Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA1301 Tallteori
Høst 2020

Løsningsforslag — Øving 11

8.1.3 Fra hintet i oppgaven har vi at 2 har orden n modulo $2^n - 1$ (ser du hvorfor?). Dermed gir teorem 8.1 i Burton at $2^h \equiv 1 \pmod{2^n - 1}$ hvis og bare hvis $n \mid h$. Spesielt betyr det at $n \mid \phi(2^n - 1)$, siden $2^{\phi(2^n-1)} \not\equiv 1 \pmod{2^n - 1}$ ved Eulers teorem. Dette var det vi ville vise.

8.1.9 **a)**

For å sjekke at 2 er en primitiv rot til 19 må vi vise at $2^j \not\equiv 1 \pmod{19}$ for alle $j < \phi(19) = 18$. Divisorene til 18 er

$$1, 2, 3, 6, 9, 18.$$

Merk at hvis $2^j \equiv 1 \pmod{19}$, så er $2^{kj} \equiv 1 \pmod{19}$ for alle $k \in \mathbb{N}$. Det betyr at vi kun trenger å sjekke 2^6 og 2^9:

$$2^6 \equiv 64 \equiv 7 \not\equiv 1 \pmod{19}$$
$$2^9 \equiv 2^6 2^3 \equiv 7 \cdot 8 \equiv 56 \equiv -1 \not\equiv 1 \pmod{19}$$

Vi trenger ikke å sjekke at $2^{18} \equiv 1 \pmod{19}$, siden det følger fra Eulers teorem. Dermed ser vi at 2 er en primitiv rot til 19.

For å vise at 2 ikke er en primitiv rot til 17 må vi finne et tall k som er mindre enn $\phi(17) = 16$ slik at $2^k \equiv 1 \pmod{17}$. Vi vet at $k \mid 16$, så la oss prøve $k = 8$:

$$2^8 \equiv 256 \equiv 17 \cdot 15 + 1 \equiv 1 \pmod{17}$$

Altså er ordenen til 2 modulo 17 mindre enn eller lik 8, som betyr at 2 ikke er en primitiv rot modulo 17.

b)

Vi regner først ut $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$. Det betyr at ordenen til ethvert heltall a med $\gcd(a, 15) = 1$ deler 8. Med andre ord er ordenen 2, 4 eller 8 for $a \neq 1$. Vi regner ut:

$$2^2 \equiv 4 \pmod{15}$$
$$4^2 \equiv 16 \equiv 1 \pmod{15}$$
$$7^2 \equiv 49 \equiv 4 \pmod{15}$$
$$8^2 \equiv 64 \equiv 4 \pmod{15}$$
$$11^2 \equiv 121 \equiv 1 \pmod{15}$$
$$13^2 \equiv 169 \equiv 4 \pmod{15}$$
$$14^2 \equiv 196 \equiv 1 \pmod{15}$$

Vi ser at 4, 11 og 14 har orden 2 modulo 15. Vi ser også at 2^4, 7^4, 8^4 og 13^4 er kongruent med 4^2 som er kongruent med 1 modulo 15. Med andre ord har 2, 7, 8 og 13 orden 4 modulo 15. Det betyr at ingen av tallene som er mindre enn 15 og relativt primisk til 15 har orden lik $\phi(15) = 8$, og følgelig har 15 ingen primitive røtter.

8.1.10 Siden r er en primitiv rot til n har r orden $\phi(n)$ modulo n. Dermed gir teorem 8.3 i Burton at r^k har orden $\frac{\phi(n)}{\gcd(\phi(n),k)}$ modulo n. Med andre ord er ordenen til r^k modulo n lik $\phi(n)$ hvis og bare hvis denne brøken er lik $\phi(n)$, som skjer nøyaktig når $\gcd(\phi(n), k) = 1$. Altså er r^k en primitiv rot til n hvis og bare hvis $\gcd(\phi(n), k) = 1$.

8.2.2 Vi skal demonstrere at vi ikke kan fjerne kravet om at modulusen i Lagranges teorem er et primtall. Merk at $0 \leq x < p$ er en løsning hvis og bare hvis p-x er en løsning av kongruensen. En mulighet er å rett og slett bare sette inn tall helt til man finner fire løsninger (se første løsning under). En annen mulighet er å faktorisere modulusen $n = pq$ og deretter finne løsninger modulo p og q. Dette gjør vi i de to siste løsningene under.

