Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA1301 Tallteori
Høst 2020

Løsningsforslag — Øving 9

7.2.4a) Dersom n er et oddetall, så er $\gcd(2, n) = 1$. Det betyr, siden ϕ er en multiplikativ funksjon, at $\phi(2n) = \phi(2)\phi(n) = (2-1)\phi(n) = \phi(n)$.

7.2.4b) Dersom n er et partall kan det faktoriseres som $2^k m$, hvor $\gcd(2, m) = 1$. Dermed er $\phi(n) = \phi(2^k)\phi(m) = (2^k - 2^{k-1})\phi(m) = 2^{k-1}\phi(m)$. Legg nå merke til at vi kan skrive $2n = 2^{k+1}m$, og dermed kan vi regne ut

$$\phi(2n) = \phi(2^{k+1})\phi(m) = (2^{k+1} - 2^k)\phi(m) = 2^k\phi(m) = 2(2^{k-1}\phi(m)) = 2\phi(n)$$

7.2.7a) Vi skal vise at for alle positive heltall n er $\frac{1}{2}\sqrt{n} \leq \phi(n) \leq (n)$. Vi følger hintet, og skriver n primtallsfaktorisert som $n = 2^{k_0}p_1^{k_1}\cdots p_r^{k_r}$, som gir at

$$\phi(n) = 2^{k_0-1}p_1^{k_1-1}\cdots p_r^{k_r-1}(p_1-1)\cdots(p_r-1).$$

Fra hintet har vi også at $\underbrace{p_i - 1 > \sqrt{p_i}}_{(*)}$ og at $\underbrace{k_i - \frac{1}{2} > \frac{k_i}{2}}_{(**)}$ for alle i. Dermed får vi

$$\begin{aligned}
\phi(n) = 2^{k_0-1}p_1^{k_1-1}\cdots p_r^{k_r-1}(p_1-1)\cdots(p_r-1) &\overset{(*)}{\geq} 2^{k_0-1}p_1^{k_1-1}\cdots p_r^{k_r-1}\sqrt{p_1}\cdots\sqrt{p_r} \\
&= 2^{k_0-1}p_1^{k_1-1}p_1^{\frac{1}{2}}\cdots p_r^{k_r-1}p_r^{\frac{1}{2}} \\
&= 2^{k_0-1}p_1^{k_1-\frac{1}{2}}\cdots p_r^{k_r-\frac{1}{2}} \\
&\overset{(**)}{\geq} 2^{k_0-1}p_1^{\frac{k_1}{2}}\cdots p_r^{\frac{k_r}{2}}
\end{aligned}$$

Observer nå at vi kan oppnå $\sqrt{n}$ ved å dele hver eksponent i primtallsfaktoriseringen til n på 2. Dermed får vi at

$$\frac{1}{2}\sqrt{n} = 2^{-1}2^{\frac{k_0}{2}}p_1^{\frac{k_1}{2}}\cdots p_r^{\frac{k_r}{2}} = 2^{\frac{k_0}{2}-1}p_1^{\frac{k_1}{2}}\cdots p_r^{\frac{k_r}{2}} \leq 2^{k_0-1}p_1^{\frac{k_1}{2}}\cdots p_r^{\frac{k_r}{2}} \leq \phi(n),$$

hvor den siste ulikheten kommer fra utregningen over. Med det har vi vist at $\frac{1}{2}\sqrt{n} \leq \phi(n)$. Det er åpenbart at $\phi(n) \leq n$, siden $\phi(n)$ teller antall positive heltall mindre enn eller lik n som er relativt primiske til n, og det totale antallet positive heltall som er mindre enn eller lik n er n.

7.2.13 La n ha primtallsfaktorisering $n = p_1^{k_1} \cdots p_r^{k_r}$. Fra teorem 6.1 i Burton vet vi da at når $d \mid n$ vil d ha primtallsfaktorisering $d = p_1^{a_1} \cdots p_r^{a_r}$, hvor $0 \leq a_i \leq k_i$ for alle i. Vi skal vise at $\phi(d) \mid \phi(n)$, og siden ϕ er en multiplikativ funksjon holder det å se på hvordan den oppfører seg på potenser av primtallsfaktorene. Merk at for noen i kan potensen a_i kan være lik 0, som betyr at $p_i^{a_i} = 1$. Da er $\phi(p_i^{a_i}) = 1$, og det er åpenbart slik at $\phi(p_i^{a_i}) \mid \phi(p_i^{k_i})$. Anta nå at $1 \leq a_i \leq k_i$. Da har vi fra teorem 7.1 i Burton at $\phi(p_i^{a_i}) = p_i^{a_i}(1 - \frac{1}{p_i})$. Teoremet gir også at $\phi(p_i^{k_i}) = p_i^{k_i}(1 - \frac{1}{p_i})$, og siden $a_i \leq k_i$ betyr det at $\phi(p_i^{k_i}) = p_i^{k_i - a_i}\phi(p_i^{a_i})$. Dermed ser vi at $\phi(p_i^{a_i}) \mid \phi(p_i^{a_i})$ for alle i, og siden $\phi(n)$ er en multiplikativ funksjon gir dette at

$$\phi(d) = \phi(p_1^{a_1}) \cdots \phi(p_r^{a_r}) \mid \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) = \phi(n),$$

som var det vi ville vise.

