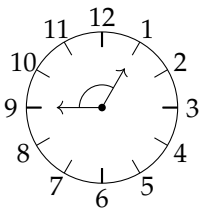
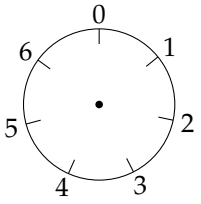
Kapittel 26

Kongruensregning

I dette kapitlet lærer du om kongruensregning. Vi definerer modulær ekvivalens, og lærer om modulære inverser, modulær potensregning, og diskrete logaritmer.



$9 + 4 \equiv 1 \pmod{12}$



$3 \cdot 4 = 12 \equiv 5 \pmod{7}$

Klokkearitmetikk

Kongruensregning kan også kalles *klokkearitmetikk*, fordi det minner om måten tallene er ordnet på en klokke. Hvis klokken er ni nå, så er den ett om fire timer. Med andre ord har vi $9 + 4 = 1$ på klokken. Tilsvarende har vi for eksempel at $3 = 15 = 27$, og $12 = 0$.

Vi kan også lage oss en teoretisk klokke som har for eksempel 7 forskjellige tall istedenfor 12. På den klokken har vi at $7 = 0$, og $3 \cdot 4 = 12 = 5$.

Hvis vi vil si at to tall er like i klokkesystemet med m forskjellige tall, så sier vi at de to tallene er *kongruente modulo* m. Vi har en egen notasjon for dette, slik at vi ser om tallene faktisk er like, eller bare like innenfor et bestemt klokkesystem.

Definisjon 26.1 Kongruenser

La a, b og m være heltall, med $m > 0$. Hvis m deler $a - b$, sier vi at a er **kongruent med** b *modulo* m, og skriver:

$$a \equiv b \pmod{m}.$$

Tallet m i kongruensen kalles **modulus**. Hvis a ikke er kongruent med b modulo m, skriver vi:

$$a \not\equiv b \pmod{m}.$$

Eksempel Vi har $50 \equiv 2 \pmod{12}$, fordi $12 \mid (50-2)$. Men $9 \not\equiv 23 \pmod{4}$, fordi $4 \nmid (9-23)$. ♦

Oppgave Hva betyr det at to positive heltall er kongruente modulo 10? Med andre ord: Hvis vi har $a \equiv b \pmod{10}$, hva kan vi da si om a og b? Tilsvarende: Hva betyr det at to vilkårlige heltall er kongruente modulo 2? ♦

Løsning Dersom to tall er kongruente modulo 10 så betyr det at siste siffer av a og siste siffer av b er identiske, fordi vi fjerner alle multiplum av 10 i tallene. Dersom to tall er kongruente modulo 2 så betyr det at de har samme paritet, altså at begge to er oddetall eller at begge to er partall. ♦

Ordet «mod» i kongruensnotasjonen ser kjent ut, for vi har tidligere definert en operator som heter det samme. Vi definerte $a \bmod b$ til å bety resten vi får når a deles på b. Det er viktig å ikke blande sammen de to betydningene – det er ikke samme «mod» i uttrykket $a \bmod b$ som i $a \equiv b \pmod{m}$!

Men er det noen sammenheng mellom de to ulike betydningene av «mod»? Ja, for det at to tall er kongruente modulo m betyr at de gir samme rest når de deles på m. Vi har altså følgende resultat:

Vi har $a \equiv b \pmod{m}$ hvis og bare hvis $a \bmod m = b \bmod m$.

Vi kan også merke oss at vi kan beskrive $a \bmod m$ på denne måten: $a \bmod m$ er det tallet r som oppfyller både $a \equiv r \pmod{m}$ og $0 \leqslant r < m$.

Det er ingen tilfeldighet at tegnet $\equiv$ for kongruens ligner på likhetstegnet. Vi tenker på kongruenser som en slags likhet, og mange av regnereglene som vi er vant til å bruke for likheter gjelder også for kongruenser.

