SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Modulär aritmetik och kvadratisk reciprocitet

av

Hilding Verdezoto Barros

2026 - No L7

Modulär aritmetik och kvadratisk reciprocitet

Hilding Verdezoto Barros

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Håkan Granath

2026

Sammanfattning

I denna uppsats studeras grundläggande begrepp inom modulär aritmetik, med särskilt fokus på kvadratiska rester modulo primtal. Efter att nödvändiga definitioner och begrepp introducerats presenteras Eulers kriterium och Legendre-symbolen som verktyg för att avgöra om ett heltal är en kvadratisk rest modulo ett udda primtal. Ett centralt resultat i uppsatsen är lagen om kvadratisk reciprocitet, som behandlas ingående och bevisas med hjälp av ett gruppteoretiskt resonemang enligt ett bevis av Rousseau.

I den avslutande delen behandlas problemet att beräkna kvadratrötter modulo ett primtal. För primtal med $p \equiv 3 \pmod 4$ ges en enkel, explicit formel, medan fallet $p \equiv 1 \pmod 4$ kräver mer avancerade metoder som bygger på aritmetik i en utvidgad ring. Flera exempel ges för att tydliggöra både de teoretiska resultaten och de beräkningsmässiga metoderna.

Abstract

This thesis studies fundamental concepts in modular arithmetic, with a particular focus on quadratic residues modulo a prime. After introducing the necessary definitions, Euler's criterion and the Legendre symbol are presented as tools for determining whether an integer is a quadratic residue modulo an odd prime. A central result of the thesis is the law of quadratic reciprocity, which is treated in detail and proved using a group-theoretic argument following a proof by Rousseau.

The final part addresses the problem of computing square roots modulo a prime. For primes with $p \equiv 3 \pmod 4$, a simple explicit formula is given, whereas the case $p \equiv 1 \pmod 4$ requires more advanced methods based on arithmetic in an extended ring. Several examples are provided to illustrate both the theoretical results and the computational methods.

Innehåll

1 Introduktion

Talteori är ett av de äldsta områdena inom matematiken och har sina rötter redan i antikens Grekland, där man studerade heltalens egenskaper och deras inbördes relationer. Under århundradena har området utvecklats från konkreta räkneproblem till en mer abstrakt och strukturell teori med djupa samband till andra delar av matematiken. En systematisk behandling av kongruenser och modulär aritmetik växte fram successivt och kom att spela en central roll i den moderna talteorin [2].

Ett av de mest betydelsefulla resultaten inom klassisk talteori är lagen om kvadratisk reciprocitet. Satsen beskriver sambandet mellan om ett heltal är en kvadratisk rest modulo två olika udda primtal. Euler formulerade lagen redan på 1700-talet men utan ett fullständigt bevis, och Legendre publicerade senare ett bevis som visade sig innehålla brister. Den första korrekta bevisningen gavs av Carl Friedrich Gauss, som betraktade satsen som en av sina viktigaste inom talteori och kallade den sitt aureum theorema, den gyllene satsen [7].

Utöver sin teoretiska betydelse har modulär aritmetik och resultat inom klassisk talteori även fått stor praktisk relevans. Talteori har visat sig vara central vid konstruktionen av moderna krypteringssystem, där aritmetik modulo stora primtal spelar en avgörande roll. Metoder för att avgöra och beräkna kvadratiska rester, såsom de som behandlas i denna uppsats, kan därmed ses som viktiga byggstenar i både teoretiska och tillämpade sammanhang [2].

1.1 Uppsatsens struktur

Denna uppsats behandlar centrala begrepp och metoder inom modulär aritmetik med särskilt fokus på kvadratiska kongruenser modulo primtal. Framställningen inleds med en genomgång av linjära kongruenser och villkor för deras lösbarhet, där Bézouts identitet och den utökade Euklides algoritm introduceras som grundläggande verktyg. Dessa resultat vidareutvecklas genom den kinesiska restsatsen, som möjliggör lösning av system av kongruenser och spelar en viktig roll i den fortsatta utvecklingen.

Därefter behandlas effektiva metoder för beräkning av potenser modulo ett heltal, vilket leder till studiet av den multiplikativa gruppens struktur modulo ett primtal. Särskild vikt läggs vid att visa att denna grupp är cyklisk och att primitiva rötter existerar för varje primtal, vilket ger en algebraisk grund för den fortsatta analysen av kvadratiska kongruenser.

Uppsatsens huvuddel ägnas åt kvadratiska kongruenser och frågan om när ett heltal är en kvadrat modulo ett primtal. Genom införandet av Legendre-symbolen och dess multiplikativa egenskaper erhålls ett effektivt verktyg för att sammanfatta

och analysera denna problematik. Vidare presenteras Eulers kriterium, som ger ett praktiskt test för att avgöra om ett tal är ett kvadratiskt resttal utan att explicit behöva bestämma någon kvadratrotslösning.

Ett centralt resultat i uppsatsen är lagen om kvadratisk reciprocitet, som etablerar ett djupt samband mellan kvadratiska rester modulo olika primtal. Lagen presenteras tillsammans med ett gruppteoretiskt bevis, vilket illustrerar hur flera av uppsatsens tidigare begrepp och metoder samverkar i ett och samma resonemang.

Avslutningsvis behandlas algoritmer för att beräkna kvadraträtter modulo ett primtal. För primtal som uppfyller $p \equiv 3 \pmod 4$ erhålls en enkel explicit formel, medan fallet $p \equiv 1 \pmod 4$ kräver mer avancerade metoder baserade på aritmetik i en utvidgad ring. Dessa algoritmer visar hur de teoretiska resultaten kan omsättas i praktiska beräkningar.

2 Linjära kongruenser

Ett av de mest grundläggande problemen i modulär aritmetik är att lösa ekvationer av typen

$$ax \equiv b \pmod{n}.$$

En sådan ekvation kallas en *linjär kongruens*. En linjär kongruens har en lösning om och endast om den största gemensamma delaren $\mathrm{SGD}(a, n)$ av a och n delar b. I det speciella fallet då $\mathrm{SGD}(a, n) = 1$ existerar alltid en unik lösning modulo n. I dessa fall kan lösningen bestämmas med hjälp av den utökade euklidiska algoritmen. En metod som beräknar heltal u och v sådana att $au+nv = \mathrm{SGD}(a, n)$ och därigenom ger den modulära inversen av a.

I det här avsnittet kommer vi först att presentera metoden för att lösa en enskild linjär kongruens. Därefter går vi vidare till den kinesiska restsatsen, som behandlar lösningen av system av kongruenser och därmed generaliserar resonemanget till flera samtidiga ekvationer.

2.1 Lösning av en linjär kongruens

För att lösa

$$ax \equiv b \pmod{n},$$

är den centrala frågan om en lösning existerar och, i så fall, hur många lösningar som finns.

Innan vi besvarar detta behöver vi ett grundläggande resultat från talteorin.

Sats 2.1 (Bézouts identitet)**.** *[1]*

För heltal a och b finns det enligt Bézouts identitet alltid heltal u och v sådana att

$$au + bv = \mathrm{SGD}(a, b).$$

Beviset av Bézouts identitet återges inte här. Ett bevis finns i [1], där satsen behandlas mer utförligt.

Bézouts identitet visar att $\mathrm{SGD}(a, b)$ kan skrivas som en linjärkombination $au+bv$ för vissa heltal u och v.

I vårt sammanhang är detta viktigt eftersom vi ofta arbetar med kongruenser av typen

$$ax \equiv 1 \pmod{n}.$$

Om a och n är relativt prima, det vill säga $\text{SGD}(a, n) = 1$, så säger Bézouts identitet (sats 2.1) att det finns heltal u och v som uppfyller

$$au + nv = 1.$$

Reducerar vi likheten modulo n försvinner termen nv, eftersom $n \mid nv$. Därmed erhålls

$$au \equiv 1 \pmod{n}.$$

Detta visar att u är den *multiplikativa inversen* av a modulo n.

Den utökade euklidiska algoritmen, som behandlas i [1], ger ett konstruktivt sätt att bestämma de heltal u och v som uppfyller Bézouts identitet. Den används därför i praktiken för att beräkna modulära inverser.

Proposition 2.2. *[6, Proposition 2.1.13]*

Om a, b heltal och $\text{SGD}(a, n) = 1$ har kongruensen

$$ax \equiv b \pmod{n}$$

en lösning x, och denna lösning är unik modulo n.

