# Oversikt over bevis at det finnes uendelig mange primtall med bestemte egenskaper

Richard Williamson

3. desember 2014

## Oppgave 1

La $n$ være et naturlig tall. Bevis at det finnes et primtall $p$ slik at $p > n$ og $p \equiv 3 \pmod 4$. *Tips*: La $q$ være produktet til alle primtallene som er mindre enn eller like $n$, og som er kongruent til 3 modulo 4. Benytt en primtallsfaktorisering til $4q - 1$.

## Hvordan løse oppgaven?

Begynnelsen og slutten på en slik oppgave er alltid den samme. Vi begynner med å benytte oss av aritmetikkens fundamentalteorem: det finnes en primtallsfaktorisering til $4q - 1$. Det vil si: det finnes et naturlig tall $t$ og primtall $p_1, p_2, \ldots, p_t$ slik at

$$4q - 1 = p_1 p_2 \cdots p_t.$$

Nå ønsker vi å bevise at minst ett av primtallene $p_1, p_2, \ldots, p_t$ har det samme egenskapet som står i oppgaven, altså at minst ett av primtallene $p_1, p_2, \ldots, p_t$ er kongruent til 3 modulo 4.

## Hvorfor kan vi fullføre beviset gitt at dette er sant?

La oss anta at $p_i$ har det samme egenskapet som står i oppgaven, altså at

$$p_i \equiv 3 \pmod 4.$$

Vi gjennomfører følgende argument for å vise at $p_i > n$, som i alt vesentlig er det samme når vi løser en hvilken som helst lignende oppgave.

(1) Anta at $p_i \leq n$. Vi ønsker å vise at dette fører til en motsigelse.

(2) Siden $p_i$ har det samme egenskapet som står i oppgaven, er $p_i$ et ledd av $q$. Derfor har vi: $p_i \mid q$.

(3) Siden $p_i$ er i tillegg et ledd av primtallsfaktoriseringen til $4q-1$, har vi i tillegg: $p_i \mid 4q-1$.

(4) Vi benytter (2) og (3) for å vise at $p_i \mid 1$. Vi kan for eksempel observere at det følger fra (2) at $p_i \mid 4q$, og at det følger fra (3) at $p_i \mid -(4q-1)$. Da følger det at

$$p_i \mid 4q + (-(4q-1)),$$

altså at $p_i \mid 1$.

(5) Nå observere vi at vi har en motsigelse: siden $p_i \mid 1$, er $p_i \leq 1$, men siden $p_i$ er et primtall, er $p_i \geq 2$.

Siden antakelsen at $p_i \leq n$ fører til en motsigelse, konkluderer vi at det ikke er sant at $p_i \leq n$, altså at $p_i > n$.

## Hvordan kan jeg bli fortrolig med dette argumentet?

Prøv å gjennomføre det i alle de seks eksemplene på påstand som ligner på Oppgave 1 som vi har sett i kurset.

(1) Benytt en primtallsfaktorisering til uttrykket som er relevant, $4q-1$ i dette tilfellet.

(2) Anta at det kan vises at minst ett av primtallene i denne primtallsfaktorisering har det samme egenskapet som primtallene påstanden handler om.

(3) Anta at dette primtallet er mindre enn er likt $n$. Vis da at vi får en motsigelse på en lignende måte som ovenfor.

(4) Konkluder at dette primtallet er større enn $n$.

Hvis en slik oppgave dukker opp på eksamen, blir du gitt en god del av poengene om du kan begynne og avslutte beviset riktig på denne måten.

## Hvordan kommer jeg fram til det riktige utsagnet å se på?

Det riktige utsagnet, $4q-1$ i dette tilfellet, er ikke lett å gjette i det hele tatt. Det blir alltid gitt som et tips i oppgaven.

