Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA1301 Tallteori
Høst 2020

Løsningsforslag — Øving 4

3.3.2 **a)**

Et vilkårlig tvillingprimtallspar kan skrives som p og $p+2$. Hvis vi legger 1 til produktet av dem får vi

$$p(p+2)+1 = p^2+2p+1 = (p+1)^2,$$

som er et kvadrattall.

b)

Siden alle tvillingprimtall er odde, kan vi skrive $p = 2k+1$ og $p+2 = 2k+3$ for en $k \in \mathbb{Z}$. Dermed blir summen

$$(2k+1)+(2k+3) = 4k+4 = 4(k+1).$$

Dette er åpenbart delelig på 4. For å se at det også er delelig på 3, observer at ett av tallene $(2k+1)$, $(2k+2)$ og $(2k+3)$ må være delelig på 3 (siden ett av tre etterfølgende tall må være delelig på 3). Verken $(2k+1)$ eller $(2k+3)$ kan være delelig på 3, siden de begge er primtall. Derfor må $(2k+2)$ være delelig på 3. Dette kan skrives som $(2k+2) = 2(k+1)$, og siden 2 åpenbart ikke er delelig på 3, må $(k+1)$ være delelig på 3.

Dette betyr at $4(k+1)$ er delelig på både 3 og 4, og derfor er det delelig på $\text{lcm}(3,4) = 12$.

3.3.14 Vi skal finne et primtall på formen $4n+3$ som deler

$$N = 4(3\cdot 7\cdot 11)-1 = 923.$$

Fra konstruksjonen av N ser vi at ingen av primtallene $2, 3, 7, 11$ vil dele N, og det er åpenbart at $5 \nmid N$. Vi prøver å dele N på det neste primtallet, nemlig 13, og får $923/13 = 71$. Siden $71 = 4\cdot 17+3$ er vi i mål.

La oss se på

$$N = 4(3\cdot 7\cdot 11\cdot 15)-1 = 13859$$

Vi finner ut (f.eks. ved å prøve å dele på alle primtallene $p \le \sqrt{13859} \approx 117.7$) at 13859 er et primtall, og det er på den ønskede formen, siden $13859 = 4\cdot 3464+3$.

For tilleggsdelen til oppgaven, la $N = 4m+3$ for $m \in \mathbb{Z}$. Vi ønsker å vise at N er delelig på et primtall på formen $4n+3$. La $N = p_1\cdot\ldots\cdot p_t$ være primtallsfaktoriseringen til N. Siden N er et oddetall er det ikke delelig på 2, så $p_i \neq 2$ for alle i. Det betyr at

hver faktor p_i enten er på formen $4k_i + 1$ eller $4k_i + 3$ for $k_i \in \mathbb{Z}$. Hvis alle faktorene er på formen $p_i = 4k_i + 1$ vil produktet av dem også være på den formen (se lemmaet før teorem 3.6 i Burton), og produktet av dem er N. Altså vil N være på formen $4k + 1$. Men vi har antatt at $N = 4m + 3$, så det er ikke mulig. Dermed må minst én av primtallsfaktorene til N være på formen $p_i = 4n + 3$. Per definisjon vil $p_i \mid N$, og med andre ord betyr det at $4n + 3 \mid 4m + 3$. Så $4m + 1$ er delelig på et primtall på formen $4n + 3$, og vi er i mål.

4.2.1 **a)**

Siden $m \mid n$ finnes en $k \in \mathbb{Z}$ slik at $n = km$. Per definisjon betyr $a \equiv b \pmod{n}$ at n deler $a - b$, det vil si $a - b = ln$ for en $l \in \mathbb{Z}$. Til sammen gir dette at

$$a - b = ln = l(km) = (lk)m,$$

som betyr at m deler $a - b$. Dermed er $a \equiv b \pmod{m}$.

b)

Igjen har vi fra definisjonen av kongruens at $a - b = kn$, for en $k \in \mathbb{Z}$.Vi ganger med c, og får

$$ca - cb = ckn = k(cn),$$

som viser at cn deler $ca - cb$, og følgelig at $ca \equiv cb \pmod{cn}$.

c)

