Oversikt over det kinesiske restteoremet

Richard Williamson

3. desember 2014

Oppgave 1

Finn et heltall x slik at:

(1) $x \equiv 2 \pmod 6$;

(2) $x \equiv 3 \pmod{11}$.

Hvordan vet jeg at vi bør benytte det kinesiske restteoremet?

Hvis x må oppfyller to eller flere kongruenser, er det alltid det kinesiske restteoremet som bør benyttes om det er mulig.

Er det alltid mulig å benytte det kinesiske restteoremet?

Nei: de to heltallene vi jobber modulo, 6 og 11 i dette tilfellet, må være relativt primitiske for å benytte det kinesiske restteoremet. Det vil si: den største felles divisoren til disse to heltallene må være 1.

Hvis dette kravet er, som i dette tilfellet, oppfylt: ja! Det kinesiske restteoremet kan da alltid benyttes.

Når vi løser Oppgave 1, bør vi altså begynne med å observere at $\mathsf{sfd}(6, 11) = 1$.

Hvordan løse oppgaven?

Løs først følgende kongruenser hver for seg:

(A) $11x \equiv 1 \pmod 6$;

(B) $6x \equiv 1 \pmod{11}$.

Hvordan gjør jeg det?

Disse er lineære kongruenser. Vi har flere måter å løse lineære kongruenser: se oversikten om dette. Husk at vi *alltid* kan benytte Euklids algoritme om vi ikke ser fort en annen måte å gjøre det.

Løs (A)

Siden 6 er lite, kan vi i dette eksemplet gå gjennom de naturlige tallene 1, 2, ..., 6 til vi kommer fram til en løsning Vi får: $x = 5$ er en løsning til kongruensen

$$11x \equiv 1 \pmod{6}.$$

Det vil si:

$$11 \cdot 5 \equiv 1 \pmod{6}.$$

Løs (B)

På lignende vis ser vi fort at $x = 2$ er en løsning til kongruensen

$$6x \equiv 1 \pmod{11}.$$

Det vil si:

$$6 \cdot 2 \equiv 1 \pmod{11}.$$

Hvordan kan jeg huske Steg 1?

Bygg opp kongruensene som følger.

(1) Begynn med

$$\pmod{6}$$

og

$$\pmod{11},$$

som i de opprinnelige kongruensene.

(2) Sett 1 til høyre i begge:

$$\equiv 1 \pmod{6}$$

og

$$\equiv 1 \pmod{11}.$$

(3) Bytt om 6 og 11, og sett dem som koeffisienter:

$$11x \equiv 1 \pmod{6}$$

og

$$6x \equiv 1 \pmod{11}.$$

Så langt

Vi har:

$$11 \cdot 5 \equiv 1 \pmod{6}$$

og

$$6 \cdot 2 \equiv 1 \pmod{11}.$$

Sammenlign med målet

I den opprinnelige oppgaven, er vi ikke interessert i noe som er kongruent til 1 modulo 6. Vi er interesert i noe som er kongruent til 2 modulo 6.

På lignende vis er vi ikke interessert i noe som er kongruent til 1 modulo 11. Vi er interesert i noe som er kongruent til 3 modulo 11.

Derfor

Gang begge sidene av kongruensen

$$11 \cdot 5 \equiv 1 \pmod{6}$$

med 2. Vi får:

$$11 \cdot 5 \cdot 2 \equiv 2 \pmod{6}.$$

Gang begge sidene av kongruensen

$$6 \cdot 2 \equiv 1 \pmod{11}$$

med 3. Vi får:

$$6 \cdot 2 \cdot 3 \equiv 3 \pmod{11}.$$

Konklusjon

La x være summen av de venstre sidene, altså

$$x = 11 \cdot 5 \cdot 2 + 6 \cdot 2 \cdot 3 = 146.$$

Dette heltallet er en løsning til oppgaven, altså

$$x \equiv 2 \pmod{6}$$

og

$$x \equiv 3 \pmod{11}.$$

Hvorfor virker metoden?

Leddet $6 \cdot 2 \cdot 3$ av x forsvinner modulo 6, fordi $6 \mid 6 \cdot 2 \cdot 3$, altså

$$6 \cdot 2 \cdot 3 \equiv 0 \pmod{6}.$$

Derfor er

$$x \equiv 11 \cdot 5 \cdot 2 \pmod{6}.$$

Vi vet at

$$11 \cdot 5 \cdot 2 \equiv 2 \pmod{6}.$$

Dermed er

$$x \equiv 2 \pmod{6}.$$

Leddet $11 \cdot 5 \cdot 2$ av x forsvinner modulo 11, fordi $11 \mid 11 \cdot 5 \cdot 2$, altså

$$11 \cdot 5 \cdot 2 \equiv 0 \pmod{11}.$$

Derfor er

$$x \equiv 6 \cdot 2 \cdot 3 \pmod{11}.$$

Vi vet at

$$6 \cdot 2 \cdot 3 \equiv 3 \pmod{11}.$$

Dermed er

$$x \equiv 3 \pmod{11}.$$

Husk!