## Hvordan gjennomføre jeg midten av beviset?

Det vil si: hvordan kan det vises at minst ett primtallene i en primtallsfaktorisering til uttrykket vi jobber med, $4q-1$ i dette tilfellet, har det samme egenskapet som står i oppgaven? Det finnes ingen generell oppskrift, men noen typer argumenter er ofte relevant.

## Hva er disse?

Når vi har et uttrykk som er lineær, som $4q - 1$ her, pleier vi å dele i tilfeller modulo koeffisienten til $q$: hvert av primtallene $p_i$ i primtallsfaktoriseringen til $4q-1$ er kongruent til 0, 1, 2, eller 3 modulo 4. Dette er ikke noe dypt: det sier egentlig at vi får 0, 1, 2, eller 3 som rest når vi deler $p_i$ med 4.

Først viser vi at det er umulig at $p_i \equiv 0 \pmod 4$, og i tillegg umulig at $p_i$ er kongruent til et hvilket som helst av mulighetene $r$ slik at $\mathsf{sfd}(4, r) \neq 1$, nemlig 2 i dette tilfellet.

## Hvordan viser jeg dette?

Dersom $p_i \equiv 0 \pmod 4$, har vi: $4 \mid p_i$. Dette er umulig siden $p_i$ er et primtall.

Dersom $p_i \equiv 2 \pmod 4$, har vi:

$$p_i \equiv 0 \pmod 2.$$

Siden $p_i$ er ett ledd av primtallsfaktoriseringen til $4q - 1$, er da

$$4q - 1 \equiv 0 \pmod 2.$$

Siden

$$4 \equiv 0 \pmod 2,$$

er imidlertid

$$4q - 1 \equiv -1 \pmod 2,$$

altså er

$$4q - 1 \equiv 1 \pmod 2.$$

Dermed er både

$$4q - 1 \equiv 0 \pmod 2$$

og

$$4q - 1 \equiv 1 \pmod 2.$$

Siden det ikke er sant at $0 \equiv 1 \pmod 2$, er dette umulig.

### Hva gjør jeg da?

Siden det er umulig at $p_i \equiv 0 \pmod 4$ eller $p_i \equiv 2 \pmod 4$, er enten $p_i \equiv 1 \pmod 4$ eller $p_i \equiv 3 \pmod 4$. Husk nå at målet er å vise at minst ett av primtallene $p_1, p_2, \ldots, p_t$ er kongruent til 3 modulo 4.

Hvordan kan dette *ikke* være sant? Siden enten $p_i \equiv 1 \pmod 4$ eller $p_i \equiv 3 \pmod 4$ for alle primtallene $p_1, p_2, \ldots, p_t$, er den eneste muligheten: $p_i \equiv 1 \pmod 4$ for alle primtallene $p_1, p_2, \ldots, p_t$.

For å vise at minst ett av primtallene $p_1, p_2, \ldots, p_t$ er kongruent til 3 modulo 4, er det derfor nok å vise at det er umulig at alle er kongruent til 1 modulo 4.

Logikken er litt subtil her! Gå gjennom argumentet flere ganger, til du blir fortrolig med det.

## Hvordan gjør jeg det?

Anta at $p_i \equiv 1 \pmod 4$ for alle primtallene $p_1, p_2, \ldots, p_t$. Da er

$$p_1 p_2 \cdots p_t \equiv \underbrace{1 \cdot 1 \cdots 1}_{t \text{ ganger}} = 1 \pmod 4.$$

Dermed er

$$4q - 1 \equiv 1 \pmod 4.$$

Siden $4 \equiv 0 \pmod 4$, er imidlertid

$$4q - 1 \equiv -1 \pmod 4,$$

altså er

$$4q - 1 \equiv 3 \pmod 4.$$

Dermed er både

$$4q - 1 \equiv 1 \pmod 4$$

og

$$4q - 1 \equiv 3 \pmod 4.$$

Det er ikke sant at

$$0 \equiv 3 \pmod 4.$$

## Konklusjon

Vi konkluderer at minst ett av primtallene $p_1, p_2, \ldots, p_t$ er kongruent til 3 modulo 4. Vi har rukket målet!

