Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA1301 Tallteori
Høst 2023

Løsningsforslag — Øving 9

7.2.6 Vi følger hintet og vurderer $n = 2^{2k+1}$ med $k = 1, 2, \ldots$. Vi ser på

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

Så $\phi(n)$ er et perfekt kvadrat for alle heltall av formen $n = 2^{2k+1}$.

7.2.13 La $n = p_1^{k_1} \ldots p_r^{k_r}$ med $k_i \geq 1$ for $i = 1, \ldots, r$. Hvis $d \mid n$, då vet vi at $d = p_1^{l_1} \ldots p_r^{l_r}$ med $0 \leq l_i \leq k_i$ for $i = 1, \ldots, r$. Det følger då at

$$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) \qquad \phi(d) = \phi(p_1^{l_1}) \cdots \phi(p_r^{l_r})$$

Hvis $l_i = 0$ då gjelder $\phi(p_i^{l_i}) = \phi(1) = 1$ og dermed $\phi(p_i^{l_i}) \mid \phi(p_i^{k_i})$.
Dersom $l_i \geq 1$ så er $\phi(p_i^{l_i}) = p_i^{l_i-1}(p_i - 1)$ og også $\phi(p_i^{k_i}) = p_i^{k_i-1}(p_i - 1)$. Siden $l_i \leq k_i$ har vi at $p_i^{l_i-1}(p_i-1) \mid p_i^{k_i-1}(p_i-1)$.
Dermed har vi vist at $\phi(p_i^{l_i}) \mid \phi(p_i^{k_i})$ for alle $i = 1, \ldots, r$. Altså gjelder $\phi(d) \mid \phi(n)$.

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 $a^{37} \equiv a \pmod{1729}$.

7.3.2 Siden $51 = 3 \cdot 17$ er $\phi(51) = \phi(3)\phi(17) = 2 \cdot 16 = 32$. Ved Eulers Teorem gjelder det då

$$10^{\phi(51)} = 10^{32} \equiv 1 \pmod{51}$$

og dermed

$$10^{32n} \equiv 1 \pmod{51}.$$

Neste ting vi ser er at

$$10^9 = (10^2)^4 \cdot 10 \equiv (-2)^4 \cdot 10 \equiv 16 \cdot 10 \equiv 160 \equiv 7 \pmod{51}.$$

Altså gjelder det

$$10^{32n+9} = 10^{32n} \cdot 10^9 \equiv 1 \cdot 7 \equiv 7 \pmod{51}$$

som er det samme som $51 \mid (10^{32n+9} - 7)$.

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).

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

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

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

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

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

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

7.3.8a Hvis vi har den lineære kongruensen $ax \equiv b \pmod{n}$ kan vi multiplisere med $a^{\phi(n)-1}$ på begge sider, og vi får da fra Eulers teorem at

$$a^{\phi(n)}x \equiv x \equiv ba^{\phi(n)-1} \pmod{n},$$

som er det vi ville vise.

7.3.8b Det første vi legger merke til er at $\gcd(3, 26) = \gcd(13, 40) = \gcd(10, 49) = 1$, som betyr at vi kan bruke (a) på alle likningene. Vi løser første likning ved å regne ut at $26 = 2 \cdot 13$, så $\phi(26) = 12$, som betyr at

$$x \equiv 5 \cdot 3^{11} \equiv 19 \pmod{26}.$$

For likning to får vi at $40 = 2^3 \cdot 5$, så $\phi(40) = 16$, og

$$x \equiv 2 \cdot 13^{15} \equiv 34 \pmod{40}.$$

For likning tre får vi at $49 = 7^2$, så $\phi(49) = 42$, og

$$x \equiv 21 \cdot 10^{41} \equiv 7 \pmod{49}.$$

Eksamen H2006 - oppg. 2 Siden vi vil finne de tre siste siffrene, skal vi se på hva 2007^{2006} er kongruent med modulo 1000. Vi vet

$$2007^{2006} \equiv 7^{2006} \pmod{1000}$$

I tillegg har vi at $\phi(1000) = 400$ og dermed gjelder ved Eulers Teorem

$$7^{400} \equiv 1 \pmod{1000}$$

Vi har då

$$2007^{2006} \equiv 7^{2006} \equiv 7^{5 \cdot 400+6} \equiv 1^5 \cdot 7^6 \equiv 649 \pmod{1000}$$