Sjekk om svaret ditt er riktig! Det vil si: sjekk om heltallet du kommer fram til oppfyller de to kongruesene i oppgaven.

Oppgave 2

Finn alle heltallene x slik at:

(1) $x \equiv 2 \pmod{6}$;

(2) $x \equiv 3 \pmod{11}$.

Hvordan løse oppgaven?

Finn først *ett* heltall x som oppfyller disse to kongruensene, som i Oppgave 1. Vi får: $x = 146$.

Hva gjør jeg da?

Gang de to heltallene vi jobber modulo: $6 \cdot 11 = 66$.

Konklusjon

Alle løsningene: $x = 146 + 66t$, hvor t er et hvilket som helst heltall.

For eksempel

Vi finner følgende løsninger ved å velge verdier av t.

t	x
-3	-52
-2	14
-1	80
0	146
1	212
2	278
3	344

Hvorfor virker metoden?

Siden $6 \mid 66$, er

$$66 \equiv 0 \pmod 6.$$

Siden $11 \mid 66$, er i tillegg

$$66 \equiv 0 \pmod{11}.$$

Derfor er både

$$146 + 66t \equiv 146 \pmod 6$$

og

$$146 + 66t \equiv 146 \pmod{11},$$

og vi vet fra Oppgave 1 at

$$146 \equiv 2 \pmod 6$$

og

$$146 \equiv 3 \pmod{11}.$$

Dermed ser vi at

$$x = 146 + 66t$$

er en løsning til begge vår opprinnelige kongruensene for alle heltallene t.

Dessuten er disse verdiene for x de *eneste* heltallene som oppfyller begge kongruensene. Dette er ikke så vanskelig å vise, men vi skal ikke gå gjennom det i denne oversikten.

Oppgave 3

Finn et heltall x slik at:

(1) $0 \leq x < 66$;

(2) $x \equiv 2 \pmod 6$;

(3) $x \equiv 3 \pmod{11}$.

Hvordan løse oppgaven?

Finn først et hvilket som helst heltall x som oppfyller disse to kongruensene, som i Oppgave 1. Vi får: $x = 146$.

Hva gjør jeg da?

Finn en verdi av t slik at $0 \leq 146 + 66t < 66$. La x være $146 + 66t$ for denne verdien av t.

Konklusjon

La x være $146 + 66 \cdot (-2) = 14$.

Hvorfor virker metoden?

Vi vet fra Oppgave 2 at alle heltallene x slik at (2) og (3) er sanne er:

$$x = 146 + 66t,$$

hvor t er et heltall. Det finnes alltid akkurat ett av disse slik at $0 \leq x < 66$.

Oppgave 4

Finn et heltall/alle heltallene x slik at:

(1) vi får 2 som rest når vi deler x med 6;

(2) vi får 3 som rest når vi deler x med 11.

Hvordan løse oppgaven?

Oversett til modulær aritmetikk. Da blir oppgaven den samme som Oppgave 1/Oppgave 2.

At $0 \leq x < 66$ kan også kreves. Når vi oversetter til modulær aritmetikk, blir oppgaven da den samme som Oppgave 3.

Oppgave 5

Finn et heltall x slik at:

(1) $x \equiv 2 \pmod 6$;

(2) $x \equiv 3 \pmod{11}$.

(3) $x \equiv 4 \pmod{13}$.

Hvordan løse oppgaven?

Finn først et heltall x som oppfyller de første to kongruensene, som i Oppgave 1. Vi får: $x = 146$.

Hva gjør jeg da?

Benytt dette heltallet for å sette opp en ny kongruens:

$$x \equiv 146 \pmod{6 \cdot 11},$$

altså

$$x \equiv 146 \pmod{66}.$$

Finn nå et heltall x slik at:

(1) $x \equiv 146 \pmod{66}$;

(2) $x \equiv 4 \pmod{13}$.

Det vil si: vi finner et heltall x som oppfyller den nye kongruensen vi har satt opp og den tredje av våre opprinnelige kongruenser.

Hvordan gjøre jeg det?

Akkurat som i Oppgave 1. Husk å sjekke om $\mathsf{sfd}(66, 13) = 1$.

Dermed

Vi løser kongruensene

$$13x \equiv 1 \pmod{66}$$

og

$$66x \equiv 1 \pmod{13}$$

hver for seg.

Når heltallene begynner vi blir store, blir det vanskelig å komme fort fram til en løsning ved å gjette og eksperimentere løsning, så vi kommer oftest til å trenge Euklids algoritme.

Konklusjon

Hvis vi følger metoden, kommer vi fram til at

$$x = 13 \cdot 61 \cdot 146 + 66 \cdot 1 \cdot 4,$$

altså

$$x = 116042,$$

oppfyller begge kongruensene.

