \end{cases}$

[25] Lindahl, s. 53.

Bevis. (a). Om $p \mid a$, är kongruensen uppenbar, och om $\text{sgd}(p, a) = 1$ så är (a) en omformulering av Eulers kriterium (sats 2.3). Resterande bevis följer ur (a):

(b). gäller eftersom $a \equiv b \Rightarrow a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}}$ (a och b tillhör samma restklass modulo p, och är därför båda kvadratiska rester eller båda kvadratiska icke-rester modulo p).

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

(d). Legendresymbolen kan endast anta värdet $+1$ eller -1 (då $a \nmid p$), därför fås $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{p}\right) = 1$ och $\left(\frac{a^2 b}{p}\right) = 1 \cdot \left(\frac{b}{p}\right) = \left(\frac{b}{p}\right)$.

(e). följer ur (a).

(f). $(p-1)/2$ är jämn om $p \equiv 1 \pmod 4$ eftersom $(p-1)/2 = (4n+1-1)/2 = 2n$, och udda om $p \equiv 3 \pmod 4$ eftersom $(p-1)/2 = (4n+3-1)/2 = 2n+1$. Därför gäller (f). □

Exempel 9. Är 48 en kvadrat modulo 61?

$$\left(\frac{48}{61}\right) = \left(\frac{2 \cdot 2 \cdot 2 \cdot 2 \cdot 3}{61}\right) = \left(\frac{2}{61}\right)\left(\frac{2}{61}\right)\left(\frac{2}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right) = \left(\frac{3}{61}\right).$$

Det har ingen betydelse om 2 är en kvadratisk rest eller inte modulo 61, och därmed vad $\left(\frac{2}{61}\right)$ är, eftersom $(+1)^2(+1)^2 = (-1)^2(-1)^2 = 1$. Det återstår att observera att $8^2 \equiv 3 \pmod{61}$, så 3 är en kvadratisk rest modulo 61. Därför är:

$$\left(\frac{48}{61}\right) = \left(\frac{3}{61}\right) = +1$$

och 48 en kvadratisk rest modulo 61.

Om sats 2.4 (c) och (f) kombineras, fås för varje positivt heltal a som är relativt primiskt till primtalet $p > 2$:

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

Ovanstående visar, att om man vill ta reda på om ett negativt heltal är en kvadratisk rest eller en kvadratisk ickerest modulo ett primtal $p > 2$, kan det härledas till att lösa problemet för talets absolutbelopp.

Legendresymbolen kan användas för att påvisa multiplikationsreglerna för kvadratiska rester och kvadratiska ickerester. De presenteras och bevisas i följande avsnitt.

2.4 Multiplikationsregler

Vad händer om man multiplicerar en kvadratisk rest med en kvadratisk rest, en kvadratisk rest med en kvadratisk ickerest eller två kvadratiska ickerester med varandra?

Exempel 10. 2 och 4 är QR:s modulo 7 och $2 \cdot 4 = 8 \equiv 1 \pmod 7$, en QR.

Hur blir det för QR · NR och NR · NR? Följande är exempel som använder informationen från tabellerna 2.1:

QR · NR ≡ ?? (mod p)	
$1 \cdot 3 \equiv 3$	**NR** (mod 5)
$4 \cdot 5 \equiv 6$	**NR** (mod 7)
$9 \cdot 2 \equiv 7$	**NR** (mod 11)
$3 \cdot 8 \equiv 11$	**NR** (mod 13)

NR · NR ≡ ?? (mod p)	
$2 \cdot 3 \equiv 1$	**QR** (mod 5)
$3 \cdot 5 \equiv 1$	**QR** (mod 7)
$6 \cdot 8 \equiv 4$	**QR** (mod 11)
$5 \cdot 7 \equiv 9$	**QR** (mod 13)

Detta leder till följande sats:

Sats 2.5. Låt p vara ett udda primtal. Då är:[26]

(a) produkten av två kvadratiska rester modulo p en kvadratisk rest;
$\mathrm{QR} \cdot \mathrm{QR} = \mathrm{QR}$,

(b) produkten av en kvadratisk rest och en icke-rest modulo p en icke-rest;
$\mathrm{QR} \cdot \mathrm{NR} = \mathrm{NR}$,

(c) produkten av två icke-rester modulo p en kvadratisk rest;
$\mathrm{NR} \cdot \mathrm{NR} = \mathrm{QR}$.

