Hvordan bruke kalkulatoren i modulær aritmetikk

Richard Williamson

3. desember 2014

Eksempel

Erstatt 12637 med et heltall x slik at

$$x \equiv 12637 \pmod{346}$$

og $0 \leq x < 346$.

Når trenger jeg å gjøre dette?

Veldig ofte! For eksempel trenger vi alltid å gjøre det når vi regner ut Legendresymboler, og når vi krypterer og dekrypterer ved å benytte RSA-algoritmen.

Det er avgjørende at du får dette til.

Hvordan gjør jeg det?

Bruk kalkulatoren din som følger.

(1) Del 12637 med 346, slik at du får en desimal: med tre desimaler, får vi 36,523.

(2) Gang heltallet til venstre for desimalkommaet, 36 i dette tilfellet, med 346. Vi får: $36 \cdot 346 = 12456$.

(3) Trekk heltallet vi fikk i (2) fra 12637. Vi får: $12637 - 12456 = 181$.

Konklusjon

$12637 \equiv 181 \pmod{346}$

Øv deg på dette!

Dette er noe du må kunne gjøre fort og uten feil! Du kan øve deg på det ved å løse repetisjonsoppgavene om Legendresymboler og kryptografi.

Vær forsiktig!

Med noen kalkulatorer må du trykke en knapp til for å få en desimal etter å ha delt. Vær forsiktig å trykke på den riktige knappen: hvis du får 0 til venstre for desimalkommaet, har du ikke trykt på den riktige knappen!

Virker dette alltid?

Ja, så lenge at heltallet vi deler ikke er for stort for kalkulatoren din. Dette skjer ofte når vi har store potenser, som i oppgaver om kryptografi. I dette tilfellet er metoden vi har sett på her fortsatt relevant, men vi må jobbe litt hardere: vi må dele den store potensen opp i mindre potenser som vi *kan* regne ut ved hjelp av kalkulatoreni som her. Se oversikten over kryptografi for hvordan gjøre dette.