Bevis. Eftersom $\text{SGD}(a, n) = 1$ finns en multiplikativ invers u till a modulo n (sats 2.1). Genom att multiplicera kongruensen

$$ax \equiv b \pmod{n}$$

med u fås

$$x \equiv u \cdot b \pmod{n}.$$

Lösningen är därmed entydig modulo n. □

Exempel 2.3. Vi bestämmer den modulära inversen till 17 modulo 43, det vill säga vi löser kongruensen

$$17x \equiv 1 \pmod{43}.$$

Eftersom $\text{SGD}(17, 43) = 1$ garanterar Bézouts identitet (sats 2.1) att det finns heltal u och v sådana att

$$17u + 43v = 1.$$

För att bestämma dessa koefficienter tillämpar vi den utökade euklidiska algoritmen. Genom successiv division erhålls

$$43 = 2 \cdot 17 + 9, \quad 17 = 9 + 8, \quad 9 = 8 + 1, \quad 8 = 8 \cdot 1 + 0.$$

Med hjälp av bakåtsubstitution kan vi nu uttrycka 1 som en linjärkombination av 17 och 43:

$$1 = 9 - 8 = 9 - (17 - 9) = 2 \cdot 9 - 17 = 2 \cdot (43 - 2 \cdot 17) - 17 = 2 \cdot 43 - 5 \cdot 17.$$

Detta visar att $-5 \cdot 17 + 2 \cdot 43 = 1$. Om vi reducerar denna likhet modulo 43 erhåller vi

$$17 \cdot (-5) \equiv 1 \pmod{43},$$

vilket innebär att inversen till 17 modulo 43 är $-5 \equiv 38 \pmod{43}$. Lösningen till kongruensen är alltså

$$x \equiv 38 \pmod{43}.$$

En enkel kontroll visar att $17 \cdot 38 = 646 \equiv 1 \pmod{43}$.

Exempel 2.4. Betrakta kongruensen

$$12x \equiv 18 \pmod{30}.$$

Här är $\mathrm{SGD}(12, 30) = 6$. Eftersom $6 \mid 18$ existerar lösningar. Dividerar vi båda sidor med 6 erhålls den ekvivalenta kongruensen

$$2x \equiv 3 \pmod{5}.$$

Eftersom $\mathrm{SGD}(2, 5) = 1$ finns en unik lösning modulo 5. Inversen till 2 modulo 5 är 3, därmed fås

$$x \equiv 3 \cdot 3 = 9 \equiv 4 \pmod{5}.$$

Varje lösning modulo 5 ger nu 6 lösningar modulo 30:

$$x \equiv 4,\ 9,\ 14,\ 19,\ 24,\ 29 \pmod{30}.$$

Om vi i stället betraktar kongruensen

$$12x \equiv 20 \pmod{30},$$

så delar $\mathrm{SGD}(12, 30) = 6$ inte talet 20, vilket innebär att kongruensen saknar lösning. Detta visar tydligt hur villkoret $\mathrm{SGD}(a, n) \mid b$ avgör om en lösning existerar.

2.2 System av linjära kongruenser

I många problem möter vi inte en enskild kongruens, utan ett helt system:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

Frågan är nu om en lösning existerar och om den i så fall är unik. Det är här den kinesiska restsatsen kommer in.

3 Kinesiska restsatsen

I detta avsnitt formuleras och bevisas den kinesiska restsatsen i fallet med två linjära kongruenser (Sats 3.1). Därefter presenteras två metoder för att lösa system med flera kongruenser.

Sats 3.1 (Kinesiska restsatsen)**.** *[6, Theorem 2.2.2]*

Låt $a, b \in \mathbb{Z}$ *och* $m, n \in \mathbb{N}$ *med* $\mathrm{SGD}(m, n) = 1$*. Då finns ett heltal* x *sådant att*

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}.$$

Dessutom är x *unik modulo* mn*.*

Bevis. Vi visar först att en lösning existerar och därefter att den är unik modulo mn.

Eftersom $\mathrm{SGD}(m, n) = 1$ följer av Bézouts identitet (Sats 2.1) att m har en multiplikativ invers modulo n.

Låt c vara en sådan invers, så att

$$cm \equiv 1 \pmod{n}.$$

För att konstruera en lösning utgår vi från den första kongruensen $x \equiv a \pmod{m}$. Det innebär att differensen $x - a$ är delbar med m, alltså finns ett heltal t sådana att

$$x - a = tm.$$

Alltså kan varje lösning skrivas på formen

$$x = a + tm.$$

För att x även ska uppfylla den andra kongruensen sätter vi in detta uttryck i $x \equiv b \pmod{n}$ och får

$$a + tm \equiv b \pmod{n}.$$

Efter subtraktion av a erhålls

$$tm \equiv b - a \pmod{n}.$$

Multiplicerar vi båda sidor med c och använder att $cm \equiv 1 \pmod{n}$ fås

$$c \cdot (tm) \equiv c \cdot (b - a) \pmod{n}.$$

Vilket reduceras till

$$t \equiv (b - a)c \pmod{n}.$$

Detta innebär att alla lösningar t kan skrivas som

$$t = (b - a)c + kn, \quad \text{för något heltal } k.$$

Sätter vi in detta i uttrycket $x = a + tm$ får vi

$$x = a + (b - a)cm + knm.$$

Eftersom termen knm är delbar med mn påverkar den inte värdet av x modulo mn. Alla val av k ger därför samma restklass modulo mn, och det räcker att välja

$$x = a + (b - a)cm.$$

Vi visar nu att lösningen x är unik modulo mn. Antag att x_1 och x_2 båda är lösningar. Då gäller

$$x_1 \equiv a \pmod{m}, \qquad x_2 \equiv a \pmod{m},$$

och

$$x_1 \equiv b \pmod{n}, \qquad x_2 \equiv b \pmod{n}.$$

Subtraherar vi kongruenserna

$$x_1 - x_2 \equiv 0 \pmod{m}, \qquad x_1 - x_2 \equiv 0 \pmod{n}.$$

Detta innebär att $x_1 - x_2$ är delbart med både m och n. Eftersom $\text{SGD}(m, n) = 1$ följer att $x_1 - x_2$ är delbart med produkten mn, vilket innebär att

$$x_1 \equiv x_2 \pmod{mn}.$$

Alltså är lösningen unik modulo mn. □

3.1 Generaliserad metod för den kinesiska restsatsen

Denna metod utgår från Steins [6, Algorithm 2.2.3], men har utvecklats för att behandla det allmänna fallet av den kinesiska restsatsen, där flera kongruenser hanteras samtidigt.

Algoritm 1. *Låt $n_1, n_2, \ldots, n_k$ vara positiva heltal som är parvis relativt prima och $a_1, a_2, \ldots, a_k$ givna heltal. Vi vill bestämma ett heltal x som uppfyller*

$$x \equiv a_i \pmod{n_i}, \quad i = 1, 2, \ldots, k.$$

Vi börjar med den första kongruensen och sätter $x_1 = a_1$ samt $N_1 = n_1$. Antag nu att vi har en lösning x_{i-1} som uppfyller de första $i-1$ kongruenserna och att N_{i-1} är produkten av de motsvarande modulerna n_j. Vi vill finna x_i som uppfyller både

$$x_i \equiv x_{i-1} \pmod{N_{i-1}}, \qquad x_i \equiv a_i \pmod{n_i}.$$

Eftersom N_{i-1} och n_i är relativt prima finns det enligt Sats 2.1 heltal c_i och d_i sådana att

$$c_i N_{i-1} + d_i n_i = 1,$$

där c_i fungerar som den modulära inversen av N_{i-1} modulo n_i.

Alla lösningar till det första villkoret kan skrivas som

$$x_i = x_{i-1} + t_i N_{i-1}, \qquad t_i \in \mathbb{Z}.$$

För att uppfylla den nya kongruensen krävs

$$t_i \equiv (a_i - x_{i-1})\, c_i \pmod{n_i}.$$

Vi väljer ett sådant värde på t_i och definierar därefter x_i enligt ovan. Produkten av modulerna definieras rekursivt genom $N_i = N_{i-1} n_i$. Genom att upprepa denna procedur för $i = 2, \ldots, k$ erhålls slutligen $x = x_k$, som är unik modulo

$$N = n_1 n_2 \cdots n_k.$$

Bevis. För att visa att algoritmen fungerar betraktar vi hur lösningen byggs upp successivt.

Antag att vi vid steg $i-1$ redan har en heltalslösning x_{i-1} som uppfyller de första $i-1$ kongruenserna. Alla tal som är kongruenta med x_{i-1} modulo N_{i-1} kan då skrivas på formen

$$x = x_{i-1} + t\, N_{i-1}, \qquad t \in \mathbb{Z}.$$

För att även uppfylla kongruensen

$$x \equiv a_i \pmod{n_i}$$

måste vi bestämma ett värde på t som gör detta möjligt. Genom att sätta in uttrycket för x i denna kongruens får vi

$$x_{i-1} + tN_{i-1} \equiv a_i \pmod{n_i},$$

vilket efter subtraktion av x_{i-1} från båda leden ger

$$tN_{i-1} \equiv a_i - x_{i-1} \pmod{n_i}.$$

Eftersom N_{i-1} och n_i är relativt prima existerar en modulär invers c_i av N_{i-1} modulo n_i, och därmed kan t bestämmas ur kongruensen

$$t \equiv (a_i - x_{i-1})\, c_i \pmod{n_i}.$$

När detta värde på t sätts in i uttrycket för x_i får vi

$$x_i = x_{i-1} + t_i N_{i-1},$$

och därav

$$x_i \equiv x_{i-1} + (a_i - x_{i-1})\, c_i N_{i-1} \pmod{n_i}.$$

Eftersom $c_i N_{i-1} \equiv 1 \pmod{n_i}$ reduceras detta till

$$x_i \equiv a_i \pmod{n_i},$$

vilket visar att den nya lösningen uppfyller både den tidigare kongruensen och den nya.