(1) Vi ser at 1 og $-1 \equiv 14$ er løsninger av kongruensen. I tillegg ser vi etter tall slik at $x^2 = 1 + 15n$. Siden $4^2 \equiv 16 \equiv 1 \pmod{15}$ er 4 og $-4 \equiv 11$ løsninger.

(2) Vi skal finne fire løsninger til $x^2 \equiv -1 \pmod{65}$. Nå er $65 = 5 \cdot 13$, så vi løser kongruensene $x^2 \equiv -1 \pmod 5$ og $x^2 \equiv -1 \pmod{13}$ hver for seg. Den første kongruensen løses av $x = 2$ og dermed også $-2 \equiv 3 \pmod 5$. For å løse den andre, må vi finne en n slik at $x^2 = 13n - 1$, for en x. Det vil si, vi må finne en n slik at $13n - 1$ er et kvadrattall. Nå er $13 \cdot 2 - 1 = 25 = 5^2$, så $x = 5$ løser den andre kongruensen. Da løser også $-5 \equiv 8 \pmod{13}$ kongruensen. Nå skriver vi opp de første heltallsløsningene til hver av kongruensene:

$$\begin{aligned} \text{mod } 5&\colon 2, 3, 7, 8, 12, 13, 17, 18, 22, 23, 27, 28, 32 \\ \text{mod } 13&\colon 5, 8, 18, 21, 31 \end{aligned}$$

Vi ser at 8 og 18 er løsninger av begge kongruensene, altså er 8 og 18 løsninger av $x^2 \equiv -1 \pmod{65}$. Dermed er også $-8 \equiv 57$ og $-18 \equiv 47$ løsninger. Dermed har vi funnet 4 inkongruente løsninger modulo 65.

Her skal vi løse $x^2 \equiv -2 \pmod{33}$. Nå er $33 = 3 \cdot 11$, og vi bruker samme metode som over. Modulo 3 har kongruensen løsninger 1 og 2. Modulo 11, så ser vi at $3^2 \equiv -2 \pmod{11}$, så $x = 3$ er en løsning, og dermed også $x \equiv -3 \equiv 8 \pmod{11}$. Som over setter vi opp en liste over heltallsløsningenr:

$$\begin{aligned} \text{mod } 3&\colon 1, 2, 4, 5, 7, 8, 10, 11, 13, 14 \\ \text{mod } 11&\colon 3, 8, 14 \end{aligned}$$

Her ser vi at 8 og 14 forekommer i begge lister, så de er løsninger av den opprinnelige kongruensen. Da er også $-8 \equiv 25$ og $-14 \equiv 19$ løsninger modulo 33. Dermed har vi 4 inkongruente løsninger modulo 33.

8.2.3 $\mathbf{p = 11}$:

Vi har at $\phi(11) = 10$, så mulige verdier for ordenen til a er 1, 2, 5 og 10. Det holder

derfor å beregne a^2, a^5 og a^10. Vi starter med 2 og ser at $2^2 \equiv 4$, $2^5 \equiv -1$ og $2^10 \equiv 1$ modulo 11, så 2 er en primitiv rot. De andre primitive røttene er da 2^k med $\gcd(k, 10) = 1$, altså:

$$2^3 \equiv 8,\ 2^7 \equiv 7 \ \text{ og } \ 2^9 \equiv 6 \qquad (\text{mod } 11)$$

p = 19 :
Nå er $\phi(19) = 18$, så mulige verdier for ordenen til a er $k = 1, 2, 3, 6, 9$ eller 18. Det holder derfor å beregne a^k for disse verdiene. Vi starter med 2 og ser at $2^2 \equiv 4$, $2^3 \equiv 8$, $2^6 \equiv 7$, $2^9 \equiv -1$ og $2^18 \equiv 1$ - alt (mod 19), så 2 er en primitiv rot til 19. De andre primitive røttene er da 2^k med $\gcd(k, 18) = 1$, altså:

$$2^5 \equiv 13,\ 2^7 \equiv 14,\ 2^{11} \equiv 15,\ 2^{13} \equiv 3 \ \text{ og } \ 2^{17} \equiv 10 \qquad (\text{mod } 19)$$

p = 23 :
Nå er $\phi(23) = 22$, så mulige verdier for ordenen til a er $k = 1, 2, 11$ eller 22. Det holder derfor å beregne a^k for disse verdiene. Vi starter igjen med 2, og ser at $2^2 \equiv 4$ og $2^{11} \equiv 1$ modulo 23. Altså er 2 ikke en primitiv rot til 23.