Eksempel Vi vil løse likningen $x + 5 \equiv 1 \pmod{7}$. Ved å bruke regnereglene for kongruenser kan vi gå frem på samme måte som om vi skulle løse en vanlig likning. Vi får:

$$x \equiv 1 - 5 = -4 \equiv 3 \pmod{7}$$

Løsningen er altså $x \equiv 3 \pmod{7}$. ♦

Legg merke til hvordan vi setter flere kongruenser sammen på samme linje, og dessuten blander inn en likhet:

$$x \equiv 1 - 5 = -4 \equiv 3 \pmod{7}$$

Dette leses som «x er kongruent med $(1-5)$, som er lik -4, som er kongruent med 3, der kongruensene er modulo 7». Merk at $\pmod 7$ her beskriver begge de to kongruensene. Når vi setter flere kongruenser etter hverandre på denne måten, må de ha samme modulus, og den skriver vi bare én gang.

Selv om vi for det meste kan behandle kongruenser som likheter, er det ett viktig unntak: Vi kan ikke uten videre forkorte bort en felles faktor fra begge sider av en kongruens. Altså: Hvis vi har en kongruens $ca \equiv cb \pmod m$, der $c \not\equiv 0 \pmod m$, får vi ikke nødvendigvis at $a \equiv b \pmod m$. For eksempel er $2 \cdot 9 \equiv 2 \cdot 5 \pmod 8$, men $9 \not\equiv 5 \pmod 8$.

Vi skal imidlertidig se at vi alltid kan gå fra $ca \equiv cb$ til $a \equiv b$, men de to kongruensene blir ikke nødvendigvis modulo samme tall.

Oppgave Vis at dersom $ca \equiv cb \pmod m$ og $d = \gcd(c, m)$, så er $a \equiv b \pmod{m/d}$. ♦

Løsning Kongruensen $ca \equiv cb \pmod m$ betyr, per definisjon, at $m \mid (ca - cb)$, og dermed finnes et heltall e slik at $em = ca - cb$. La $m' = m/d$ og $c' = c/d$. Da har vi:

$$em'd = em = ca - cb = c(a-b) = c'd(a-b)$$

Nå kan vi forkorte bort d og få:

$$em' = c'(a-b)$$

Det betyr at $m' \mid c'(a-b)$. Siden vi dessuten har at $m' \perp c'$ (vi delte bort $d = \gcd(c, m)$, så derfor må $\gcd(c', m') = 1$), så følger det at $m' \mid (a-b)$. Dermed har vi vist at $a \equiv b \pmod{m'}$. ♦

Eksempel Fra teksten ovenfor har vi $2 \cdot 9 \equiv 2 \cdot 5 \pmod 8$, og da får vi at $9 \equiv 5 \pmod 4$. ♦

Følgende to resultater, som følger lett fra oppgaven over, beskriver tilfeller der vi kan forkorte bort en felles faktor fra begge sider av en kongruens uten å skifte modulus.

Eksempel Hvis $ca \equiv cb \pmod m$ og $c \perp m$, så er $a \equiv b \pmod m$. Siden $c \perp m$ er $\gcd(c, m) = 1$, får vi at $a \equiv b \pmod{m/1}$. ♦

Eksempel Hvis $ca \equiv cb \pmod p$, der p er et primtall og $p \nmid c$, så er $a \equiv b \pmod p$. Siden p er et primtall og $p \nmid c$ får vi $p \perp c$, og resultatet følger. ♦

Modulære inverser

Hvis vi skal løse en lineær likning

$$ax = b$$

over de reelle tallene (eller de rasjonale tallene), så vil vi ganske enkelt dele på a på begge sider og få $x = b/a$. Dette kan vi også tenke på som at vi ganger med $1/a$:

$$\underbrace{\frac{1}{a} \cdot a}_{=1} \cdot x = \frac{1}{a} \cdot b$$

Når vi skal løse kongruenslikningen

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

kan vi ikke dele på a eller gange med $1/a$. Men noen ganger kan vi gjøre noe veldig liknende. Dersom det finnes et tall c som er slik at

$$c \cdot a \equiv 1 \pmod{m},$$

så vil c spille en tilsvarende rolle som tallet $1/a$ gjør: Å gange med det opphever virkningen av å gange med a.