## Hvordan kan je bli fortrolig med dette argumentet?

Prøv å vise at at minst ett av primtallene i en primtallsfaktorisering til $6q-1$ er kongruent til 5 modulo 6.

(1) Vi at hvert primtall i primtallsfaktoriseringen til $6q - 1$ er kongruent enten til 1 modulo 6 eller til 5 modulo 6, ved å vise at det er umulig at primtallet er kongruent til 0, 2, 3, eller 4 modulo 6.

(2) Vis at det er umulig at alle primtallene i primtallsfaktoriseringen til $6q - 1$ er kongruent til 1 modulo 6.

### Oppsummering

Et svar på Oppgave 1 har tre deler.

(1) Begynnelsen: benytt en primtallsfaktorisering til $4q - 1$.

(2) Midten: vis at minst ett av primtallene i denne primtallsfaktoriseringen har det samme egenskapet som står i oppgaven, det vil si er kongruent til 3 modulo 4.

(3) Slutten: anta at dette primtallet er mindre enn eller likt $n$, og vis at vi da får en motsigelse. Konkluder at dette primtallet er større enn $n$.

Et svar på en hvilken som helst oppgave som ligner på Oppgave 1 har de samme tre delene. Delene (1) og (3) er kan gjennomføres på nesten den samme måten i alle slike oppgaver.

Det er (2) som må tilpasses hver gang: hvis du ikke får dette steget til, er det helt fint på eksamen å anta at det kan vises, og forklare hvordan beviset kan fullføres deretter.

## Oppgave 2

La $n$ være et naturlig tall. Bevis at det finnes et primtall $p$ slik at $p > n$ og $p \equiv 7 \pmod 8$. *Tips*: La $q$ være produktet til alle primtallene som er mindre enn eller like $n$, og som er kongruent til 7 modulo 8. Benytt en primtallsfaktorisering til $8q^2 - 1$. Benytt i tillegg at, dersom et primtall deler $8q^2 - 1$, deler det også $(4q)^2 - 2$, og forklar hvorfor dette er sant.

### Hvordan løse oppgaven?

Som nevnt ovenfor, kan begynnelsen og slutten på oppgaven gjennomføres som i svaret på Oppgave 1 ovenfor. Målet midten på beviset er å vise at det finnes minst ett primtall i primtallsfaktoriseringen

$$p_1 p_2 \cdots p_t$$

til $8q^2 - 1$ som er kongruent til 7 modulo 8.

### Kan jeg ikke gjennomføre det samme argumentet som i Oppgave 1?

Vi trenger et nytt argument. Hvis vi prøver å gjennomføre et argument som ligner på argumentet vi ga for å svare på Oppgave 1, har vi et problem: vi kan ikke vise at det er umulig at

$$p_i \equiv 3 \pmod 8$$

eller

$$p_i \equiv 5 \pmod 8.$$

## Hva gjør jeg da?

Vi trenger et nytt argument. Idéen er å benytte kvadratisk gjensidighet som følger.

(1) Siden $p_i$ er et ledd av primtallsfaktoriseringen til $8q^2 - 1$, har vi:

$$p_i \mid 8q^2 - 1.$$

Som tipset i oppgaven foreslår, har vi da:

$$p_i \mid (4q)^2 - 2,$$

siden

$$(4q)^2 - 2 = 16q^2 - 2 = 2\left(8q^2 - 1\right).$$

Da er

$$(4q)^2 - 2 \equiv 0 \pmod{p_i},$$

altså er

$$(4q)^2 \equiv 2 \pmod{p_i}.$$

Dermed er 2 en kvadratisk rest modulo $p_i$, altså er $\mathbb{L}_{p_i}^2 = 1$.