Bevis. I sats 2.4 (c) såg vi att multiplikationsreglerna kan uttryckas med hjälp av Legendresymbolen:[27]

$$\mathrm{QR} \cdot \mathrm{QR} = (+1) \cdot (+1) = +1,$$

$$\mathrm{QR} \cdot \mathrm{NR} = (+1) \cdot (-1) = -1,$$

$$\mathrm{NR} \cdot \mathrm{NR} = (-1) \cdot (-1) = +1. \qquad \square$$

Exempel 11.

$$\mathrm{QR} \cdot \mathrm{QR}\text{: } \left(\frac{2}{7}\right)\left(\frac{4}{7}\right) = \left(\frac{8}{7}\right) = 1 \quad (\mathrm{QR}),$$

$$\mathrm{QR} \cdot \mathrm{NR}\text{: } \left(\frac{1}{5}\right)\left(\frac{3}{5}\right) = \left(\frac{3}{5}\right) = -1 \quad (\mathrm{NR}),$$

$$\mathrm{NR} \cdot \mathrm{NR}\text{: } \left(\frac{6}{11}\right)\left(\frac{8}{11}\right) = \left(\frac{48}{11}\right) = 1 \quad (\mathrm{QR}).$$

[26] Silverman, s. 146.
[27] Silverman, s. 148.

2.5 Gauss lemma

Ett annat sätt att beräkna $\left(\frac{a}{p}\right)$ görs med hjälp av Gauss lemma:

Sats 2.6 (Gauss lemma)**.** Om p är ett udda primtal och a ett heltal som inte är delbart med p, då gäller:[28]

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

där N står för antal tal i följden

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a, \tag{2.2}$$

vilkas rester modulo p är $> \frac{p}{2}$.

Bevis. Talen (2.2) är parvis inkongruenta modulo p, eftersom de bildar en del av ett fullständigt restsystem modulo p (enligt sats 1.9). Inget av talen är delbart med p (enligt korollarium 1.3.2) och därför är alla huvudrester nollskilda. Huvudresterna ligger alltså i intervallet $[1, p-1]$. Om $r_1, r_2, \ldots, r_N$ är de huvudrester, som är $> \frac{p}{2}$, och $s_1, s_2, \ldots, s_M$ är de huvudrester, som är $< \frac{p}{2}$, då är $N + M = (p-1)/2$. Observera att talen r_N och s_M är alla olika, eftersom talen $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ är inkongruenta modulo p. Talen

$$p - r_1, p - r_2, \ldots, p - r_N, s_1, s_2, \ldots, s_M \tag{2.3}$$

är också alla olika. Det innebär, att inget tal $p - r_i$ är alltså lika med något tal s_k, eftersom antag att $p - r_i = s_k$, och låt $r_i \equiv ma \pmod{p}$ och $s_k \equiv na \pmod{p}$, där m och n är olika tal mellan 1 och $(p-1)/2$. Då är $p = r_i + s_k \equiv (m+n)a \pmod{p}$, och eftersom $\text{sgd}(a, p)=1$ måste $p \mid (m+n)$, vilket är en motsägelse eftersom $m + n \leqslant \frac{p-1}{2} + \frac{p-1}{2} = p - 1 < p$. Det är beviset för att talen (2.3) är alla olika heltal i intervallet $[1, \frac{p-1}{2}]$, och eftersom de är

[28] Sjöberg, s. 84.