Ikke bekmyr deg om du får et veldig stort heltall

Som vi ser her, blir oftest x veldig stort. Husk å sjekke om heltallet du får oppfyller alle de tre kongruensene i oppgaven.

Hvorfor virker metoden?

Vi vet fra Oppgave 2 at et heltall x oppfyller både (1) og (2) om og bare om det finnes et heltall t slik at $x = 146 + 66t$. Dette er det samme som å si:

$$x \equiv 146 \pmod{66}.$$

For å finne et heltall som oppfyller både (1), (2), og (3), er det derfor nok å finne et heltall som oppfyller både denne nye kongruensen og (3).

Oppgave 6

Finn alle heltallene x slik at:

(1) $x \equiv 2 \pmod{6}$;

(2) $x \equiv 3 \pmod{11}$.

(3) $x \equiv 4 \pmod{13}$.

Hvordan løse oppgaven?

Finn først ett heltall x som oppfyller de tre kongruensene, som i Oppgave 5. Vi får: $x = 116042$.

Hva gjør jeg da?

Gang de tre heltallene vi jobber modulo: $6 \cdot 11 \cdot 13 = 858$.

Konklusjon

Alle løsningene: $x = 116042 + 858t$, hvor t er et hvilket som helst heltall.

Hvorfor virker metoden?

Vi vet fra Oppgave 2 at et heltall x oppfyller både (1) og (2) om og bare om det finnes et heltall t slik at $x = 146 + 66t$. Dette er det samme som å si:

$$x \equiv 146 \pmod{66}.$$

For å finne alle heltallene som oppfyller både (1), (2), og (3), er det derfor nok å finne alle heltallene som oppfyller både denne nye kongruensen og (3).

Oppgave 7

Finn et heltall x slik at:

(1) $0 \leq x < 858$;

(2) $x \equiv 2 \pmod 6$;

(3) $x \equiv 3 \pmod{11}$;

(4) $x \equiv 4 \pmod{13}$.

Hvordan løse oppgaven?

Finn først et hvilket som helst heltall x som oppfyller disse tre kongruensene, som i Oppgave 5. Vi får: $x = 116042$.

Hva gjør jeg da?

Finn en verdi av t slik at $0 \leq 116042 + 858t < 858$. La x være $116042 + 858t$ for denne verdien av t.

Konklusjon

La x være $116042 + 858 \cdot (-135) = 212$.

Hvorfor virker metoden?

Vi vet fra Oppgave 6 at alle heltallene x slik at (2) – (4) er sanne er:

$$x = 116042 + 858t,$$

hvor t er et heltall. Det finnes alltid akkurat ett av disse slik at $0 \leq x < 858$.

Oppgave 8

Finn et heltall/alle heltallene x slik at:

(1) vi får 2 som rest når vi deler x med 6;

(2) vi får 3 som rest når vi deler x med 11;

(3) vi får 4 som rest når vi deler x med 13.

Hvordan løse oppgaven?

Oversett til modulær aritmetikk. Da blir oppgaven den samme som Oppgave 5/Oppgave 6.

At $0 \leq x < 858$ kan også kreves. Når vi oversetter til modulær aritmetikk, blir oppgaven da den samme som Oppgave 7.

Oppgave 9

Finn et heltall slik at:

(1) $x \equiv 2 \pmod 6$;

(2) $x \equiv 3 \pmod{11}$;

(3) $x \equiv 4 \pmod{13}$;

(4) $x \equiv 5 \pmod{17}$.

Hvordan løse oppgaven?

Finn først et heltall som oppyfyller (1) – (3), som i Oppgave 5. Vi får: $x = 116042$.

Hva gjør jeg da?

Benytt dette heltallet for å sette opp en ny kongruens:

$$x \equiv 116042 \pmod{6 \cdot 11 \cdot 13},$$

altså

$$x \equiv 116042 \pmod{858}.$$

Finn nå et heltall x slik at:

(1) $x \equiv 1116042 \pmod{858}$;

(2) $x \equiv 5 \pmod{17}$.

Det vil si: vi finner et heltall x som oppfyller den nye kongruensen vi har satt opp og den fjerde av våre opprinnelige kongruenser.

Videre

Forhåpentligvis er det klart hvordan fullføre oppgaven, og å løse ligner oppgaver som ber om å finne alle heltallene som oppfyller fire kongruenser, osv.

I tillegg er det forhåpentligvis klart hvordan metoden kan tilpasses for å finne et heltall/alle heltallene som oppfyller fem eller flere kongruenser.

Poenget

Det er nok å kunne løse et par kongruenser for å løse et hvilket som helst antall kongruenser. Etter at vi har løst et par kongruenser, setter vi opp en ny kongruens for å oppsummere det vi har kommet fram til.

Hvor finner jeg teorien for det kinesiske restteoremet i forelesningsnotatene?

Proposisjon 5.7.2 og eksemplene som følger den.