Hvis vi har funnet et slikt tall c, så kan vi gange med det på begge sider av likningen og få:

$$\underbrace{c \cdot a}_{\equiv 1} \cdot x \equiv bc \pmod{m}$$

Dermed har vi løsningen $x \equiv bc \pmod{m}$.

Når vi snakker om reelle eller rasjonale tall, sier vi at tallet $1/a$ er *inversen* til a. Tilsvarende snakker vi i kongruensregning om «invers modulo m».

Definisjon 26.2 Modulære inverser

La a, c og m være heltall, med $m > 0$. Hvis $c \cdot a \equiv 1 \pmod{m}$, sier vi at c er en *invers* til a modulo m.

Eksempel La oss løse kongruenslikningen

$$12x \equiv 4 \pmod{25}.$$

Det går selvfølgelig fint å løse den på vanlig måte med Euclids algoritme, men dersom vi prøver oss litt frem så ser vi at

$$23 \cdot 12 \equiv 1 \pmod{25}.$$

Vi ganger så med inversen på begge sider av likningen:

$$\underbrace{23 \cdot 12}_{\equiv 1} \cdot x \equiv 4 \cdot 23 \pmod{25}.$$

Dermed får vi $x \equiv 4 \cdot 23 = 92 \equiv 17 \pmod{25}$. ♦

Men er det alltid mulig å finne en invers? La oss se på et nytt eksempel.

Eksempel Finnes det noen invers til 4 modulo 6? Ethvert heltall er kongruent modulo 6 med enten 0, 1, 2, 3, 4 eller 5. La oss sjekke om noen av disse tallene oppfyller kriteriet for å være en invers til 4 (alle kongruensene er modulo 6):

$$4 \cdot 0 = 0 \not\equiv 1 \qquad 4 \cdot 3 = 12 \equiv 0 \not\equiv 1$$
$$4 \cdot 1 = 4 \not\equiv 1 \qquad 4 \cdot 4 = 16 \equiv 4 \not\equiv 1$$
$$4 \cdot 2 = 8 \equiv 2 \not\equiv 1 \qquad 4 \cdot 5 = 20 \equiv 2 \not\equiv 1$$

Vi har altså funnet ut at 4 ikke har noen invers modulo 6. ♦

Det at a har en invers modulo m er det samme som at likningen $ax \equiv 1 \pmod{m}$ er løsbar. Ved hjelp av det vi vet om slike likninger kan vi beskrive akkurat hvilke tall som har inverser:

Oppgave La a og m være heltall, med $m > 0$. Vis at a har invers modulo m hvis og bare hvis $a \perp m$. ♦

Løsning Tallene som er inverser til a er nøyaktig de som er løsninger av likningen $ax \equiv 1 \pmod{m}$. Det kan vi se ved å skrive dette om til den Diofantiske likningen $ax + my = 1$. Tidligere har vi sett at denne likningen har en løsning hvis og bare hvis $\gcd(a, m) = 1$, altså hvis og bare hvis $a \perp m$. ♦

Det er lett å se at 0, og alle tall som er kongruente med 0, ikke kan ha noen invers. Men hvis modulusen er et primtall, har alle andre tall inverser. Dette skjer hvis og bare hvis modulusen er et primtall, som beskrevet i følgende oppgave.

Oppgave Vis at alle tall (unntatt de som er kongruente med 0) har invers modulo m hvis og bare hvis m er et primtall. ♦

Løsning Anta først at m er et primtall og a et tall slik at $a \not\equiv 0 \pmod{m}$. Da er $a \perp m$, og dermed vet vi at a har en invers modulo m.