Eftersom modulerna $n_1, \ldots, n_i$ är parvis relativt prima garanterar den kinesiska restsatsen dessutom att en sådan lösning är unik modulo produkten $N_i = n_1 n_2 \cdots n_i$. Genom att upprepa denna konstruktion för varje kongruens erhålls till slut ett tal x_k som uppfyller samtliga villkor och som är unikt modulo

$$N = n_1 n_2 \cdots n_k.$$

Detta visar att algoritmen korrekt bestämmer den lösning som den kinesiska restsatsen garanterar. □

Exempel 3.2. Betrakta systemet

$$x \equiv 3 \pmod 4, \qquad x \equiv 4 \pmod 9, \qquad x \equiv 5 \pmod{11}.$$

Vi inleder med de två första kongruenserna. Eftersom varje tal av formen

$$x = 3 + 4t, \qquad t \in \mathbb{Z},$$

uppfyller villkoret $x \equiv 3 \pmod 4$, bestämmer vi nu t så att även den andra kongruensen $x \equiv 4 \pmod 9$ är uppfylld. Insättning ger

$$3 + 4t \equiv 4 \pmod 9 \quad \Longleftrightarrow \quad 4t \equiv 1 \pmod 9.$$

För att lösa denna kongruens bestämmer vi den modulära inversen av 4 modulo 9. Den euklidiska algoritmen ger att

$$1 = 9 - 2 \cdot 4,$$

vilket visar att inversen till 4 modulo 9 är $-2 \equiv 7 \pmod 9$. Därmed erhålls

$$t \equiv 7 \pmod 9.$$

Väljer vi $t = 7$ fås

$$x = 3 + 4 \cdot 7 = 31,$$

vilket innebär att

$$x \equiv 31 \pmod{36}.$$

Denna lösning kombineras nu med den tredje kongruensen $x \equiv 5 \pmod{11}$. Alla tal av formen

$$x = 31 + 36t$$

uppfyller de två första kongruenserna. Vi bestämmer därför t så att även den tredje kongruensen uppfylls. Insättning ger

$$31 + 36t \equiv 5 \pmod{11} \quad \Longleftrightarrow \quad 36t \equiv -26 \equiv 7 \pmod{11}.$$

Eftersom $36 \equiv 3 \pmod{11}$ reduceras detta till

$$3t \equiv 7 \pmod{11}.$$

För att lösa denna kongruens bestämmer vi inversen av 3 modulo 11. En beräkning ger

$$1 = 4 \cdot 3 - 11,$$

vilket innebär att inversen är 4. Därmed fås

$$t \equiv 7 \cdot 4 \equiv 6 \pmod{11}.$$

Med $t = 6$ erhålls slutligen

$$x = 31 + 36 \cdot 6 = 247,$$

vilket innebär att

$$x \equiv 247 \pmod{396}.$$

Kontroll:

$$247 \equiv 3 \pmod{4}, \qquad 247 \equiv 4 \pmod{9}, \qquad 247 \equiv 5 \pmod{11}.$$

Samtliga kongruenser är alltså uppfyllda.

3.2 En alternativ metod för lösning av kongruenssystem

Vi presenterar nu en alternativ metod för att lösa system av kongruenser. Metoden bygger på en explicit formel för lösningen och följer framställningen i [4]. Till skillnad från den föregående algoritmen konstrueras lösningen här direkt genom en summa av särskilt valda termer.

Sats 3.3. *[4, Theorem 1]*

Låt $n_1, n_2, \ldots, n_k$ vara positiva heltal som är parvis relativt prima, och låt $a_1, a_2, \ldots, a_k$ vara heltal. Sätt

$$N = n_1 n_2 \cdots n_k.$$

För varje i definiera $N_i = N/n_i$, och välj ett heltal M_i sådant att

$$N_i M_i \equiv 1 \pmod{n_i}.$$

Då ger uttrycket

$$x = a_1 N_1 M_1 + a_2 N_2 M_2 + \cdots + a_k N_k M_k \tag{3.4}$$

en lösning till systemet

$$x \equiv a_i \pmod{n_i}, \quad \text{för } i = 1, 2, \ldots, k.$$

Dessutom är lösningen unik modulo N.

Följande bevis bygger på Radcliffes framställning i [4], men har här utvecklats och förklarats mer utförligt för ökad tydlighet.

Bevis. Vi visar att uttrycket i (3.4) verkligen definierar ett heltal som uppfyller samtliga kongruenser och att denna lösning är unik modulo N.

Låt N och N_i vara definierade som i satsen 3.3.

För varje i gäller att N_i är produkten av alla moduler utom n_i. Eftersom n_i är relativt primt med de övriga modulerna följer att $\text{SGD}(N_i, n_i) = 1$. Det finns därför ett heltal M_i som uppfyller

$$N_i M_i \equiv 1 \pmod{n_i}.$$

Idén bakom metoden är att konstruera lösningen som en summa av flera termer, där varje term bidrar till exakt en kongruens och samtidigt inte påverkar de övriga.

För varje i vill vi därför konstruera ett tal som uppfyller

$$x_i \equiv a_i \pmod{n_i} \quad \text{och} \quad x_i \equiv 0 \pmod{n_j} \text{ för alla } j \neq i.$$

Om vi lyckas skapa ett sådant x_i för varje i kan vi addera dessa tal och på så sätt erhålla en lösning till hela systemet.

Vi börjar med att observera att N_i är delbart med varje n_j där $j \neq i$, vilket ger

$$N_i \equiv 0 \pmod{n_j} \quad \text{för alla } j \neq i.$$

Samtidigt är N_i inte nödvändigtvis kongruent med 1 modulo n_i. Genom att multiplicera med M_i som är den modulära inversen av N_i modulo n_i, erhåller vi

$$N_i M_i \equiv 1 \pmod{n_i}.$$

Talet $N_i M_i$ uppfyller därmed

$$N_i M_i \equiv 1 \pmod{n_i} \quad \text{och} \quad N_i M_i \equiv 0 \pmod{n_j} \text{ för alla } j \neq i.$$

Om vi dessutom multiplicerar detta med a_i får vi

$$a_i N_i M_i \equiv a_i \pmod{n_i}, \quad a_i N_i M_i \equiv 0 \pmod{n_j} \text{ för alla } j \neq i.$$

Termen $a_i N_i M_i$ bidrar alltså endast till den i :te kongruensen.

Genom att summera alla dessa termer erhåller vi därmed uttrycket i (3.4).

När detta uttryck reduceras modulo n_i försvinner alla termer utom $a_i N_i M_i$, vilket ger

$$x \equiv a_i N_i M_i \equiv a_i \pmod{n_i}.$$

Alltså uppfyller x samtliga kongruenser i systemet.

För unikheten hänvisar vi till Sats 3.1, där det visades att lösningen till ett sådant system är unik modulo produkten av modulerna.

□

Exempel 3.5. Vi betraktar samma exempel 3.2, men löser det nu med metod 2.

$$x \equiv 3 \pmod{4}, \qquad x \equiv 4 \pmod{9}, \qquad x \equiv 5 \pmod{11}.$$

Vi börjar med att beräkna produkten av modulerna:

$$N = 4 \cdot 9 \cdot 11 = 396.$$

Därefter bestämmer vi

$$N_1 = \frac{N}{4} = 99, \qquad N_2 = \frac{N}{9} = 44, \qquad N_3 = \frac{N}{11} = 36.$$

Eftersom $\mathrm{SGD}(N_i, n_i) = 1$ för varje i finns heltal M_i sådana att

$$N_i M_i \equiv 1 \pmod{n_i}.$$

Vi reducerar först N_i modulo respektive n_i och får

$$N_1 = 99 \equiv 3 \pmod{4}, \qquad N_2 = 44 \equiv 8 \pmod{9}, \qquad N_3 = 36 \equiv 3 \pmod{11}.$$

Vi bestämmer de modulära inverserna och får:

$$3^{-1} \equiv 3 \pmod{4}, \qquad 8^{-1} \equiv 8 \pmod{9}, \qquad 3^{-1} \equiv 4 \pmod{11},$$

alltså får vi

$$M_1 = 3, \qquad M_2 = 8, \qquad M_3 = 4.$$

Lösningen kan nu konstrueras som

$$x = a_1 N_1 M_1 + a_2 N_2 M_2 + a_3 N_3 M_3 = 3 \cdot 99 \cdot 3 + 4 \cdot 44 \cdot 8 + 5 \cdot 36 \cdot 4 = 3019.$$

Reducerar vi detta modulo N erhålls

$$x \equiv 3019 \equiv 247 \pmod{396}.$$

Som visades i Exemplet 3.2 uppfyller denna lösning samtliga kongruenser.