Vi prøver så med 3, og ser at $3^2 \equiv 9$, $3^{11} \equiv 1$ modulo 23, så 3 er ikke en primitiv rot til 23.

Vi prøver så med 5, og ser at $5^2 \equiv 2$, $5^1 1 \equiv -1$ og $5^2 2 \equiv 1$ modulo 23. Altså er 25 en primitiv rot til 23. De andre primitive røttene er da 5^k med $\gcd(k, 22) = 1$, altså:

$5^3 \equiv 10$, $5^5 \equiv 20$, $5^7 \equiv 17$, $5^9 \equiv 11$, $5^{13} \equiv 21$, $5^{15} \equiv 19$, $5^{17} \equiv 15$, $5^{19} \equiv 7$ og $5^{21} \equiv 14$,

hvor alle kongruensene er regnet modulo 23.

8.2.10 Hvis r er en primitiv rot til p så er tallene $r, r^2, r^3, \ldots, r^{p-1}$ de samme som $1, 2, 3, \ldots, p-1$ modulo p (men i en annen rekkefølge). Derfor blir

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv r r^2 r^3 \cdots r^{p-1}$$
$$\equiv r^{1+2+3+\cdots p-1} \equiv r^{\frac{p(p-1)}{2}} \equiv \left(r^{\frac{p-1}{2}}\right)^p \equiv (-1)^p \equiv= -1 \ (\text{mod } p)$$

Dette beviser Wilsons teorem.

Eksamen H2018 oppgave 4 **a)**
For definisjon, se kapittel 8.1 i Burton. Modulo 15 er ethvert tall kongruent med ett av tallene $0, 1, 2, \ldots .14$. Så dersom a er et heltall med $\gcd(a, 15) = 1$, så er a kongruent med ett av tallene $1, 2, 4, 7, 8, 11, 13, 14$ modulo 15. Vi må derfor finne orden til hver av disse tallene modulo 15. Dette gjorde vi i oppgave 8.1.9*b*), se den for løsningen.

b)
Et tall a er en primitiv rot til n hvis ordenen til a modulo n er $\phi(n)$. Siden $\phi(18) = 6$ vil de mulige verdiene for ordenen til a modulo 18 være $k = 1, 2, 3$ eller 6. Derfor er det nok å sjekke a^k for disse verdiene. Vi trenger at $\gcd(a, 18) = 1$, så vi prøver med $a = 5$, og ser at $5^2 \equiv 7$, $5^3 \equiv -1$ og $5^6 \equiv 1$ modulo 18. Altså har 5 orden 6 modulo 18, og er følgelig en primitiv rot til 18.

Som vi har sett har alle tall a med $\gcd(a, 15) = 1$ orden lik 1, 2 eller 4 modulo 15. Det betyr at ingen tall har orden $\phi(15) = 8$ modulo 15, og følgelig har ikke 15 noen primitive røtter.

Eksamen H2013 oppgave 3 **a)**

Se boka for definisjonene

b)

Vi har at $\phi(7) = 6$, så de mulige verdiene for ordenen til et tall a modulo 7 er $k = 1, 2, 3$ elller 6. Fra Eulers teorem har vi at $a^6 \equiv 1 \pmod 7$ for alle a med $\gcd(a, 7) = 1$, så det holder det å sjekke a^k for $k = 1, 2, 3$. Vi regner ut:

$$
\begin{aligned}
1^1 &\equiv 1 \pmod 7 & & \\
2^2 &\equiv 4 \pmod 7 & 2^3 &\equiv 8 \equiv 1 \pmod 7 \\
3^2 &\equiv 9 \equiv 2 \pmod 7 & 3^3 &\equiv 27 \equiv 6 \pmod 7 \\
4^2 &\equiv 16 \equiv 2 \pmod 7 & 4^3 &\equiv 64 \equiv 1 \pmod 7 \\
5^2 &\equiv 25 \equiv 4 \pmod 7 & 5^3 &\equiv 125 \equiv 6 \pmod 7 \\
6^2 &\equiv 36 \equiv 1 \pmod 7 & 6^3 &\equiv 216 \equiv 6 \pmod 7
\end{aligned}
$$

Fra dette ser vi at 1 har orden 1, 6 har orden 2, 2 og 4 har orden 3, og 3 og 5 har orden 6.

c)

Vi ser dette direkte fra utregningene i oppgave **b)**.