Anta nå at m ikke er et primtall. Hvis $m = 1$, er alle tall kongruente med 0 modulo m, så det er ingenting å vise. Anta derfor at $m > 3$, og at m er et sammensatt tall. Da finnes en divisor d av m slik at $1 < d < m$, og vi vet at at d ikke har invers modulo m fordi $d \not\equiv 1 \pmod{m}$. Altså finnes det minst ett tall som ikke er kongruent med 0 og som heller ikke har invers. ♦

Eksempel La oss finne alle inverser modulo 7. Vi vet fra tidligere at alle tall som ikke er kongruente med 0 har inverser. For å finne inversene kan vi prøve oss frem ved å gange sammen forskjellige tall, og observere at:

$$1 \cdot 1 = 1 \equiv 1 \pmod{7}$$
$$2 \cdot 4 = 8 \equiv 1 \pmod{7}$$
$$3 \cdot 5 = 15 \equiv 1 \pmod{7}$$
$$6 \cdot 6 \equiv (-1) \cdot (-1) = 1 \pmod{7}$$

Dermed kan vi lage følgende oversikt over inverser modulo 7:

a:	1	2	3	4	5	6
invers til a modulo 7:	1	4	5	2	3	6

♦

Modulær potensregning

Vi vil se på hvordan vi kan regne ut et uttrykk på formen

$$a^e \bmod m$$

når eksponenten e kan være veldig stor.

Eksempel Vi vil regne ut $3^{371} \bmod 5$. Den åpenbare måten å gjøre det på er å først regne ut 3^{371}, og så dele på 5 og finne resten. Problemet er at 3^{371} er et veldig stort og uhåndterlig tall. Vi kan bruke kongruensregning til å gjøre utregningen på en smartere måte, der vi unngår å få store tall underveis.

Vi begynner med å se på noen lavere potenser av 3 redusert modulo 5:

$$\begin{aligned} 3^2 &= 9 \equiv 4 \pmod 5 \\ 3^3 &= 3^2 \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 2 \pmod 5 \\ 3^4 &= 3^3 \cdot 3 \equiv 2 \cdot 3 = 6 \equiv 1 \pmod 5 \end{aligned}$$

Legg merke til at når vi først vet at 3^2 er kongruent med 4, så kan vi regne ut 3^3 som $4 \cdot 3$. Og når vi vet at 3^3 er kongruent med 2, så kan vi regne ut 3^4 som $2 \cdot 3$. Slik klarer vi å hele tiden holde oss til små tall.

Legg også merke til det vi fant på den siste linjen: $3^4 \equiv 1 \pmod 5$. Der hadde vi kjempeflaks, for nå kan vi enkelt regne ut så store potenser av 3 som vi vil modulo 5. Vi ville regne ut $3^{371} \bmod 5$. Vi får:

$$3^{371} = 3^{92 \cdot 4 + 3} = (3^4)^{92} \cdot 3^3 \equiv 1^{92} \cdot 2 = 2 \pmod 5$$

Altså har vi $3^{371} \bmod 5 = 2$. ♦

I dette eksemplet hadde vi flaks og fikk at 3^4 var kongruent med 1, slik at vi umiddelbart kunne se bort fra alle potenser av 3^4, eller med andre ord alle multipler av 4 i eksponenten.

Vi kan imidlertid ikke regne med å ha like mye flaks alltid. Hvis vi ikke satser på et lykketreff, er det en bedre strategi å regne ut

$$a^2,\ a^4,\ a^8,\ a^{16},\ a^{32},\ \ldots$$

modulo m, og så finne $a^e \bmod m$ ved å kombinere disse. Det neste eksemplet viser denne fremgangsmåten.

Eksempel Vi vil regne ut 5^{22} mod 77. Vi begynner med å regne ut 5 opphøyd i toerpotensene 2, 4, 8 og 16:

$$\begin{aligned} 5^2 &= 25 \\ 5^4 &= 5^2 \cdot 5^2 = 25 \cdot 25 \equiv 9 \pmod{77} \\ 5^8 &= 5^4 \cdot 5^4 \equiv 9 \cdot 9 \equiv 4 \pmod{77} \\ 5^{16} &= 5^8 \cdot 5^8 \equiv 4 \cdot 4 = 16 \pmod{77} \end{aligned}$$

Vi kan skrive eksponenten 22 som en sum av toerpotenser slik:

$$22 = 16 + 4 + 2$$

Dermed har vi:

$$5^{22} = 5^{16+4+2} = 5^{16} \cdot 5^4 \cdot 5^2 \equiv 16 \cdot 9 \cdot 25 \equiv 58 \pmod{77}$$

Dette vil si at 5^{22} mod $77 = 58$. ♦

Totallssystemet. Denne fremgangsmåten baserer seg på at vi alltid kan skrive et naturlig tall e som en sum av toerpotenser. Dette tilsvarer å skrive tallet e i *totallssystemet*, eller som *binærtall*.