4 Beräkning av potenser modulo n

4.1 Effektiv exponentiering

En effektiv metod för att beräkna potenser modulo ett heltal n är att genomföra upprepad kvadrering, som presenteras och analyseras i [6, §2.3.2].

När man arbetar med modulär aritmetik måste man ofta beräkna uttryck av typen

$$a^m \pmod{n}.$$

Om exponenten m är stor blir en direkt beräkning opraktisk eftersom antalet multiplikationer växer snabbt. Därför finns en effektiv metod som stegvis förenklar beräkningen genom att upprepade gånger dela exponenten med 2 och samtidigt kvadrera basen. Efter varje steg reduceras resultatet modulo n, vilket gör att talen aldrig blir alltför stora.

Ett heltal m kan skrivas i binär form som

$$m = \varepsilon_0 2^0 + \varepsilon_1 2^1 + \cdots + \varepsilon_r 2^r,$$

där varje $\varepsilon_i \in \{0, 1\}$. Enligt potenslagarna gäller då

$$a^m = a^{\varepsilon_0 2^0} \cdot a^{\varepsilon_1 2^1} \cdots a^{\varepsilon_r 2^r}.$$

Det innebär att man endast behöver multiplicera de potenser a^{2^i} där den binära siffran $\varepsilon_i = 1$. För att få dessa potenser kvadrerar man a upprepade gånger, och tar resten modulo n efter varje steg.

Metoden steg för steg.

1. Skriv exponenten m i binär form.
2. Beräkna a^{2^i} mod n genom upprepad kvadrering. Det betyder att varje nytt värde fås genom att kvadrera det föregående:

$$a^{2^{i+1}} = a^{2^i \cdot 2} = (a^{2^i})^2 \pmod{n}.$$

3. Multiplicera ihop de potenser som motsvarar binära siffror med värdet 1 i representationen av m.
4. Reducera modulo n efter varje multiplikation.

Exempel 4.1 (Beräkna 17^{87} mod 33). Vi börjar med att skriva exponenten i binär form. Eftersom

$$87 = 2^6 + 2^4 + 2^2 + 2^1 + 2^0 = 1010111_2,$$

vet vi att de potenser som motsvarar ettor i binärrepresentationen kommer att ingå i produkten.

Därefter beräknas de successiva kvadreringarna av basen modulo 33. Utgående från $17^{2^0} \equiv 17$ erhålls:

Potens	Beräkning	Rest mod 33
17^{2^0}	17	17
17^{2^1}	$17^2 = 289$	25
17^{2^2}	$25^2 = 625$	31
17^{2^3}	$31^2 = 961$	4
17^{2^4}	$4^2 = 16$	16
17^{2^5}	$16^2 = 256$	25
17^{2^6}	$25^2 = 625$	31

Eftersom exponentens binärsiffror är ettor på positionerna $2^6, 2^4, 2^2, 2^1$ och 2^0, multipliceras motsvarande värden ihop modulo 33:

$$r = 31 \cdot 16 \cdot 31 \cdot 25 \cdot 17 \pmod{33}.$$

Genom successiva modulära multiplikationer fås

$$31 \cdot 16 \equiv 1, \qquad 1 \cdot 31 \equiv 31, \qquad 31 \cdot 25 \equiv 16, \qquad 16 \cdot 17 \equiv 8 \pmod{33}.$$

Vi får alltså slutligen

$$17^{87} \equiv 8 \pmod{33}.$$

Metoden kan tolkas så att varje gång exponenten halveras ($m \to m/2$) motsvarar det att vi går till nästa binära siffra. När en binär siffra är 1 multipliceras basen in i resultatet. Genom att hela tiden ta resten modulo n undviker man att talen växer snabbt.

Algoritmen utför en kvadrering för varje binär siffra i exponenten och, om siffran är 1, dessutom en multiplikation. Antalet operationer växer därför ungefär proportionellt mot $\log_2(m)$. Ett tal med r binära siffror kräver alltså r kvadreringar, där

$$r = \lfloor \log_2(m) \rfloor + 1.$$

I vårt exempel har $m = 87$ binärformen 1010111_2, som består av sju siffror. Det innebär att endast 7 kvadreringar krävs även upp till 7 multiplikationer, jämfört med 86 multiplikationer vid en direkt beräkning av 17^{87}. Metoden har därför tidskomplexitet $O(\log_2 m)$ och är mycket effektiv även för stora exponenter.

4.2 Primitiva rötter

När vi nu vet hur man effektivt beräknar potenser modulo n, kan vi undersöka vilka mönster som uppstår när modulen är ett primtal. Detta leder till begreppet *primitiva rötter*.

Proposition 4.2. *[6, Proposition 2.5.5] Låt p vara ett primtal och låt d vara en delare av $p-1$. Då har ekvationen*

$$x^d \equiv 1 \pmod{p}$$

exakt d lösningar i $(\mathbb{Z}/p\mathbb{Z})^\times$.

Lemma 4.3. *[6, Lemma 2.5.7] Om två element $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ har ordningarna r respektive s, och $\mathrm{SGD}(r,s) = 1$, så har produkten ab ordning rs.*

Bevisen för båda Proposition 4.2 och Lemma 4.3 återfinns i [6].

Sats 4.4 (Primitiva rötter)**.** *[6, Theorem 2.5.8] För varje primtal p finns ett heltal g som är en* primitiv rot modulo p*. Det innebär att den multiplikativa gruppen*

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\}$$

är cyklisk, det vill säga att varje element kan skrivas som en potens av g modulo p:

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{g^1, g^2, \ldots, g^{p-1}\} \pmod{p}.$$

Bevis. Fallet $p = 2$ är trivialt, eftersom 1 är en primitiv rot modulo 2. Vi antar därför härefter att $p > 2$.

Skriv $p-1$ som en produkt av primpotenser

$$p - 1 = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r},$$

där $q_1, \ldots, q_r$ är distinkta primtal.

För varje $i = 1, \ldots, r$ betraktar vi kongruensen

$$x^{q_i^{n_i - 1}} \equiv 1 \pmod{p}.$$

Enligt Proposition 4.2 har denna kongruens exakt $q_i^{n_i-1}$ lösningar i $(\mathbb{Z}/p\mathbb{Z})^\times$, medan kongruensen

$$x^{q_i^{n_i}} \equiv 1 \pmod{p}$$

har exakt $q_i^{n_i}$ lösningar. Eftersom varje lösning till den första kongruensen även är en lösning till den andra, men inte omvänt, följer att antalet element med ordning exakt $q_i^{n_i}$ är

$$q_i^{n_i} - q_i^{n_i - 1} = q_i^{n_i - 1}(q_i - 1).$$

Välj ett sådant element och beteckna det a_i.

Observera att varje a_i har ordning $q_i^{n_i}$ och att dessa ordningar är parvis relativt prima. Enligt Lemma 4.3 har då produkten av dessa element en ordning som är lika med produkten av ordningarna. Alltså har

$$g = a_1 a_2 \cdots a_r$$

ordning

$$\operatorname{ord}(g) = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r} = p - 1.$$

Därmed är g en primitiv rot modulo p. □

Exempel 4.5 (Primitiv rot modulo 11). Vi bestämmer en primitiv rot modulo 11. Eftersom 11 är ett primtal har varje element i $(\mathbb{Z}/11\mathbb{Z})^\times$ en ordning som delar

$$p - 1 = 10 = 2 \cdot 5.$$

Enligt Proposition 4.2 finns exakt två lösningar till $x^2 \equiv 1 \pmod{11}$ och fem lösningar till $x^5 \equiv 1 \pmod{11}$. För att identifiera dessa beräknar vi potenserna modulo 11:

Tabell 1: Värden av x^2 och x^5 modulo 11

x	$x^2 \bmod 11$	$x^5 \bmod 11$
1	1	1
2	4	10
3	9	1
4	5	1
5	3	1
6	3	10
7	5	10
8	9	10
9	4	1
10	1	10

Här ser vi att lösningarna till $x^2 \equiv 1$ är $\{1, 10\}$. Eftersom ordningen måste vara större än 1 följer att

10 har ordning 2.

Vidare gäller $x^5 \equiv 1$ för $\{1, 3, 4, 5, 9\}$. För elementet 3 fås

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv 5, \quad 3^4 \equiv 4, \quad 3^5 \equiv 1,$$

och därmed har

$$3 \text{ ordning } 5.$$

Enligt Lemma 4.3 ger produkten av två element med ordning 2 respektive 5 ett element av ordning 10. Vi får alltså

$$g = 10 \cdot 3 = 30 \equiv 8 \pmod{11}.$$

Genom att beräkna potenserna av 8 erhålls

$$8^1 \equiv 8,\ 8^2 \equiv 9,\ 8^3 \equiv 6,\ 8^4 \equiv 4,\ 8^5 \equiv 10,\ 8^6 \equiv 3,\ 8^7 \equiv 2,\ 8^8 \equiv 5,\ 8^9 \equiv 7,\ 8^{10} \equiv 1 \pmod{11}.$$

Eftersom 1 först uppträder vid exponent 10 har 8 ordning 10, och är alltså en primitiv rot modulo 11.