7.3.1a) Vi skal vise at $a^{37} \equiv a \pmod{1729}$, og vi gjør det ved å vise at $1729 \mid (a^{37} - a)$. Vi har at $1729 = 7 \cdot 13 \cdot 19$, og siden hver av dem er primtall holder det å vise at $7 \mid (a^{37} - a)$, $13 \mid (a^{37} - a)$ og $19 \mid (a^{37} - a)$.

Dersom $7 \mid a$ så vil $7 \mid (a^{37} - a)$. Dersom $7 \nmid a$ så er $\gcd(7, a) = 1$, og da gir Eulers teorem at $a^{\phi(7)} \equiv a^6 \equiv 1 \pmod{7}$. Dermed er $a^{36} \equiv 1 \pmod{7}$, som betyr at $7 \mid (a^{36} - 1)$, og følgelig at $7 \mid (a^{37} - a)$.

Dersom $13 \mid a$ så vil $13 \mid (a^{37} - a)$. Dersom $13 \nmid a$ så er $\gcd(13, a) = 1$, og da gir Eulers teorem at $a^{\phi(13)} \equiv a^{12} \equiv 1 \pmod{13}$. Dermed er $a^{36} \equiv 1 \pmod{13}$, som betyr at $13 \mid (a^{36} - 1)$, og følgelig at $13 \mid (a^{37} - a)$.

Dersom $19 \mid a$ så vil $19 \mid (a^{37} - a)$. Dersom $19 \nmid a$ så er $\gcd(19, a) = 1$, og da gir Eulers teorem at $a^{\phi(19)} \equiv a^{18} \equiv 1 \pmod{19}$. Dermed er $a^{36} \equiv 1 \pmod{19}$, som betyr at $19 \mid (a^{36} - 1)$, og følgelig at $19 \mid (a^{37} - a)$.

Vi har nå vist at 7, 13 og 19 deler $(a^{37} - a)$, og siden de er parvis relativt primiske vil produktet av dem også dele $(a^{37} - a)$. Dermed er $a^{37} \equiv a \pmod{1729}$.

7.3.3 Vi skal vise at $(2^{15} - 2^3) \mid (a^{15} - a^3)$ for alle heltall a. Vi bruker at $2^{15} - 2^3 = 5 \cdot 7 \cdot 8 \cdot 9 \cdot 13$, og som i forrige oppgave holder det å vise at $a^{15} - a^3$ er delelig på hver av disse faktorene. Merk at 8 og 9 ikke er primtall, men at Eulers teorem fortsatt fungerer for dem (gitt at de er relativt primiske til a).

$$
\begin{aligned}
&5 \mid a \implies 5 \mid (a^{15} - a^3) \\
&5 \nmid a \overset{\text{Euler}}{\implies} a^{\phi(5)} \equiv a^4 \equiv 1 \pmod{5} \\
&\qquad \implies a^1 2 \equiv 1 \pmod{5} \\
&\qquad \implies 5 \mid a^{12} - 1 \\
&\qquad \implies 5 \mid a^3(a^{12} - 1)
\end{aligned}
$$

$$
\begin{aligned}
&7 \mid a \implies 7 \mid (a^{15} - a^3) \\
&7 \nmid a \overset{\text{Euler}}{\implies} a^{\phi(7)} \equiv a^6 \equiv 1 \pmod{7} \\
&\qquad \implies a^1 2 \equiv 1 \pmod{7} \\
&\qquad \implies 7 \mid a^{12} - 1 \\
&\qquad \implies 7 \mid a^3(a^{12} - 1)
\end{aligned}
$$

$$
\begin{aligned}
&2 \mid a \implies 8 \mid (a^{15} - a^3) \\
&2 \nmid a \overset{\text{Euler}}{\implies} a^{\phi(8)} \equiv a^4 \equiv 1 \pmod 8 \\
&\quad \implies a^1 2 \equiv 1 \pmod 8 \\
&\quad \implies 8 \mid a^{12} - 1 \\
&\quad \implies 8 \mid a^3(a^{12} - 1)
\end{aligned}
\qquad
\begin{aligned}
&3 \mid a \implies 9 \mid (a^{15} - a^3) \\
&3 \nmid a \overset{\text{Euler}}{\implies} a^{\phi(9)} \equiv a^6 \equiv 1 \pmod 9 \\
&\quad \implies a^1 2 \equiv 1 \pmod 9 \\
&\quad \implies 9 \mid a^{12} - 1 \\
&\quad \implies 9 \mid a^3(a^{12} - 1)
\end{aligned}
$$

$$
\begin{aligned}
&13 \mid a \implies 13 \mid (a^{15} - a^3) \\
&13 \nmid a \overset{\text{Euler}}{\implies} a^{\phi(13)} \equiv a^{12} \equiv 1 \pmod{13} \\
&\quad \implies a^1 2 \equiv 1 \pmod{13} \\
&\quad \implies 13 \mid a^{12} - 1 \\
&\quad \implies 13 \mid a^3(a^{12} - 1)
\end{aligned}
$$