I titallssystemet, som vi bruker til vanlig, står hvert siffer for en tierpotens:

$$1387_{10} = 1 \cdot 10^3 + 3 \cdot 10^2 + 8 \cdot 10^1 + 7 \cdot 10^0$$

I totallssystemet står hvert siffer for en toerpotens. Da trenger vi bare sifrene 0 og 1:

$$10110_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 22$$

Hvordan kan vi skrive et tall e i totallssystemet? Merk at siste siffer må være 0 hvis e er et partall, og 1 hvis det er et oddetall. Vi kan dele e på 2 med heltallsdivisjon og få:

$$e = q \cdot 2 + r \qquad 0 \leqslant r < 2$$

La $d_s, d_{s-1}, \ldots, d_2, d_1, d_0$ være sifrene til e i totallssystemet. Da har vi:

$$e = (\underbrace{d_s\ d_{s-1}\ \cdots\ d_2\ d_1}_{q}\ \underbrace{d_0}_{r})_2$$

Altså: Det siste sifferet er e mod 2, og de øvrige sifrene er lik sifrene for tallet $q = \frac{e-(e \bmod 2)}{2}$.

Modulær potensiering ved hjelp av totallssystemet. Som vi har sett, kan vi altså benytte totallssystemet til å forenkle utregningen av modulære potenser.

Eksempel Vi vil skrive tallet 83 i totallssystemet. Vi har:

$$\begin{aligned} 83 &= 41 \cdot 2 + 1 & 5 &= 2 \cdot 2 + 1 \\ 41 &= 20 \cdot 2 + 1 & 2 &= 1 \cdot 2 + 0 \\ 20 &= 10 \cdot 2 + 0 & 1 &= 0 \cdot 2 + 1 \\ 10 &= 5 \cdot 2 + 0 \end{aligned}$$

Fra den første linjen ser vi at siste siffer i 83 er 1, og alle sifrene unntatt det siste er sifrene for 41. Neste linje gir oss at siste siffer i 41 skal være 1, og at alle unntatt det siste er sifrene for 20. Så får vi at siste siffer i 20 er 0, og så videre. Totalt får vi:

$$83_{10} = 1010011_2$$

♦

Eksempel Vi regner ut 36^{83} mod 125. Vi begynner med å opphøye 36 i toerpotenser og redusere modulo 125 (alle kongruensene er modulo 125):

$$\begin{aligned} 36^1 &= 36 & 36^{16} &\equiv 81^2 = 6561 \equiv 61 \\ 36^2 &= 1296 \equiv 46 & 36^{32} &\equiv 61^2 = 3721 \equiv 96 \\ 36^4 &\equiv 46^2 = 2116 \equiv 116 & 36^{64} &\equiv 96^2 = 9216 \equiv 91 \\ 36^8 &\equiv 116^2 = 13456 \equiv 81 \end{aligned}$$

Vi vet fra forrige eksempel at

$$83_{10} = 1010011_2 = 64 + 16 + 2 + 1,$$

og dermed får vi:

$$\begin{aligned} 36^{83} &= 36^{64+16+2+1} = 36^{64} \cdot 36^{16} \cdot 36^2 \cdot 36^1 \\ &\equiv 91 \cdot 61 \cdot 46 \cdot 36 \equiv 81 \pmod{125} \end{aligned}$$

Dette betyr at 36^{83} mod 125 = 81. ♦

Diskrete logaritmer

Til slutt i dette kapittelet skal vi studere *diskrete logaritmer*. Når vi regner med reelle tall, kan vi alltid beregne en logaritme av et positivt tall x gitt en base y som $z = \log_y x$ og få et nytt reelt tall z som svar. Dette er det samme som å si at $y^z = x$. Men hva skjer når vi regner med en modulus?