Man kan även direkt ur tabell 1 se vilka element som är primitiva rötter. De som varken uppfyller $x^2 \equiv 1$ eller $x^5 \equiv 1$ måste ha ordning 10. Därför är de fyra primitiva rötterna modulo 11

$$2, 6, 7, 8.$$

5 Kvadratiska ekvationer i modulär aritmetik

I detta avsnitt studeras kongruenser av typen

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

där p är ett primtal. Framställningen bygger huvudsakligen på [6].

Till skillnad från linjära kongruenser är det för kvadratiska kongruenser inte givet att en lösning existerar. Den centrala frågan är därför när det finns ett heltal x som uppfyller

$$x^2 \equiv a \pmod{p}.$$

För att kunna besvara denna fråga inför vi begreppet kvadratiskt resttal och utvecklar verktyg såsom Eulers kriterium och Legendre-symbolen, vilka leder fram till lagen om kvadratisk reciprocitet, ofta kallad den gyllene satsen inom klassisk talteori.

5.1 Definition av kvadratiska rester

Ett heltal a, där $\text{SGD}(a, p) = 1$, kallas ett *kvadratiskt resttal modulo p* om det finns ett heltal x sådant att

$$x^2 \equiv a \pmod{p}.$$

Om inget sådant x finns, kallas a ett *icke-resttal modulo p*.

Att avgöra om ett tal är en kvadrat modulo p är kärnan i studiet av kvadratiska kongruenser [6, Definition 4.1.1, s.70].

Exempel 5.1 (Kvadratiska rester modulo 11). För att illustrera begreppet kvadratiska rester undersöker vi alla möjliga kvadrater modulo $p = 11$.

Vi beräknar $x^2 \pmod{11}$ för alla $x = 1, 2, \ldots, 10$:

x	1	2	3	4	5	6	7	8	9	10
$x^2 \bmod 11$	1	4	9	5	3	3	5	9	4	1

De olika kvadratiska resterna modulo 11 är alltså

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

och de tal som inte förekommer i tabellen är icke-rester:

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

Metoden ovan fungerar väl för små primtal men blir snabbt ineffektiv för större värden på p. För att sammanfatta denna information på ett mer kompakt och kraftfullt sätt inför vi nu Legendre-symbolen.

5.2 Legendre-symbolen

För ett primtal p och ett heltal a definieras Legendre-symbolen enligt [6, Definition 4.1.2, s. 70]:

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

Legendre-symbolen ger alltså ett snabbt sätt att avgöra om ett heltal är en kvadrat modulo p.

Om vi återvänder till exempel 5.1 kan informationen nu uttryckas mer kompakt:

$$\left(\frac{a}{11}\right) = \begin{cases} 1 & \text{om } a \in \{1, 3, 4, 5, 9\}, \\ -1 & \text{om } a \in \{2, 6, 7, 8, 10\}. \end{cases}$$

Multiplikativitet hos Legendre-symbolen. En av de viktigaste egenskaperna hos Legendre-symbolen är dess goda samspel med multiplikation. I [6, s. 71] beskrivs symbolen som en surjektiv grupphomomorfism

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{1, -1\}.$$

Detta innebär att Legendre-symbolen bevarar multiplikation på samma sätt som gruppoperationen i $(\mathbb{Z}/p\mathbb{Z})^\times$. Mer konkret betyder detta att om vi multiplicerar två tal innan vi beräknar deras Legendre-symbol, får vi samma resultat som om vi först beräknar symbolerna var för sig och därefter multiplicerar dessa.

Lemma 5.2. *[6, Lemma 4.1.4] Låt p vara ett udda primtal. Avbildningen*

$$\psi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, \qquad \psi(a) = \left(\frac{a}{p}\right),$$

är en surjektiv grupphomomorfism.

Som en direkt följd gäller för alla $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ att

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

Bevis. Enligt sats 4.4 är den multiplikativa gruppen $(\mathbb{Z}/p\mathbb{Z})^\times$ cyklisk. Det finns alltså en primitiv rot g modulo p, sådan att varje element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ kan skrivas som

$$a \equiv g^k \pmod{p}$$

för något heltal k.

Ett sådant element är en kvadratisk rest modulo p om och endast om exponenten k är jämn. Om $k = 2m$ för något heltal m gäller nämligen

$$g^k = g^{2m} \equiv (g^m)^2 \pmod{p},$$

så att g^k är en kvadrat modulo p. Omvänt kan varje kvadrat modulo p skrivas på formen $(g^m)^2 \equiv g^{2m}$, vilket innebär att exponenten måste vara jämn. Detta innebär att Legendre-symbolen uppfyller

$$\left(\frac{g^k}{p}\right) = (-1)^k.$$

Om $a \equiv g^k$ och $b \equiv g^m$, följer då

$$ab \equiv g^{k+m} \pmod{p},$$

och därmed

$$\left(\frac{ab}{p}\right) = (-1)^{k+m} = (-1)^k(-1)^m = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Alltså är Legendre-symbolen multiplikativ. Surjektiviteten är uppenbar, eftersom både jämna och udda exponenter förekommer. □

5.3 Eulers kriterium

Ett elegant sätt att avgöra om ett tal a är ett kvadratiskt resttal modulo p ges av Eulers kriterium. Denna sats knyter samman potensegenskaper i kroppen $\mathbb{Z}/p\mathbb{Z}$ med Legendre-symbolens värde, och utgör därför en central länk mellan aritmetiska och algebraiska perspektiv på kvadratiska rester.

Proposition 5.3. *[6, Proposition 2.5.3]*

Låt p vara ett primtal och låt $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ vara ett polynom av grad n. Då har $f(x)$ högst n olika rötter i $(\mathbb{Z}/p\mathbb{Z})$.

Denna proposition används för att garantera att polynomet $x^2 - a$ modulo ett primtal p inte kan ha fler än två rötter. Detta faktum kommer senare att vara avgörande när vi kopplar kvadratiska rester till potensegenskaper, särskilt i beviset av Eulers kriterium.

Proposition 5.4 (Eulers kriterium)**.** *[6, Proposition 4.2.1]*

Låt p vara ett udda primtal och låt $\mathrm{SGD}(a, p) = 1$*. Då gäller*

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

Som en omedelbar konsekvens av Eulers kriterium gäller:

- *Om $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, är a ett kvadratiskt resttal.*
- *Om $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, är a ett icke-resttal.*

Beviset för Proposition 5.3 återges inte här utan återfinns i Stein [6]. Följande bevis av Proposition 5.4 bygger på framställningen i Stein [6], men presenteras här i något mer utförligt form.

Bevis. Enligt Lemma 5.2 är Legendre-symbolen en surjektiv grupphomomorfism

$$\psi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}.$$

Definiera vidare avbildningen

$$\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times, \qquad \varphi(a) = a^{(p-1)/2}.$$

Eftersom exponentiering bevarar multiplikation är även φ en grupphomomorfism.

Notera att

$$\ker(\psi) = \{a \in (\mathbb{Z}/p\mathbb{Z})^\times : \psi(a) = 1\}$$

är mängden av kvadratiska rester modulo p.

Om $a \in \ker(\psi)$ finns ett element b sådant att $a = b^2$. Då gäller

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

Eftersom $(\mathbb{Z}/p\mathbb{Z})^\times$ är en grupp av ordning $p-1$ följer att

$$b^{p-1} = 1.$$

Alltså $\varphi(a) = 1$, och vi får

$$\ker(\psi) \subseteq \ker(\varphi).$$

Eftersom Lemma 5.2 visar att ψ är en surjektiv grupphomomorfism har dess kärna index 2 i $(\mathbb{Z}/p\mathbb{Z})^\times$. Detta innebär att precis hälften av elementen i gruppen är kvadratiska rester, och därmed

$$|\ker(\psi)| = (p-1)/2.$$

Detta ger då endast två möjligheter för $\ker(\varphi)$. Antingen $\ker(\varphi) = \ker(\psi)$ eller φ är trivial (dvs $\varphi(a) = 1$, för alla a).

Antag att φ vore trivial. Då skulle polynomet

$$f(x) = x^{(p-1)/2} - 1$$

ha alla $p-1$ element i $(\mathbb{Z}/p\mathbb{Z})^\times$ som rötter, vilket strider mot Proposition 5.3, eftersom ett polynom av grad $(p-1)/2$ högst kan ha $(p-1)/2$ rötter. Alltså kan φ inte vara trivial, och vi måste ha

$$\ker(\varphi) = \ker(\psi).$$

Därmed gäller för alla $a \in (\mathbb{Z}/p\mathbb{Z})^\times$

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

Eftersom båda sidor endast kan anta värdena ± 1 följer Eulers kriterium. □

Eulers kriterium används inte för att hitta den faktiska lösningen till en kvadratisk kongruens. Det fungerar istället som ett effektivt test för att avgöra om en lösning existerar. Med andra ord avgör kriteriet om ett tal a är ett kvadratiskt resttal modulo p.

Exempel 5.5 (Kvadratiska rester modulo 11). Vi återvänder till modulen $p = 11$ från exempel 5.1. Denna gång använder vi Eulers kriterium istället för att beräkna alla kvadrater direkt.