$M + N = (p-1)/2$ till antalet, så är de lika med talen $1, 2, \ldots, (p-1)/2$ i någon ordning. Därför gäller att:

$$(p - r_1)(p - r_2) \cdots (p - r_N) s_1 s_2 \cdots s_M = \left(\frac{p-1}{2}\right)!$$

$(p - r_i)$ är kongruent med $-r_i$, så om varje $(p - r_i)$ ersätts med $-r_i$ fås:

$$(-1)^N r_1 r_2 \cdots r_N s_1 s_2 \cdots s_M \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Men talen $r_1, r_2, \ldots, r_N, s_1, s_2, \ldots, s_M$ är även i någon ordning kongruenta med talen $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ $(= a^{(p-1)/2}\left(\frac{p-1}{2}\right)!)$ och det följer att

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^N a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}a \equiv a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \pmod{p}.$$

Eftersom varje faktor i $\left(\frac{p-1}{2}\right)!$ är relativt prima mot p, kan båda leden i kongruensen ovan divideras med $\left(\frac{p-1}{2}\right)!$, vilket leder till

$$a^{(p-1)/2} \equiv (-1)^N \pmod{p}.$$

Med Eulers kriterium fås:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv (-1)^N \pmod{p}. \qquad \square$$

Exempel 12 (Gauss lemma)**.** Låt $p = 13$ och $a = 3$. Då gäller att $a \nmid p$ och $N = 4$ eftersom N betecknar de tal i följden $\{3 \cdot 1,\ 3 \cdot 2,\ 3 \cdot 3,\ 3 \cdot 4,\ 3 \cdot 5,\ 3 \cdot \frac{12}{2}\} = \{3,\ 6,\ 9,\ 12,\ 15,\ 18\}$ vilkas huvudrester modulo 13 är $> p/2 = 13/2$. Huvudresterna blir $\{3, 6, 9, 12, 2, 5\}$ varav 2 stycken, 9 och 12, är $> 13/2$. Då blir $\left(\frac{3}{13}\right) = (-1)^2 = 1$. Alltså är 3 en kvadratisk rest modulo 13.

Gauss lemma kan tillämpas på $\left(\frac{2}{p}\right)$:

Sats 2.7. Låt p vara ett udda primtal. Då är 2 en kvadratisk rest till p om $p \equiv \pm 1 \pmod{8}$, och en kvadratisk ickerest till p om $p \equiv \pm 3 \pmod{8}$. Det kan skrivas som:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 \text{ om } p \equiv \pm 1 \pmod{8}, \\ -1 \text{ om } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Bevis. Om $a = 2$ väljs i Gauss lemma, står N för antalet tal som är större än $p/2$ i följden $2, 4, 6, \ldots, p-1$. Uttryckt på annat sätt är N antalet heltal k sådana att $p/2 < 2k < p$ (ekvivalent med $p/4 < k < p/2$). Därav följer att $N = [p/2] - [p-4]$. Udda tal kan skrivas antingen på formen $p = 4n+1$ eller $p = 4n-1$, och för den första formen blir $N = 2n - n = n$, och för andra blir också $N = (2n-1) - (n-1) = n$. Det innebär att talet N är jämnt om n är jämnt, det vill säga om $p = 8m \pm 1$ (där $n = 2m$), och N är udda om n är udda, det vill säga om $p = 8m \pm 3$ (där $n = 2m+1$).[29] □

Exempel 13. Kongruensen $x^2 \equiv 2 \pmod 7$ är lösbar eftersom 2 enligt sats 2.7 är en kvadratisk rest modulo 7 ($7 \equiv -1 \pmod 8$).

$1^2 \equiv 1 \pmod 7$

$2^2 \equiv 4 \pmod 7$

$3^2 \equiv 2 \pmod 7$

$4^2 \equiv 2 \pmod 7$

$5^2 \equiv 4 \pmod 7$

$6^2 \equiv 1 \pmod 7$

Av beräkningarna framgår, att $x^2 \equiv 2 \pmod 7$ har två lösningar, $x = 3$ och $x = 4$.

Exempel 14. Beräkna $\left(\frac{75}{11}\right)$. Vi börjar med att reducera talet 75 modulo 11 och får $75 \equiv -2 \pmod{11}$. Om sats 2.4 (b), (c) och (f) kombineras med sats 2.7 fås:

$$\left(\frac{75}{11}\right) = \left(\frac{-2}{11}\right) = (-1)^5 \left(\frac{2}{11}\right) = (-1)^5(-1)^{15} = 1,$$

vilket innebär att 75 är en kvadratisk rest modulo 11.