Gitt en modulus m og base a, så vi ovenfor hvordan vi kan beregne

$$a^e \bmod m$$

selv når eksponenten e er veldig stor. Dersom vi multipliserte a med seg selv e ganger så kan det ta veldig lang tid, nemlig e modulære multiplikasjoner.

Men dersom vi benytter algoritmen ovenfor så trenger vi bare gjøre ca. $\log_2 e$ modulære multiplikasjoner. Dette er eksponentielt raskere!

Dersom man blir gitt et tall b, en base a og en modulus m, hvordan beregner man da $e = \log_a b$ slik at $b = a^e \bmod m$? Merk at vi kun jobber med heltall, og vi definerer dermed e på følgende vis.

Definisjon 26.3 Diskrete logaritmer

La a, b, e og m være heltall, med $m > 0$. Hvis $b \equiv a^e \bmod m$, sier vi at e er den *diskrete logaritmen* til b med hensyn til basen a modulo m.

Først observerer vi at dersom man regner med reelle tall, så er eksponentiering en strengt voksende funksjon (dersom $e_1 < e_2$ så er $a^{e_1} < a^{e_2}$), og tilsvarende for logaritmer (dersom $b_1 < b_2$ så er $\log_a b_1 < \log_a b_2$). Dette er ikke (nødvendigvis) tilfellet for modulære potenser og diskrete logaritmer.

Eksempel La oss benytte basen $a = 2$ i begge tilfeller. Dersom vi beregner 2^i for stigende heltall i, vil resultatet vokse:

$$2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16, \quad 2^5 = 32, \quad 2^6 = 64,$$
$$2^7 = 128, \quad 2^8 = 256, \quad 2^9 = 512, \quad 2^{10} = 1024, \ldots$$

Dersom vi velger, for eksempel, modulus $m = 11$, får vi et annet resultat:

$$2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 5, \quad 2^5 \equiv 10, \quad 2^6 \equiv 9,$$
$$2^7 \equiv 7, \quad 2^8 \equiv 3, \quad 2^9 \equiv 6, \quad 2^{10} \equiv 1, \ldots$$ ♦

Denne rekken med tall ser faktisk ganske tilfeldig ut …

Så hvordan beregner man $\log_a b$ dersom man er gitt et tall b, en base a og en modulus m? På samme måte som ved faktorisering så er det mulig å prøve alle muligheter: først beregner man $a^2 \bmod m$ og sjekker om dette er likt b. Dersom de er like så har vi funnet $e = 2$, og dersom de er ulike så må vi prøve neste potens helt frem til vi finner den rette. Vi prøve maksimalt m forskjellige potenser før vi finner den rette (senere skal vi lære at vi trenger færre, avhengig av primtallsfaktoriseringen til m), dersom den eksisterer, og både e og m kan være veldig store tall. Kan vi gjøre bedre?

For å kunne finne e så må vi være sikre på at den eksisterer, og dette avhenger av a, b, og m.

Eksempel Dersom $\gcd(a, m) \neq 1$ så finnes det minst en b slik at det ikke finnes noen e som gir $b \equiv a^e \bmod m$. For eksempel, dersom $a = 2$ og $m = 8$ så vil $a^i \bmod m$ alltid være et partall, og en slik e vil ikke eksistere dersom b er et oddetall. ♦

I siste seksjon skal vi se hvordan vi kan beregne e mer effektivt når m er et primtall, men vi bemerker at denne algoritmen kan utvides til vilkårlige positive heltall a, b og m, gitt at en slik logaritme e eksisterer.

Shanks algoritme

Fordi m nå er et primtall så jobber vi heller med primtallsmodulus p. La a være en base slik at $1 < a < p$. Målet er at for en gitt b, så ønsker vi å finne en e slik at $b \equiv a^e \bmod p$. Shanks algoritme lar oss beregne dette ved hjelp av ca. $\sqrt{p}$ modulære multiplikasjoner.

Først definerer vi $n = \sqrt{p}$ (rund opp til nærmeste heltall). Videre sier vi at $e = i \cdot n + j$ for ukjente heltall i og j fra mengden $\{0, \ldots, n-1\}$; målet blir dermed å finne i og j.

