MA1301 Tallteori — Høsten 2014 — Løsninger til Eksamen

Richard Williamson

11. desember 2014

Innhold

Oppgave 1

a)

Først regner vi ut u_3:

$$u_3 = u_2 + u_1 = 1 + 1 = 2.$$

Da er

$$u_4 = u_3 + u_2 = 2 + 1 = 3$$

og

$$u_5 = u_4 + u_3 = 3 + 2 = 5.$$

b)

Vi har:

$$u_4 - u_1 = 3 - 1 = 2$$

og $2 \mid 2$. Derfor er

$$u_4 \equiv u_1 \pmod 2.$$

Vi har

$$u_5 - u_2 = 5 - 1 = 4$$

og $2 \mid 4$. Derfor er

$$u_5 \equiv u_2 \pmod 2.$$

c)

Ut ifra b), er utsagnet sant når $n = 1$ og når $n = 2$.

Anta at utsagnet har blitt bevist når $n = m$ og når $n = m - 1$, hvor m er et gitt naturlig tall slik at $m \geq 2$. Således har det blitt bevist at

$$u_{m+3} \equiv u_m \pmod 2$$

og at

$$u_{(m-1)+3} \equiv u_{m-1} \pmod 2,$$

altså at

$$u_{m+3} \equiv u_m \pmod 2$$

og at

$$u_{m+2} \equiv u_{m-1} \pmod 2.$$

Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen til Fibonaccitallene, er

$$u_{m+4} = u_{m+3} + u_{m+2}.$$

Derfor er

$$\begin{aligned} u_{(m+1)+3} &= u_{m+4} \\ &= u_{m+3} + u_{m+2}. \end{aligned}$$

(2) Ut ifra antakelsen at

$$u_{m+3} \equiv u_m \pmod 2$$

og at

$$u_{m+2} \equiv u_{m-1} \pmod 2,$$

er

$$u_{m+3} + u_{m+2} \equiv u_m + u_{m-1} \pmod 2.$$

(3) Ut ifra definisjonen til Fibonaccitallene, er

$$u_m + u_{m-1} = u_{m+1}$$

Det følger fra (1) – (3) at

$$u_{(m+1)+3} \equiv u_{m+1} \pmod 2.$$

Således har vi bevist at utsagnet er sant når $n = m + 1$.

Ved induksjon konkluderer vi at utsagnet er sant for et hvilket som helst naturlig tall n.

Utsagnet kan også bevises på følgende måte uten å benytte induksjon. Ut ifra definisjonen til Fibonaccitallene, er

$$u_{n+3} = u_{n+2} + u_{n+1}$$

og

$$u_{n+2} = u_{n+1} + u_n.$$

Derfor er

$$\begin{aligned} u_{n+3} &= u_{n+2} + u_{n+1} \\ &= (u_{n+1} + u_n) + u_{n+1} \\ &= 2u_{n+1} + u_n \end{aligned}$$

Vi har:

$$2u_{n+1} + u_n \equiv 0 \cdot u_{n+1} + u_n = u_n \pmod 2.$$

Vi konkluderer at

$$u_{n+3} \equiv u_n \pmod 2.$$

d)

Siden $u_{371} = u_{2+123\cdot 3}$, følger det fra c) ved induksjon at

$$u_{371} \equiv u_2 \pmod 2.$$

Siden $u_2 = 1$, følger det at

$$u_{371} \equiv 1 \pmod 2,$$

altså at u_{371} er et oddetall.

Alternativt kan vi argumentere som følger. Dersom u_{371} er et partall, har vi: $2 \mid u_{371}$. Siden $u_3 = 2$, har vi da: $u_3 \mid u_{371}$. Det følger da fra et resultat fra kurset at $3 \mid 371$. Siden dette ikke er sant, konkluderer vi at u_{371} ikke er et partall, altså at u_{371} er et oddetall.

Oppgave 2

a)

Vi gjør følgende observasjoner.

(1) Vi har: $x = 1$ er en løsning til kongruensen

$$17x \equiv 1 \pmod 4.$$

(2) Vi har: $x = -4$ er en løsning til kongruensen

$$4x \equiv 1 \pmod{17}.$$

(3) Det følger fra (1), (2), og det kinesiske restteoremet at

$$x = 17 \cdot 1 \cdot 3 + 4 \cdot (-4) \cdot 2 = 19$$

er en løsning både til kongruensen

$$x \equiv 3 \pmod 4$$

og til kongruensen

$$x \equiv 2 \pmod{17}.$$

I tillegg fastslår det kinesiske restteoremet at

$$x \equiv 3 \pmod 4$$

og

$$x \equiv 2 \pmod{17}$$

for et hvilket som helst heltall x slik at

$$x \equiv 19 \pmod{4 \cdot 17}$$

altså

$$x \equiv 19 \pmod{68}.$$

(4) For å løse kongruensene

$$19x \equiv 1 \pmod{68}$$

og

$$68x \equiv 1 \pmod{19},$$

benytter vi Euklids algoritme.