Igjen gir $a \equiv b \pmod{n}$ at $a - b = kn$ for en $k \in \mathbb{Z}$. Dersom d deler a, b og d, så vil $\frac{a}{d}$, $\frac{b}{d}$ og $\frac{n}{d}$ være heltall. Det betyr at vi kan skrive $a = d \cdot \frac{a}{d}$, $b = d \cdot \frac{b}{d}$ og $n = d \cdot \frac{n}{d}$. Dermed kan vi skrive om

$$a - b = d \cdot \frac{a}{d} - d \cdot \frac{b}{d} = d\left(\frac{a}{d} - \frac{b}{d}\right),$$
$$kn = k\left(d \cdot \frac{n}{d}\right) = d\left(k \cdot \frac{n}{d}\right).$$

Dette gjør at vi kan skrive likheten $a - b = kn$ som $d(\frac{a}{d} - \frac{b}{d}) = d(k \cdot \frac{n}{d})$, og så stryke d fra begge sidene. Da står vi igjen med $\frac{a}{d} - \frac{b}{d} = k \cdot \frac{n}{d}$, som betyr at $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

4.2.2 Moteksempel: $1^2 \equiv 2^2 \pmod 3$, men $1 \not\equiv 2 \pmod 3$.

4.2.5 Vi prøver oss fram, og finner at $53^2 \equiv 1 \pmod{39}$ og $103^2 \equiv 1 \pmod{39}$. Dermed kan vi skrive om uttrykket

$$\begin{aligned} 53^{103} + 103^{53} &= 53(53^2)^{51} + 103(103^2)^{26} \\ &\equiv 53 \cdot 1^{51} + 103 \cdot 1^{26} \pmod{39} \\ &= 53 + 103 \\ &= 156 \\ &\equiv 0 \pmod{39}. \end{aligned}$$

La oss nå se på $111^{333} + 333^{111}$. Vi begynner med å observere at $111 \equiv -1 \pmod 7$ og ved å gange med 3 ser vi at $333 \equiv -3 \pmod 7$. Dette gir at $111^2 \equiv 1 \pmod 7$, og at $333^3 \equiv (-3)^3 \equiv -27 \equiv 1 \pmod 7$. Dermed kan vi skrive om uttrykket

$$\begin{aligned} 111^{333} + 333^{111} &= 111(111^2)^{166} + (333^3)^{37} \\ &\equiv 111 \cdot 1^{166} + 1^{37} \pmod 7 \\ &= 111 + 1 \\ &\equiv 0 \pmod 7 \end{aligned}$$

Eksamen H2012 oppg. 6 Vi følger hintet, og prøver å løse ligningen modulo 5. Vi begynner med å undersøke hva n^2 kan være modulo 5:

$$\begin{aligned} n \equiv 0 \pmod 5 \quad &\Longrightarrow \quad n^2 \equiv 0^2 \equiv 0 \pmod 5 \\ n \equiv 1 \pmod 5 \quad &\Longrightarrow \quad n^2 \equiv 1^2 \equiv 1 \pmod 5 \\ n \equiv 2 \pmod 5 \quad &\Longrightarrow \quad n^2 \equiv 2^2 \equiv -1 \pmod 5 \\ n \equiv 3 \pmod 5 \quad &\Longrightarrow \quad n^2 \equiv 3^2 \equiv -1 \pmod 5 \\ n \equiv 4 \pmod 5 \quad &\Longrightarrow \quad n^2 \equiv 4^2 \equiv 1 \pmod 5 \end{aligned}$$

Dette betyr at $n^2 + 2$ er kongruent med enten 1, 2 eller 3 modulo 5. Fra dette ser vi også at $m^4 \equiv 1 \pmod 5$ for alle $m \not\equiv 0 \pmod 5$, siden $(-1)^2 = 1^2 = 1$. Det betyr at for alle $m \in \mathbb{Z}$ så er enten $m \equiv 0 \pmod 5$ eller så er $m^4 - 1 \equiv 0 \pmod 5$. Dermed vil $m^5 - m = m(m^4 - 1) \equiv 0 \pmod 5$ for alle $m \in \mathbb{Z}$. Til sammen betyr dette at

$$m^5 - m \not\equiv n^2 + 2 \pmod 5,$$

uansett hva m og n er.