För att beräkna Legendresymbolen för stora tal a och p, blir Gauss lemma för besvärligt att använda. Därför används i stället Gauss reciprocitetslag

[29] Lindahl, s. 55.

som är innehållet i nästa avsnitt.

2.6 Kvadratisk reciprocitet

Satsen om kvadratisk reciprocitet har en lång och komplicerad historia.[30] Viktiga bidrag gjordes av Euler och Legendre men Gauss gav det första korrekta beviset år 1796 och det publicerades först i hans *Disquitiones arithmeticae* från 1801. Senare presenterade han ytterligare sju bevis, och sedan dess har över hundra bevis offentliggjorts av andra matematiker.[31]

Gauss reciprocitetslag går ut på att för två från varandra skilda, udda primtal, kan Legendresymbolen för den ena fås om den andra är känd. Namnet för satsen kommer ifrån att Legendresymbolen för p med avseende på q är lika med Legendresymbolen för q med avseende på p (eventuellt med ett minustecken framför). Ordet ”reciprotas” kommer från latin och betyder ”ömsesidighet”. Om p är en kvadratisk rest modulo q är alltså samma sak som att fråga om q är en kvadratisk rest modulo p. Satsen formuleras på följande sätt:

Sats 2.8 (Gauss reciprocitetslag)**.** Om p och q är två olika udda primtal, så gäller:

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

Det finns som sagt flera bevis för satsen, men i detta arbete presenteras endast ett, varav nedanstående framställning kommer från Boris Sjöbergs *Grundkurs i talteori*:[32]

[30]Frans Lemmermeyer, *Reciprocity Laws: from Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[31]Sjöberg, s. 86.

[32]Sjöberg, ss. 86-88.

Bevis. I talföljderna

$$p,\ 2p,\ 3p, \ldots,\ \frac{q-1}{2} \cdot p \tag{2.4}$$

och

$$q,\ 2q,\ 3q,\ \ldots,\ \frac{p-1}{2} \cdot q \tag{2.5}$$

betecknas med s antalet tal i (2.4) vilkas huvudrester modulo q är $> q/2$, och på motsvarande sätt står t för antalet tal i följden (2.5) vilkas huvudrester modulo p är $> p/2$. Enligt Gauss lemma gäller:

$$\left(\frac{p}{q}\right) = (-1)^s \ \text{ och } \ \left(\frac{q}{p}\right) = (-1)^t.$$

Om de multipliceras med varandra, fås:

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

Reciprocitetssatsen är bevisad, om det går att visa att

$$s + t \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2. \tag{2.6}$$

Vi noterar först, att s är lika med antal minsta absoluta rester < 0 modulo q, eftersom mot varje huvudrest r_1 $\left(\frac{q}{2} < r_1 < q\right)$ finns en absolut rest $r_1 - q$ med $-\frac{q}{2} < r_1 - q < 0$. På motsvarande sätt är t lika med antal minsta absoluta rester < 0 modulo p, eftersom det mot varje r_2 $\left(\frac{p}{2} < r_2 < p\right)$ finns en absolut rest $r_2 - p$ med $-\frac{p}{2} < r_2 - p < 0$. Detta betyder, att när talen s och t ska bestämmas, kan vi hålla på med minsta absoluta rester < 0.

Låt hp vara något av talen i (2.4). Minsta absoluta rest modulo q fås genom $hp - kq$, där k är det entydigt bestämda positiva heltal sådant att $-\frac{q}{2} < hp - kq < \frac{q}{2}$. För en negativ rest $hp - kq$ bestäms k av olikheterna

$$-\frac{q}{2} < hp - kq < 0. \tag{2.7}$$

I detta sammanhang är kq något av talen (2.5), eftersom om motsatsen antas (d.v.s. $k \geqslant \frac{p+1}{2}$), skulle vi ha $hp - kq \leqslant \frac{q-1}{2} \cdot p - \frac{p+1}{2} \cdot q = -\frac{p}{2} - \frac{q}{2} < -\frac{q}{2}$, vilket inte stämmer överens med (2.7). kq är alltså något av talen (2.5). Enligt antagandena finns det därför i (2.4) och (2.5) s talpar (hp, kq) som uppfyller olikheterna (2.7).