(2) Ut ifra regel (F) i oversikten over Legendresymboler og kvadratiske kongruenser, er da

$$p_i \equiv 1 \pmod{8}$$

eller

$$p_i \equiv 7 \pmod{8}.$$

Husk nå at målet er å vise at minst ett av primtallene $p_1, p_2, \ldots, p_t$ er kongruent til 7 modulo 8. Vi kan gjøre dette ved å gjennomføre akkurat det samme argumentet som i svaret vårt på Oppgave 1. Logikken er som følger.

Hvordan kan det *ikke* være sant at minst ett av primtallene $p_1, p_2, \ldots, p_t$ er kongruent til 7 modulo 8? Siden enten

$$p_i \equiv 1 \pmod{8}$$

eller

$$p_i \equiv 7 \pmod{8}$$

for alle primtallene $p_1, p_2, \ldots, p_t$, er den eneste muligheten:

$$p_i \equiv 1 \pmod{8}$$

for alle primtallene $p_1, p_2, \ldots, p_t$.

For å vise at minst ett av primtallene $p_1, p_2, \ldots, p_t$ er kongruent til 7 modulo 8, er det derfor nok å vise at det er umulig at alle er kongruent til 1 modulo 8. Vi gjør dette akkurat som i svaret på Oppgave 1.

## Vi må være forsiktig!

For å kunne benytte regel (F) i oversikten over Legendresymboler og kvadratiske kongruenser som ovenfor, må vi har: $p_i > 2$. For å kunne gjennomføre argumentet ovenfor, må vi derfor vise at det er sant at $p_i > 2$.

Dette kan gjøres som i svaret på Oppgave 1. Siden $p_i$ er et ledd av primtallsfaktoriseringen til $8q^2 - 1$, har vi: $p_i \mid 8q^2 - 1$. Dersom $p_i = 2$, har vi da: $2 \mid 8q^2 - 1$, altså

$$8q^2 - 1 \equiv 0 \pmod{2}.$$

Vi kan vise at dette er umulig akkurat i svaret vårt på Oppgave 1, ved å benytte at

$$8 \equiv 0 \pmod{2}.$$

## Oppsummering

Et svar på Oppgave 2 har samme tre deler som et svar på Oppgave 1.

(1) Begynnelsen: benytt en primtallsfaktorisering til $8q^2 - 1$.

(2) Midten: vis at minst ett av primtallene i denne primtallsfaktoriseringen har det samme egenskapet som står i oppgaven, det vil si er kongruent til 7 modulo 8.

(3) Slutten: anta at dette primtallet er mindre enn eller likt $n$, og vis at vi da får en motsigelse. Konkluder at dette primtallet er større enn $n$.

For å gjennomføre (2), benytte vi et dypt regel om Legendresymboler i tillegg til noen av argumentene vi benytt oss av i svaret vårt på Oppgave 1. For å kunne gjøre dette, er det typisk nødvendig å vise at ingen av primtallene i primtallsfaktoriseringen er lik 2.

Et svar på en hvilken som helst oppgave som ligner på Oppgave 2, hvor uttrykket vi ser på, $8q^2 - 1$ i dette tilfellet, er kvadratisk, kan gjennomføres på denne måten. Vi benytter enten ett av reglene om Legendresymboler, eller noe som følger fra disse, som du blir bedt om å vise tidligere i oppgaven.

## Hvordan kan jeg bli fortrolig med argumentet?

Prøv æ vise at minst ett av primtallene, faktisk alle primtallene, i en primtallsfaktorisering til $(2q)^2 + 1$ er kongruent til 1 modulo 4.

(1) Vis at $p_1$ ikke er lik 2.

(2) Observer at det følger at $\mathbb{L}_{p_1}^{-1} = 1$. Benytt da regel (E) i oversikten over Legendresymboler og kvadratiske kongruenser for å få at

$$p_1 \equiv 1 \pmod{4}.$$

Det er ikke noe spesielt med $p_1$ her: argumentet kan gjennomføres for hvert $p_i$.