Enligt Eulers kriterium gäller

$$\left(\frac{a}{11}\right) \equiv a^{\frac{11-1}{2}} = a^5 \pmod{11}.$$

Exempelberäkningar:

- För $a = 3$:
$$3^5 = 243 \equiv 1 \pmod{11}.$$
Alltså är $\left(\frac{3}{11}\right) = 1$, vilket betyder att 3 är ett kvadratiskt resttal modulo 11.
- För $a = 2$:
$$2^5 = 32 \equiv 10 \equiv -1 \pmod{11}.$$
Här får vi $\left(\frac{2}{11}\right) = -1$, vilket betyder att 2 är ett icke-resttal.
- För $a = 7$:
$$7^5 = 16807 \equiv 10 \equiv -1 \pmod{11}.$$
Alltså gäller $\left(\frac{7}{11}\right) = -1$, och 7 är ett icke-resttal modulo 11.

Med hjälp av Eulers kriterium kan vi alltså snabbt avgöra om ett tal är en kvadratisk rest, utan att behöva testa alla möjliga kvadrater. Detta illustrerar hur teorin från de föregående avsnitten kan tillämpas på ett effektivt och praktiskt sätt.

5.4 Lagen om Kvadratisk reciprocitet

Efter att ha definierat Legendre-symbolen och etablerat dess multiplikativa egenskaper kan vi nu formulera ett av talteorins mest centrala resultat: lagen om kvadratisk reciprocitet. Denna lag beskriver hur kvadratiska rester modulo två olika primtal hänger samman och gör det möjligt att ”byta plats” på täljare och nämnare i Legendre-symbolen.

Sats 5.6 (Gauss lag om kvadratisk reciprocitet)**.** *[6, Theorem 4.1.7] Låt p och q vara två olika udda primtal. Då gäller*

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

Beviset ges i avsnitt 5.5. Sats (5.6) gör det möjligt att byta plats på p och q i Legendre-symbolen. Formeln är enkel till sin form men mycket djup i sitt innehåll, eftersom den knyter samman kvadratiska rester modulo p och modulo q.

Ett särskilt viktigt komplement till kvadratisk reciprocitet är fallet då övre talet är 2.

Proposition 5.7. *Låt p vara ett udda primtal. Då gäller*

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

Proposition 5.7 anger exakt när 2 är en kvadratisk rest modulo ett udda primtal.

Beviset av Proposition 5.7 kan ges med hjälp av Gauss lemma. Idén är att lemmat gör det möjligt att bestämma värdet av Legendre-symbolen, genom att titta på om vissa reducerade produkter blir positiva eller negativa. Själva härledningen för fallet $a = 2$ kräver dock en mer detaljerad analys av dessa produkter, och vi går därför inte igenom beviset här. (Gauss Lemma och dess fullständiga bevis finns framställt i Stein ([6, sid. 76-80]).

Exempel 5.8. Vi vill beräkna Legendre-symbolen

$$\left(\frac{-79}{101}\right).$$

Eftersom värdet endast beror på täljaren modulo nämnaren reducerar vi först

$$-79 \equiv 22 \pmod{101}$$

vilket ger

$$\left(\frac{-79}{101}\right) = \left(\frac{22}{101}\right).$$

Faktoriseringen $22 = 2 \cdot 11$ och multiplikativiteten (lemma 5.2) ger

$$\left(\frac{22}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{11}{101}\right).$$

Eftersom $101 \equiv 5 \pmod 8$ följer av 5.7 att

$$\left(\frac{2}{101}\right) = -1.$$

För den andra faktorn använder vi sats 5.6. Vi får

$$\left(\frac{11}{101}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{101-1}{2}}\left(\frac{101}{11}\right). \tag{5.9}$$

Eftersom exponenten är jämn ger (5.9) att

$$\left(\frac{11}{101}\right) = \left(\frac{101}{11}\right).$$

Vidare gäller $101 \equiv 2 \pmod{11}$, och således

$$\left(\frac{11}{101}\right) = \left(\frac{2}{11}\right).$$

Eftersom $11 \equiv 3 \pmod{8}$ ger 5.7 att

$$\left(\frac{2}{11}\right) = -1.$$

Vi kan nu samla beräkningen:

$$\left(\frac{-79}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{11}{101}\right) = (-1)(-1) = 1.$$

Detta visar att -79 är ett kvadratiskt resttal modulo 101.

5.5 Rousseaus bevis av kvadratisk reciprocitet

Det finns många olika bevis av lagen om kvadratisk reciprocitet, med varierande grad av algebraisk och analytisk komplexitet. I detta avsnitt presenterar vi ett bevis av G. Rousseau från 1991 [5]. Detta bevis har valts eftersom det bygger på elementära gruppteoretiska resonemang och den kinesiska restsatsen, utan att använda mer tekniska hjälpresultat såsom Gauss lemma.

Bevisidén är att betrakta en viss grupp som konstrueras utifrån primtalen p och q, multiplicera samtliga element i denna grupp och sedan beräkna produkten på två olika sätt. Genom att jämföra resultaten erhålls lagen om kvadratisk reciprocitet som en omedelbar konsekvens.

I den följande framställningen har beviset utvecklats med utförliga mellanled för att tydliggöra resonemanget, eftersom originalbeviset i [5] är mycket kortfattat.

För att kunna jämföra produkterna i Rousseaus bevis kommer vi att behöva värdet av fakulteten modulo ett primtal. Detta ges av Wilsons sats:

Sats 5.10. *[3, sats 9.6] Om p är ett primtal gäller*

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

Wilsons sats kommer att användas senare i beviset för att förenkla vissa fakulteter modulo primtal.

Vi kan nu gå vidare till Rousseaus bevis av lagen om kvadratisk reciprocitet.

Bevis. Låt p och q vara två olika udda primtal. Vi betraktar grupperna

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}, \qquad \mathbb{Z}_q^* = \{1, 2, \ldots, q-1\},$$

med multiplikation modulo p respektive modulo q. Deras direkta produkt $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ består av alla par (a, b) där a räknas modulo p och b modulo q.

I denna grupp inför Rousseau delgruppen

$$U = \{(1, 1), (-1, -1)\},$$

och bildar kvotgruppen

$$G = (\mathbb{Z}_p^* \times \mathbb{Z}_q^*)/U.$$

Eftersom (a, b) och $(-a, -b)$ identifieras i kvotgruppen, och inga element i $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ är sina egna negationer (det vill säga, $(a, b) = (-a, -b)$ skulle innebära $2a \equiv 0 \pmod{p}$ och $2b \equiv 0 \pmod{q}$, vilket är omöjligt då p och q är udda primtal), består G av

$$\frac{(p-1)(q-1)}{2}$$

element.

Låt n beteckna produkten av alla element i G. Vi börjar med att beräkna n genom att välja representanter för varje ekvivalensklass. Vi låter den första koordinaten anta alla värden $i = 1, 2, \ldots, p-1$, medan den andra koordinaten endast varierar över $j = 1, 2, \ldots, (q-1)/2$. Detta ger ett system av representanter, eftersom operationen $(a, b) \mapsto (-a, -b)$ redan har identifierats i kvotgruppen.

Genom detta val erhåller vi exakt ett element från varje ekvivalensklass i G, och därmed ingår varje element i produkten n precis en gång. Vi definierar därför mängden

$$S = \{(i, j) \mid i = 1, 2, \ldots, p-1,\ j = 1, 2, \ldots, (q-1)/2\}.$$

I mängden S förekommer varje värde $i \in \{1, \ldots, p-1\}$ exakt $(q-1)/2$ gånger som första koordinat. Därmed erhålls

$$\prod_{(i,j) \in S} i = ((p-1)!)^{(q-1)/2}.$$

Den andra koordinaten varierar över $j = 1, \ldots, (q-1)/2$, och varje sådant värde förekommer $p-1$ gånger. Alltså fås

$$\prod_{(i,j)\in S} j = \Big(\Big(\frac{q-1}{2}\Big)!\Big)^{p-1}.$$

För att förenkla detta uttryck analyserar vi hur fakulteten $(q-1)!$ kan delas upp i två halvor. Vi skriver

$$(q-1)! = (1 \cdot 2 \cdots \tfrac{q-1}{2}) \cdot \Big((\tfrac{q+1}{2}) \cdot (\tfrac{q+3}{2}) \cdots (q-1)\Big).$$

Den första halvan är precis:

$$\Big(\frac{q-1}{2}\Big)!.$$

I den andra halvan sätter vi $j = q - r$ för $1 \le r \le (q-1)/2$, vilket ger

$$\prod_{j=\frac{q+1}{2}}^{q-1} j = \prod_{r=1}^{(q-1)/2} (q-r).$$

Modulo q gäller

$$q - r \equiv -r,$$

och därmed

$$\prod_{r=1}^{(q-1)/2} (q-r) \equiv \prod_{r=1}^{(q-1)/2} (-r) = \prod_{r=1}^{(q-1)/2} (-1) \cdot \prod_{r=1}^{(q-1)/2} r = (-1)^{\frac{q-1}{2}} \cdot \Big(\frac{q-1}{2}\Big)!.$$

Multiplicerar vi halvorna får vi identiteten

$$\Big(\frac{q-1}{2}\Big)!^2 \equiv (-1)^{\frac{q-1}{2}}(q-1)! \pmod{q}. \tag{5.11}$$

Denna identitet (5.11) gör det möjligt att skriva om faktorn

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

i termer av $(q-1)!$. Detta är avgörande för att kunna jämföra de två beräkningarna av produkten n.