Eksamen H2014 oppg. 6 **a)**

De første fem primtallene p som oppfyller $p \equiv 2 \pmod 3$ er:

$$2,\ 5,\ 11,\ 17,\ 23$$

b)

La q være produktet av alle de primtallene som er mindre enn eller lik n, og som er kongruent med 2 modulo 3. Ut ifra aritmetikkens fundamentalteorem finnes det et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at

$$3q - 1 = p_1 \cdots p_t.$$

For hvert naturlige tall i slik at $i \leq t$ er ett av følgende sant:

(1) $p_i \equiv 0 \pmod 3$
(2) $p_i \equiv 1 \pmod 3$
(3) $p_i \equiv 2 \pmod 3$

Anta at det finnes et naturlig tall i slik at (1) er sant. Da vil $3 \mid p_i$, og siden p_i er et primtall må $p_i = 3$. Siden p_i er en faktor i $3q - 1$ betyr det at $3 \mid 3q - 1$, som gir at

$$3q - 1 \equiv 0 \pmod{3}.$$

Imidlertid er

$$3q - 1 \equiv -1 \equiv 2 \pmod{3},$$

og siden det ikke kan være begge samtidig (siden $1 \not\equiv 2 \pmod{3}$), må antakelsen være usann. Antakelsen vi gjorde her var at det finnes et naturlig tall i slik at $p_i \equiv 0 \pmod{3}$, og siden det ikke stemmer må p_i være kongruent med 1 eller 2 modulo 3 for alle i. Derfor er ett av følgende sant:

(A) For alle de naturlige tallene i slik at $i \leq t$, er

$$p_i \equiv 1 \pmod{3}.$$

(B) Det finnes minst ett naturlig tall i slik at $i \leq t$ og

$$p_i \equiv 2 \pmod{3}.$$

Anta at (A) er sant. Da er

$$3q - 1 = p_1 \cdots p_t \equiv \underbrace{1 \cdot 1 \cdots 1}_{t \text{ ganger}} = 1 \pmod{3},$$

altså

$$3q - 1 \equiv 1 \pmod{3}.$$

På samme måte som over kan heller ikke dette være sant, siden $3k - 1 \equiv 2 \pmod{3}$. Dermed er antakelsen at (A) stemmer usann, som betyr at (B) må være sann. Altså finnes det et naturlig tall $i \leq t$ slik at

$$p_i \equiv 2 \pmod{3}.$$

Det som gjenstår er å vise at $p_i > n$. Anta at $p_i \leq n$. Per konstruksjon er tallet q produktet av alle primtall $p \leq n$ på formen $p \equiv 2 \pmod{3}$. Dermed vil p_i være en faktor i q, som betyr at $p_i \mid q$. Men p_i er per definisjon en faktor i $3q - 1$, så vi har også at $p_i \mid 3q - 1$. Dermed vil $p_i \mid 3 \cdot q - (3q - 1)$, altså $p_i \mid 1$. Dette er ikke mulig, siden p_i er et primtall, som betyr at $p_i > 1$. Følgelig må $p_i > n$

Vi konkluderer med at p_i er et primtall somer større enn n, slik at $p_i \equiv 2 \pmod{3}$.

c)

De primtallene som er mindre enn 14 og som er kongruent med 2 modulo 3 er 2, 5 og 11. Vi regner ut $3 \cdot (2 \cdot 5 \cdot 11) = 329$, og finner primtallsfaktoriseringen $329 = 7 \cdot 47$. Siden $47 = 3 \cdot 15 + 2$ er 47 et primtall på riktig form, så vi får $p = 47$.

Eksamen K2017 oppg. 3 Vi skal finne der minste naturlige tallet n slik at $n \equiv 21^{547} \pmod{80}$. Vi begynner med å prøve å finne en potens av 21 som er kongruent med 1 modulo 80:

$$21^2 = 441 \equiv 41 \pmod{80}$$
$$21^3 = 21 \cdot 41 = 861 \equiv 61 \pmod{80}$$
$$21^4 = 21 \cdot 61 = 1281 \equiv 1 \pmod{80}$$

Dermed får vi at

$$21^{547} = 21^{4 \cdot 136 + 3} = 21^3 \cdot (21^4)^1 36 \equiv 61 \cdot 1^1 36 = 61 \pmod{80}$$

Altså er 61 det minste naturlige tallet som er kongruent med 2^{547} modulo 80.

Merknad: denne oppgaven kan også løses ved bruk av Eulers teorem, som vi kommer til senere i pensum.