Dersom $b \equiv a^e \bmod p$, så får vi at

$$b \equiv a^{i \cdot n + j} \bmod p \Leftrightarrow b \cdot (a^{-n})^i \equiv a^j \bmod p$$

La $c = a^{-n} \bmod p$ (og siden modulusen p er et primtall så vet vi at inverser er veldefinerte). Da kan vi gjøre det følgende:

(1) Lag en liste med tuplene $(j, a^j \bmod p)$ for alle $0 \leqslant j < n$.

(2) For hver verdi $i = 0, ..., n-1$ så beregner vi verdien $b \cdot c^i \bmod p$.

(3) Dersom $b \cdot c^i \bmod p$ er i listen ovenfor har vi funnet $e = i \cdot n + j$.

Da ser vi at til slutt så har vi sjekket alle verdier, og algoritmen må ha funnet e i prosessen. Her antar vi at det er enkelt å sjekke om en verdi er i listen eller ikke uten at man må sjekke alle elementene, for eksempel dersom listen er sortert og man benytter binærsøk. Først beregner vi $\sqrt{p}$ etterfølgende potenser, og deretter maksimalt $\sqrt{p}$ nye potenser og sjekker hver for om de er med i listen. Dette er mye raskere enn å sjekke alle muligheter!

Oppgave Klarer du, ved hjelp av Shanks algoritme, å finne den diskrete logaritmen e til $b = 54$ med hensyn til $a = 3$ modulo $p = 101$? ♦

Digresjon

Siden kongruenser er refleksive, symmetriske og transitive, oppfyller de kravene til en ekvivalensrelasjon som definert i kapittel 6. Dette er kanskje lettere å se hvis vi introduserer den følgende notasjonen for kongruenser: For et gitt heltall m, la relasjonen $\equiv_m$ være slik at $a \equiv_m b$ hvis og bare hvis $a \equiv b \pmod{m}$. Da har vi at:

(1) $\equiv_m$ er refleksiv: $a \equiv_m a$.

(2) $\equiv_m$ er symmetrisk: $a \equiv_m b$ hvis og bare hvis $b \equiv_m a$.

(3) $\equiv_m$ er transitiv: $a \equiv_m b$ og $b \equiv_m c$ medfører at $a \equiv_m c$.

Siden $\equiv_m$ er en ekvivalensrelasjon, kan vi derfor også definere *ekvivalensklasser* på den, som definert i kapittel 17:

$$[a]_m = \{b \mid a \equiv_m b\}.$$

Disse ekvivalensklassene kalles gjerne kongruensklasser, og vi har for eksempel kongruensklassene $[1]_3 = \{\ldots, -2, 1, 4, 7, \ldots\}$ og $[2]_3 = \{\ldots, -1, 2, 5, 8, \ldots\}$. Hvis man definerer operasjoner elementvis, går det da an å gjøre beregninger på dem. For eksempel har vi da at

$$[2]_3 + [2]_3 = [4]_3 = [1]_3.$$

Mengden av alle kongruensklasser kalles en kvotientmengde (se kapittel 17). Hvis for eksempel de mulige verdiene a er fra mengden av alle heltall $\mathbb{Z}$, så gir relasjonen $\equiv_m$ oss kvotientmengden:

$$\mathbb{Z}/\equiv_m = \{[a]_m \mid a \in \mathbb{Z}\}.$$

Denne mengden skrives ofte simpelthen $\mathbb{Z}_m$, og inneholder nøyaktig m elementer, nemlig de m kongruensklassene fra $[0]_m$ til $[m-1]_m$. Når man driver kongruensregning på et mer avansert nivå vil denne mengden ofte erstatte mengden $\mathbb{Z}$ helt, slik at kongruensmengdene $[a]_m$ også erstatter selve heltallene, og bare skrives a. Dersom vi for eksempel visste at vi jobbet i $\mathbb{Z}_3$, ville det derfor ikke vært uvanlig å se noen skrive at

$$2 + 2 = 1.$$