För att skriva om denna faktor i en form som lätt kan jämföras med den andra beräkningen av n upphöjer vi därför båda sidor av (5.11) till potensen $(p-1)/2$. Detta ger

$$\Big(\Big(\frac{q-1}{2}\Big)!^2\Big)^{\frac{p-1}{2}} \equiv \Big((-1)^{\frac{q-1}{2}}(q-1)!\Big)^{\frac{p-1}{2}} \pmod{q}.$$

Detta förenklas till

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

Alltså får vi att produkten av alla element i G är

$$n = \left((p-1)!^{\frac{q-1}{2}},\ (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}}\right)U. \tag{5.12}$$

Vi bestämmer nu produkten n genom att istället låta varje ekvivalensklass i G representeras av ett heltal k modulo pq. Den kinesiska restsatsen ger en isomorfi

$$\mathbb{Z}_{pq}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$

Denna isomorfi ges explicit av avbildningen

$$k \longmapsto (k \bmod p,\ k \bmod q),$$

vilken är väldefinierad och bijektiv eftersom $\mathrm{SGD}(p,q) = 1$.

Varje par $(a,b) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ motsvaras av precis två heltal k och $-k$ modulo pq. I kvotgruppen G identifieras dessa två element, vilket innebär att vi kan välja

$$k = 1, 2, \ldots, \frac{pq-1}{2}$$

som dessutom uppfyller $(k, pq) = 1$. För att bestämma n räcker det alltså att beräkna produkten av koordinaterna

$$(k \pmod p,\ k \pmod q)$$

för alla sådana k.

Vi börjar med den första koordinaten. När k varierar över detta intervall antar restklassen k mod p varje värde $i \in \{1, 2, \ldots, p-1\}$ exakt $(q-1)/2$ gånger. Alltså är produkten av de första koordinaterna (innan vi tar hänsyn till k som är delbara med q) lika med

$$\prod_{i=1}^{p-1} i^{(q-1)/2} = (p-1)!^{(q-1)/2}.$$

Vissa av dessa k är delbara med q och ger därmed första koordinaten lika med 0 modulo q, vilket måste uteslutas. Det finns exakt $(p-1)/2$ sådana tal

$$q, 2q, \ldots, \frac{p-1}{2}q.$$

Var och en bidrar med faktorn q i den första koordinaten. För att kompensera detta dividerar vi därför med $q^{\frac{p-1}{2}}$.

Med hjälp av Eulers kriterium 5.4 fås

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

och eftersom Legendre-symbolen antar värdena ± 1 erhålls

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

På motsvarande sätt fås i den andra koordinaten uttrycket

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

Den andra beräkningen av produkten n ger alltså

$$n = \left((p-1)!^{\frac{q-1}{2}} \left(\tfrac{q}{p}\right),\ (q-1)!^{\frac{p-1}{2}} \left(\tfrac{p}{q}\right)\right)U. \tag{5.13}$$

För att kunna jämföra (5.12) och (5.13) använder vi Wilsons sats 5.10:

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

Eftersom (5.12) och (5.13) beskriver samma element i kvotgruppen G måste deras koordinater överensstämma.

Vi jämför först den första koordinaten. Detta ger

$$(-1)^{\frac{q-1}{2}} = \left(\frac{q}{p}\right). \tag{5.14}$$

På motsvarande sätt ger jämförelsen av den andra koordinaten

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{p}{q}\right). \tag{5.15}$$

Kombinerar vi (5.14) och (5.15), får vi

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

vilket är lagen om kvadratisk reciprocitet. □

6 Algoritmer för kvadraträtter

I detta avsnitt behandlas algoritmer för att beräkna kvadraträtter modulo ett primtal. Framställningen bygger huvudsakligen på [6].

När man har väl bestämt att ett tal a är ett kvadratiskt resttal (t.ex. med hjälp av Eulers kriterium 5.4) uppstår nästa fråga, hur hittar man själva kvadratroten? Det innebär att man vill bestämma ett heltal x som uppfyller

$$x^2 \equiv a \pmod{p}.$$

Detta är ett centralt problem inom både talteori och tillämpad matematik.

För små primtal kan man lösa problemet genom att testa alla $x = 1, 2 \ldots, p-1$, men för stora primtal krävs mer effektiva metoder. Vilken metod man använder beror på hur primtalet p ser ut.

6.1 Fallet för $p \equiv 3 \pmod 4$

Om primtalet p lämnar resten 3 vid division med 4, finns en enkel och effektiv formel för att bestämma kvadraträtter modulo p, nämligen

$$x \equiv a^{\frac{p+1}{4}} \pmod{p}. \tag{6.1}$$

Denna formel följer direkt från Eulers kriterium 5.4. För en kvadratisk rest a gäller nämligen att

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Vi vill nu hitta ett heltal x som uppfyller $x^2 \equiv a \pmod p$. För att använda Eulers kriterium sätter vi x enligt (6.1).

Om vi kvadrerar båda sidor får vi

$$x^2 = \left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}}.$$

Eftersom $a^{(p-1)/2} \equiv 1 \pmod p$ enligt Eulers kriterium 5.4, följer att

$$x^2 \equiv a \cdot 1 \equiv a \pmod{p}.$$

Alltså ger (6.1) en lösning till kongruensen $x^2 \equiv a \pmod p$.

Exempel 6.2. Vi vill hitta ett heltal x som uppfyller

$$x^2 \equiv 5 \pmod{19}.$$

Eftersom $19 \equiv 3 \pmod 4$ kan vi tillämpa formeln (6.1). Här är $a = 5$ och $p = 19$, vilket ger

$$x \equiv 5^{\frac{19+1}{4}} = 5^5 \pmod{19}.$$

Vi beräknar stegvis:

$$5^2 \equiv 6 \pmod{19}, \quad 5^4 \equiv 6^2 = 36 \equiv 17 \pmod{19},$$

varpå

$$5^5 \equiv 5^4 \cdot 5 \equiv 17 \cdot 5 = 85 \equiv 85 - 76 = 9 \pmod{19}.$$

En snabb kontroll ger:

$$9^2 = 81 \equiv 5 \pmod{19}.$$

vilket visar att $x = 9$ är en lösning. Den andra lösningen ges av $x \equiv -9 \equiv 10 \pmod{19}$.

6.2 Fallet för $p \equiv 1 \pmod 4$

När $p \equiv 1 \pmod 4$ kan den enkla formeln från föregående avsnitt inte användas för att bestämma kvadraträtter modulo p. I detta fall bestäms kvadraträtter modulo p med hjälp av en metod som bygger på att man konstruerar en ring där ett symboliskt element α uppfyller relationen

$$\alpha^2 = a.$$

Idén är att man istället för att direkt försöka hitta $\sqrt{a}$ i $\mathbb{Z}/p\mathbb{Z}$, arbetar i en ring där ett sådant element redan existerar formellt. Detta gör det möjligt att utföra algebraiska beräkningar där α beter sig som en kvadratroten till a.

För att kunna konstruera den algebraiska struktur som används i fallet $p \equiv 1 \pmod 4$ introducerar vi först begreppet ring. Metoden bygger på att kunna arbeta med element av typen $u + v\alpha$ och utföra addition och multiplikation på dessa. Vi börjar därför med definition av en ring.

Definition 6.3 (Ring)**.** *[6, Definition 2.1.3] En ring är en mängd försedd med två operationer, addition och multiplikation, som uppfyller följande egenskaper:*

- *Addition. Mängden är en abelsk grupp under addition:*
  - *det finns ett nollelement* 0 *sådant att* $a + 0 = 0 + a = a$*,*
  - *varje element* a *har en additivt invers* $-a$ *med* $a + (-a) = 0$*,*
  - *additionen är kommutativ och associativ.*

- *Multiplikation. Multiplikationen är associativ och det finns ett multiplikativt enhetselement* 1 *sådant att* $1a = a1 = a$.
- *Distributivitet. Multiplikation och addition samverkar enligt de distributiva lagarna*
$$a(b+c) = ab + ac, \qquad (a+b)c = ac + bc.$$

I en allmän ring behöver multiplikationen inte vara kommutativ, men i de ringar vi arbetar med här är den det. Dessa regler gör det möjligt att utföra algebraiska beräkningar på ett liknande sätt som i heltalen eller i polynomringar.

Vi kommer även att använda avbildningar mellan ringar, vilket motiverar följande definition.