På motsvarande sätt visas, att det i (2.4) och (2.5) finns t talpar (hp, kq) som uppfyller olikheterna

$$-\frac{p}{2} < kq - hp < 0. \tag{2.8}$$

Av (2.7) och (2.8) följer att det i (2.4) och (2.5) finns $s + t$ talpar (hp, kq), som uppfyller olikheterna

$$-\frac{q}{2} < hp - kq < \frac{p}{2}. \tag{2.9}$$

Alla övriga talpar (hp, kq) i (2.4) och (2.5) uppfyller därför

$$hp - kq < -\frac{q}{2} \quad \text{eller} \quad hp - kq > \frac{p}{2}. \tag{2.10}$$

Sätt $h' = \frac{q+1}{2} - h \;\; (1 \leqslant h \leqslant \frac{q-1}{2})$ och $k' = \frac{p+1}{2} - k \;\; (1 \leqslant k \leqslant \frac{p-1}{2})$. Då är $h'p$ det h:te talet i (2.4) från slutet räknat, och $k'q$ det k:te talet i (2.5) från slutet räknat. Då blir

$$(hp - kq) + (h'p - k'q) = hp - kq + \frac{pq}{2} + \frac{p}{2} - \frac{2ph}{2} - \frac{pq}{2} - \frac{q}{2} + \frac{2qk}{2} = \frac{p}{2} - \frac{q}{2}.$$

Antag nu att $hp - kq$ uppfyller $hp - kq < -\frac{q}{2}$ (d.v.s. första av olikheterna (2.10)). Då är $h'p - k'q = \frac{p}{2} - \frac{q}{2} - (hp - kq) > \frac{p}{2} - \frac{q}{2} - \left(-\frac{q}{2}\right) = \frac{p}{2}$.

Alltså om $hp - kq$ uppfyller den första olikheten i (2.10), så uppfyller $h'p - k'q$ den andra. På motsvarande sätt går det att visa, att om $hp - kq$ uppfyller den andra olikheten i (2.10), så uppfyller $h'p - k'q$ den första. Det innebär, att om talparet (hp, kq) uppfyller ena olikheten, så uppfyller $(h'p, k'q)$ den

andra.

Antag nu att det finns u talpar (hp, kq) som uppfyller första olikheten av (2.10). Då finns det även u talpar, som uppfyller den andra olikheten av (2.10). Det finns alltså totalt $u + u = 2u$ talpar (hp, kq) som uppfyller en av olikheterna (2.10). Av (2.4) och (2.5) går det att bilda $\frac{p-1}{2} \cdot \frac{q-1}{2}$ talpar (hp, kq). Av dessa uppfyller $s + t$ stycken talpar olikheterna (2.9), medan de övriga $2u$ talparen uppfyller en av olikheterna (2.10). Därför är

$$s + t + 2u = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

vilket innebär att kongruensen (2.6) gäller eftersom reducering modulo 2 gör att $2u$ försvinner. Därmed är reciprocitetssatsen bevisad. □

Exempel 15. Är $a = 3$ en kvadratisk rest modulo $p = 97$?
$\left(\frac{3}{97}\right) = (-1)^{1 \cdot 98} \left(\frac{97}{3}\right) = \left(\frac{1}{3}\right) = +1$. Med hjälp av kvadratiska reciprocitetssatsen kunde konstateras, att 3 är en kvadratisk rest modulo 97.