Altså vil $5, 7, 8, 9$ og 13 alle dele $a^{15} - a^3$, og følgelig vil $5 \cdot 7 \cdot 8 \cdot 9 \cdot 13 = 2^{15} - 2^3 \mid (a^{15} - a^3)$.

7.3.7 Vi regner først ut $\phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$. Siden $\gcd(3, 10) = 1$ gir Eulers teorem at $3^{\phi(10)} \equiv 3^4 \equiv 1 \pmod{10}$. Dette bruker vi til å regne ut at

$$3^{100} \equiv (3^4)^{25} \equiv 1^{25} \equiv 1 \pmod{10}$$

Altså er sifferet på enerplassen i 3^{100} lik 1.

Eksamen H2019 oppgave 8 Vi viser først at $3 \nmid n \implies \phi(3n) = 2\phi(n)$. Siden 3 er et primtall har vi at $3 \nmid n \implies \gcd(3, n) = 1$. Dermed kan vi bruke at ϕ er en multiplikativ funksjon til å si at

$$\phi(3n) = \phi(3)\phi(n) = 2\phi(n).$$

For den andre implikasjonen viser vi det kontrapositive, nemlig at $3 \mid n \implies \phi(3n) \neq 2\phi(3n)$. Anta at $3 \mid n$. Da kan vi skrive n som $3^k \cdot m$ for $k \geq 1$ $m \in \mathbb{N}$ slik at $3 \neq m$. Da vil $\phi(n) = \phi(3^k)\phi(m) = (3^k - 3^{k-1})\phi(m)$. Dermed vil

$$
\begin{aligned}
\phi(3n) = \phi(3^{k+1})\phi(m) &= (3^{k+1} - 3^k)\phi(m) \\
&= 3(3^k - 3^{k-1})\phi(m) \\
&= 3\phi(n) \neq 2\phi(n) \forall n \in \mathbb{N}
\end{aligned}
$$

Dermed har vi vist at $\phi(3n) = 2\phi(n) \iff 3 \nmid n$.

Eksamen H2012 oppgave 3 For definisjonen, se teorem 7.1 i Burton. La $n = p_1^{k_1} \cdots p_r^{k_r}$ være primtallsfaktoriseringen til n. Da vil

$$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1}).$$

De ulike mulige faktoriseringene av 8 er $8 = 4 \cdot 2 = 2 \cdot 2 \cdot 2$, så vi må ha at $\phi(p_i^{k_i}) \in \{1, 2, 4, 8\}$, og produktet av dem må være lik 8. Siden $\phi(7) = 6$ og $\phi 11 = 10 > 8$ kan vi se bort ifra alle primtall som er større eller lik 7. Vi ser også at for primtall som er større enn 2 må potensen $k_i \leq 1$, fordi hvis ikke vil $p_i \mid \phi(p_i^{k_i})$. For $p_i = 2$ har vi at $\phi(2_i^k) = (2^{k_i} - 2^{k_i - 1}) = 2^{k_i - 1}$, som for $k_i \geq 5$ er større enn 8. Vi står altså igjen med følgende mulige faktorer i $\phi(n)$:

$$\begin{aligned}
\phi(2) &= 2 - 1 = 1 \\
\phi(2^2) &= 2^2 - 2 = 2 \\
\phi(2^3) &= 2^3 - 2^2 = 4 \\
\phi(2^4) &= 2^4 - 2^3 = 8 \\
\phi(3) &= 3 - 1 = 2 \\
\phi(5) &= 5 - 1 = 4
\end{aligned}$$

Disse kan kombineres til produkt på formen $2^{k_1} 3^{k_2} 5^{k_3}$ slik at

$$\phi(2^{k_1} 3^{k_2} 5^{k_3}) = \phi(2^{k_1}) \phi(3^{k_2}) \phi(5^{k_3}) = 8.$$

Dermed er følgende alle tall n slik at $\phi(n) = 8$:

$$3 \cdot 5 = 15, \quad 2^4 = 16, \quad 2^2 \cdot 5 = 20, \quad 2^3 \cdot 3 = 24, \quad 2 \cdot 3 \cdot 5 = 30$$