$$\begin{aligned} 68 &= 3 \cdot 19 + 11 \\ 19 &= 1 \cdot 11 + 8 \\ 11 &= 1 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Da får vi:

$$\begin{aligned} 11 &= 68 - 3 \cdot 19 \\ 8 &= 19 - 1 \cdot 11 \\ &= 19 - 1 \cdot (68 - 3 \cdot 19) \\ &= (-1) \cdot 68 + 4 \cdot 19 \\ 3 &= 11 - 1 \cdot 8 \\ &= (68 - 3 \cdot 19) - 1 \cdot (4 \cdot 19 - 1 \cdot 68) \\ &= 2 \cdot 68 - 7 \cdot 19 \\ 2 &= 8 - 2 \cdot 3 \\ &= ((-1) \cdot 68 + 4 \cdot 19) - 2 \cdot (2 \cdot 68 - 7 \cdot 19) \\ &= (-5) \cdot 68 + 18 \cdot 19 \\ 1 &= 3 - 1 \cdot 2 \\ &= (2 \cdot 68 - 7 \cdot 19) - 1 \cdot ((-5) \cdot 68 + 18 \cdot 19) \\ &= 7 \cdot 68 + (-25) \cdot 19. \end{aligned}$$

Dermed er $x = -25$ en løsning til kongruensen

$$19x \equiv 1 \pmod{68},$$

og $x = 7$ er en løsning til kongruensen

$$68x \equiv 1 \pmod{19}.$$

(5) Det følger fra (4) og det kinesiske restteoremet at

$$x = 19 \cdot (-25) \cdot 19 + 68 \cdot 7 \cdot 3,$$

altså $x = -7597$, er en løsning både til

$$x \equiv 19 \pmod{68}$$

og til

$$x \equiv 3 \pmod{19}.$$

I tillegg fastslår det kinesiske restteoremet at

$$x \equiv 19 \pmod{68}$$

og

$$x \equiv 3 \pmod{19}$$

for et hvilket som helst heltall x slik at

$$x \equiv -7597 \pmod{68 \cdot 19}$$

altså

$$x \equiv -7597 \pmod{1292}.$$

Siden

$$-7597 \equiv 155 \pmod{1292},$$

følger det at $x = 155$ er en løsning både til

$$x \equiv 19 \pmod{68}$$

og til

$$x \equiv 3 \pmod{19}.$$

(6) Det følger fra (3) og (5) at $x = 155$ er en løsning til alle de tre kongruensene i oppgaven. I tillegg oppfyller x kravet

$$0 \leq x < 1292.$$

b)

Anta at det finnes et heltall x slik at disse to kongruensene er sanne.

Siden

$$x \equiv 4 \pmod{6},$$

er

$$x \equiv 4 \pmod{3}.$$

Siden

$$4 \equiv 1 \pmod{3},$$

følger det at

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

Siden

$$x \equiv 11 \pmod{15},$$

er

$$x \equiv 11 \pmod{3}.$$

Siden

$$11 \equiv 2 \pmod{3},$$

følger det at

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

Det følger at

$$2 \equiv 1 \pmod{3}.$$

Dette er ikke sant! Vi konkluderer at det ikke finnes et heltall x slik at de to kongruense i oppgaven er sanne.

Oppgave 3

a)

Vi har: 53 er et primtall. Da fastslår Fermats lille teorem at

$$3^{52} \equiv 1 \pmod{53}.$$

Dermed er

$$3^{472} = 3^{9 \cdot 52 + 4} = \left(3^{52}\right)^9 \cdot 3^4 \equiv 1^9 \cdot 3^4 = 81 \equiv 28 \pmod{53}.$$

Det følger at

$$2 \cdot 3^{472} \equiv 2 \cdot 28 = 56 \equiv 3 \pmod{53}.$$

b)

Vi har:

$$\begin{aligned} 36 \cdot (49!) &= (-6) \cdot (-3) \cdot (-2) \cdot (-1) \cdot (49!) \\ &\equiv (-6) \cdot 50 \cdot 51 \cdot 52 \cdot (49!) \\ &= (-6) \cdot (49!) \cdot 50 \cdot 51 \cdot 52 \pmod{53}. \end{aligned}$$

Dermed er

$$36 \cdot (49!) \equiv (-6) \cdot (52!) \pmod{53}.$$

Siden 53 er et primtall, fastslår Wilsons teorem at

$$52! \equiv -1 \pmod{53}.$$

Derfor er

$$(-6) \cdot (52!) \equiv (-6) \cdot (-1) = 6 \pmod{53}.$$

Dermed er

$$36 \cdot (49!) \equiv 6 \pmod{53}.$$

Da er

$$36 \cdot (49!) - 4 \cdot 3^{472} = 36 \cdot (49!) - 2 \cdot \left(2 \cdot 3^{472}\right) \equiv 6 - 2 \cdot 3 = 6 - 6 \equiv 0 \pmod{53}.$$

Vi konkluderer at

$$36 \cdot (49!) - 4 \cdot 3^{472}$$

er delelig med 53.