Det finns en alternativ formulering till reciprocitetssatsen:

Korollarium 2.8.1. Om p och q är två olika udda primtal, så gäller:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) \text{ om } p \equiv 1 \,(\mathrm{mod}\ 4) \text{ eller } q \equiv 1 \,(\mathrm{mod}\ 4), \\ -\left(\frac{q}{p}\right) \text{ om } p \equiv q \equiv 3 \,(\mathrm{mod}\ 4). \end{cases}$$

Bevis. $\frac{p-1}{2} \cdot \frac{q-1}{2} = \frac{(p-1)(q-1)}{4}$ är udda endast om talen $(p-1)/2$ och $(q-1)/2$ båda är udda, d.v.s. om $p \equiv q \equiv 3 \,(\mathrm{mod}\ 4)$. Legendresymbolerna $\left(\frac{p}{q}\right)$ och $\left(\frac{q}{p}\right)$ har i det fallet motsatta tecken.[33] □

Exempel 16. Låt $p = 17$ och $q = 21$. Eftersom $17 \equiv 1 \,(\mathrm{mod}\ 4)$ och $21 \equiv 1 \,(\mathrm{mod}\ 4)$, gäller enligt korollarium 2.8.1 att $\left(\frac{17}{21}\right) = \left(\frac{21}{17}\right)$. På grund av sats 2.4 (b) är $\left(\frac{21}{17}\right) = \left(\frac{4}{17}\right)$ och det följer av sats 2.4 (d) att $\left(\frac{4}{17}\right) = \left(\frac{2}{17}\right) \cdot \left(\frac{2}{17}\right) = 1$. Det innebär, att även $\left(\frac{17}{21}\right) = 1$.

[33] Sjöberg, s.88

Exempel 17. Är kongruensen $x^2 \equiv -38 \pmod{61}$ lösbar?

Lösning. Kongruensen är lösbar, om $\left(\frac{-38}{61}\right) = +1$. Sats 2.4 (c) ger:

$$\left(\frac{-38}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{19}{61}\right).$$

$\left(\frac{-1}{61}\right) = (-1)^{30} = +1$ enligt sats 2.4 (f).

$\left(\frac{2}{61}\right) = (-1)^{465} = -1$ enligt sats 2.7.

Med användning av reciprocitetssatsen samt sats 2.4 (d) fås

$$\left(\frac{19}{61}\right) = (-1)^{9\cdot 30}\left(\frac{61}{19}\right) = \left(\frac{4}{19}\right) = \left(\frac{2^2}{19}\right) = +1.$$

Därför är

$$\left(\frac{-38}{61}\right) = (+1)(-1)(+1) = -1,$$

och kongruensen är inte lösbar.

Avslutning

Den kvadratiska reciprocitetssatsen gäller för kongruenser på formen $x^2 \equiv p \pmod{q}$, där p och q är udda primtal. Finns det en liknande konstruktion för exempelvis kubiska eller bikvadratiska rester (där kubiska rester härrör från lösning av kongruenser på formen $x^3 \equiv p \pmod{q}$, och bikvadratiska, eller kvartiska, rester av kongruenser på formen $x^4 \equiv q \pmod{p}$)? Svaret är ja. Den kvadratiska reciprocitetssatsen är egentligen bara början på en lång rad av reciprocitetssatser, och Gauss - och många andra matematiker - lade ned mycket tid på att försöka finna dem. Generaliserandet av Gauss reciprocitetssats har länge varit ett ledande problem inom matematik, och arbetet med det berikar talteorin än i dag.

Referenser

Chandrasekharan, K. (2012). *Introduction to analytic number theory* (vol. 148). Springer Science & Business Media.

Engblom, A. & Sola, A. (2008). *Talteori*. KTHs Matematiska cirkel. Institutionen för matematik.

Lemmermeyer, F. (2000). *Reciprocity laws: from Euler to Eisenstein*. Springer Monographs in Mathematics, Springer-Verlag.

Lindahl, L. (2012). *Elementär talteori*. Uppsala universitet.

Ma, D. (2013, 15 oktober). Solving Quadratic Congruences [Bloggin-lägg]. Hämtad 7 juni 2019, från `https://exploringnumbertheory.wordpress.com/2013/10/15/solving-quadratic-congruences/`

Silverman, J. H. (2001). *A friendly introduction to number theory*. Prentice-Hall.

Sjöberg, B. (1992). *Grundkurs i talteori*. Sigma vid Åbo Akademi.