Definition 6.4 (Ringhomomorfi)**.** *En avbildning* $f\colon R \to S$ *mellan två ringar kallas en ringhomomorfi om den bevarar addition och multiplikation, det vill säga*

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y),$$

samt uppfyller $f(1_R) = 1_S$.

Låt nu p vara ett udda primtal och låt a vara en kvadratisk rest modulo p. Vi definierar ringen

$$R = (\mathbb{Z}/p\mathbb{Z})[x]/(x^2 - a),$$

och betecknar bilden av x i R med α. I ringen R gäller därmed $\alpha^2 = a$.

Ringen R består av alla uttryck av formen

$$u + v\alpha, \qquad u, v \in \mathbb{Z}/p\mathbb{Z},$$

där addition och multiplikation ges av

$$(u_1 + v_1\alpha) + (u_2 + v_2\alpha) = (u_1 + u_2) + (v_1 + v_2)\alpha,$$

$$(u_1 + v_1\alpha)(u_2 + v_2\alpha) = (u_1u_2 + av_1v_2) + (u_1v_2 + v_1u_2)\alpha.$$

Eftersom $\alpha^2 = a$ kan varje element i R reduceras till just denna form.

För att bestämma en kvadratrotslösning till kongruensen

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

väljer man ett slumpmässigt element $z \in (\mathbb{Z}/p\mathbb{Z})^\times$ och bildar elementet

$$1 + z\alpha \in R.$$

Detta element upphöjs därefter till potensen $(p-1)/2$, vilket ger

$$w = (1 + z\alpha)^{\frac{p-1}{2}} = u + v\alpha, \qquad u, v \in \mathbb{Z}/p\mathbb{Z}. \tag{6.5}$$

Om koefficienten v är noll ger detta val av z ingen information. Man väljer i så fall ett nytt slumpmässigt värde på z. Om däremot $v \neq 0$ kan koefficienterna u och v användas för att bestämma en kvadratrotslösning till $x^2 \equiv a \pmod{p}$.

Låt b beteckna en faktisk kvadratrotslösning till a i $\mathbb{Z}/p\mathbb{Z}$, det vill säga $b^2 \equiv a \pmod{p}$. Konstruktionen innebär då att uttrycket

$$u + vb$$

är en $(p-1)/2$-te potens i $\mathbb{Z}/p\mathbb{Z}$. Enligt Eulers kriterium 5.4 måste ett sådant uttryck vara kongruent med 0, 1 eller -1 modulo p. Detta leder till tre möjliga linjära ekvationer i b:

$$\begin{cases} u + vb \equiv 0 \pmod{p} & \Rightarrow b \equiv -\frac{u}{v}, \\ u + vb \equiv 1 \pmod{p} & \Rightarrow b \equiv \frac{1-u}{v}, \\ u + vb \equiv -1 \pmod{p} & \Rightarrow b \equiv -\frac{1+u}{v}. \end{cases} \tag{6.6}$$

Eftersom u och v är kända kan man pröva dessa tre uttryck och kontrollera vilket som uppfyller kongruensen $b^2 \equiv a \pmod{p}$. Divisionen med v är väldefinierad eftersom $\mathbb{Z}/p\mathbb{Z}$ är en kropp och $v \neq 0$.

Bevis. Vi visar nu varför metoden ovan alltid leder till en korrekt kvadratrotslösning när $v \neq 0$. Resonemanget följer i huvudsak framställningen i Stein [6, §4.5, s. 88], men ges här i en mer utförlig form.

Låt b och $-b$ vara de två kvadraträtterna till a i $\mathbb{Z}/p\mathbb{Z}$, det vill säga $b^2 \equiv a \pmod{p}$. Definiera avbildningarna

$$f(u + v\alpha) = u + vb, \qquad g(u + v\alpha) = u + v(-b).$$

Dessa är ringhomomorfier, eftersom relationen $\alpha^2 = a$ i R motsvaras av $b^2 = a$ respektive $(-b)^2 = a$ i $\mathbb{Z}/p\mathbb{Z}$.

Tillsammans ger dessa avbildningar en ringisomorfi

$$\varphi\colon R \longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \qquad \varphi(u + v\alpha) = (u + vb,\ u - vb).$$

Betrakta nu elementet w enligt (6.5). Dess bild under φ är

$$\varphi(w) = (u + vb,\ u - vb).$$

Varje komponent är en $(p-1)/2$-te potens av ett element i $\mathbb{Z}/p\mathbb{Z}$ och är därför enligt Eulers kriterium 5.4, lika med 1 eller -1 med möjlighet att bli 0 om komponenten är noll i kroppen.

Detta visar att $u + vb \in \{-1, 0, 1\}$, vilket ger de tre linjära ekvationerna i (6.6). Eftersom $v \neq 0$ kan dessa lösas entydigt, och den lösning som uppfyller $b^2 \equiv a \pmod{p}$ är en kvadratrotslösning. □

Exempel 6.7. I föregående avsnitt visade vi med kvadratisk reciprocitet att

$$\left(\frac{-79}{101}\right) = 1,$$

vilket innebär att $a = -79$ är en kvadratisk rest modulo $p = 101$. Eftersom $101 \equiv 1 \pmod{4}$ befinner vi oss i det fall där den enklare formeln inte gäller. Vi behöver istället använda metoden som bygger på ringen

$$R = (\mathbb{Z}/101\mathbb{Z})[x]/(x^2 - a).$$

Vi låter α vara bilden av x i R, så att $\alpha^2 = a$. Eftersom $-79 \equiv 22 \pmod{101}$ kan vi arbeta med relationen $\alpha^2 = 22$.

Vi väljer därefter ett slumpmässigt element $z \in (\mathbb{Z}/101\mathbb{Z})^\times$ (till exempel $z = 4$) och bildar elementet w enligt (6.5):

$$w = (1 + 4\alpha)^{50}.$$

Beräkningen utförs i `Sage`(se nedan), vilket ger resultatet på formen

$$w = u + v\alpha, \qquad u, v \in \mathbb{Z}/101\mathbb{Z}.$$

Om $v = 0$ måste man välja ett nytt värde på z. I detta fall får vi dock $v \neq 0$, och närmare bestämt

$$u \equiv 0, \qquad v \equiv 86 \pmod{101}.$$

Eftersom $v \neq 0$ kan vi bestämma b med hjälp av de tre linjära relationerna i (6.6)

Med $u = 0$ och $v = 86$ reduceras dessa till

$$b \equiv 0, \qquad b \equiv 86^{-1}, \qquad b \equiv -86^{-1} \pmod{101}.$$

Inversen 86^{-1} beräknas med den utökade Euklidiska algoritmen, vilket ger

$$86^{-1} \equiv 74 \pmod{101}.$$

De möjliga kandidaterna är alltså

$$b \equiv 0,\ 74,\ 27 \pmod{101}.$$

Direkt beräkning visar att

$$74^2 \equiv 22 \pmod{101}, \qquad 27^2 \equiv 22 \pmod{101}.$$

Eftersom $22 \equiv -79 \pmod{101}$ följer att de två icke-triviala lösningarna är

$$x \equiv 74 \quad \text{eller} \quad x \equiv 27 \pmod{101}.$$

Detta bestämmer kvadratrötterna till $a = -79$ modulo 101.

Beräkningsanmärkning. I exemplet ovan användes `Sage` för att beräkna elementet

$$w = (1 + z\alpha)^{(p-1)/2}$$

i ringen

$$R = (\mathbb{Z}/101\mathbb{Z})[x]/(x^2 - 22).$$

Nedan visas den kod som användes för fallet $z = 4$, vilket gav

$$w = 0 + 86\alpha.$$

```
p = 101
a = 22
S.<x> = PolynomialRing(GF(p))
R.<alpha> = S.quotient(x^2 - a)

z = 4
w = (1 + z*alpha)^((p-1)//2)

u, v = w
print("w =", u, "+", v, "* alpha")
```

```
w = 0 + 86 * alpha
```

Referenser

[1] Rikard Bøgvad m. fl. *Algebra I*. Matematiska institutionen, Stockholms universitet, 2023.

[2] Encyclopædia Britannica. *Number Theory in the 19th Century*. 2024. URL: https://www.britannica.com/science/number-theory.

[3] Lars-Åke Lindahl. *Elementär Talteori*. Kompendium, Uppsala universitet. 2012. URL: https://www2.math.uu.se/~lakelind/kompendier/Talteori_svenska.pdf.

[4] Mary Radcliffe. *Chinese Remainder Theorem*. Math 127 Lecture Notes, Carnegie Mellon University. URL: https://www.math.cmu.edu/~mradclif/teaching/127S19/Notes/ChineseRemainderTheorem.pdf.

[5] George Rousseau. "On the Quadratic Reciprocity Law". I: *Journal of the Australian Mathematical Society (Series A)* 51 (1991), s. 423–425.

[6] William Stein. *Elementary Number Theory: Primes, Congruences, and Secrets*. Version 3.1. University of Washington, 2017.

[7] Eric W. Weisstein. *Quadratic Reciprocity Theorem*. From MathWorld–A Wolfram Resource. 2024. URL: https://mathworld.wolfram.com/QuadraticReciprocityTheorem.html.