Oppgave 4

a)

Vi har:

$$(-21)^2 - 4 \cdot 12 \cdot 8 = 57.$$

Siden

$$39^2 \equiv 57 \pmod{61},$$

følger det fra teorien for kvadratiske kongruenser fra kurset at en løsning til kongruensen

$$(2 \cdot 12)x \equiv 39 - (-21) \pmod{61},$$

altså til kongruensen

$$24x \equiv 60 \pmod{61},$$

er en løsning til den kvadratiske kongruensen i oppgaven. For å løse kongruensen

$$24x \equiv 60 \pmod{61},$$

benytter vi Euklids algoritme.

$$\begin{aligned} 61 &= 2 \cdot 24 + 13 \\ 24 &= 1 \cdot 13 + 11 \\ 13 &= 1 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Da får vi:

$$\begin{aligned}
13 &= 61 - 2 \cdot 24 \\
11 &= 24 - 1 \cdot 13 \\
&= 24 - 1 \cdot (61 - 2 \cdot 24) \\
&= (-1) \cdot 61 + 3 \cdot 24 \\
2 &= 13 - 1 \cdot 11 \\
&= (61 - 2 \cdot 24) - 1 \cdot ((-1) \cdot 61 + 3 \cdot 24) \\
&= 2 \cdot 61 + (-5) \cdot 24 \\
1 &= 11 - 5 \cdot 2 \\
&= ((-1) \cdot 61 + 3 \cdot 24) - 5 \cdot (2 \cdot 61 + (-5) \cdot 24) \\
&= (-11) \cdot 61 + 28 \cdot 24.
\end{aligned}$$

Dermed er $x = 28 \cdot 60$, altså $x = 1680$, en løsning til kongruensen

$$24x \equiv 60 \pmod{61}.$$

Vi konkluderer at $x = 1680$ er en løsning til den kvadratiske kongruensen i oppgaven.

b)

Vi gjør følgende observasjoner.

(1) Vi har:

$$238^2 - 4 \cdot 13 \cdot 269 = 42656.$$

Da er

$$\mathbb{L}_{43789}^{42656} = \mathbb{L}_{43789}^{2^5 \cdot 31 \cdot 43} = \mathbb{L}_{43789}^{2^5} \cdot \mathbb{L}_{43789}^{31} \cdot \mathbb{L}_{43789}^{43}.$$

(2) Vi har:

$$\mathbb{L}_{43789}^{2^5} = \mathbb{L}_{43789}^{\left(2^2\right)^2 \cdot 2} = \mathbb{L}_{43789}^{\left(2^2\right)^2} \cdot \mathbb{L}_{43789}^{2} = 1 \cdot \mathbb{L}_{43789}^{2} = \mathbb{L}_{43789}^{2}.$$

Siden

$$43789 \equiv 5 \pmod{8},$$

er $\mathbb{L}_{43789}^{2} = -1$. Dermed er $\mathbb{L}_{43789}^{2^5} = -1$.

(3) Siden

$$43789 \equiv 1 \pmod{4},$$

er $\mathbb{L}_{43789}^{31} = \mathbb{L}_{31}^{43789}$. Siden

$$43789 \equiv 17 \pmod{31},$$

er $\mathbb{L}_{31}^{43789} = \mathbb{L}_{31}^{17}$.

(4) Siden 17 er et primtall og

$$17 \equiv 1 \pmod 4,$$

er $\mathbb{L}_{31}^{17} = \mathbb{L}_{17}^{31}$. Siden

$$31 \equiv 14 \pmod{17},$$

er

$$\mathbb{L}_{17}^{31} = \mathbb{L}_{17}^{14} = \mathbb{L}_{17}^{2\cdot 7} = \mathbb{L}_{17}^{2} \cdot \mathbb{L}_{17}^{7}.$$

(5) Siden

$$17 \equiv 1 \pmod 8,$$

er $\mathbb{L}_{17}^{2} = 1$.

(6) Siden

$$17 \equiv 1 \pmod 4,$$

er $\mathbb{L}_{17}^{7} = \mathbb{L}_{7}^{17}$. Siden

$$17 \equiv 3 \pmod 7,$$

er $\mathbb{L}_{7}^{17} = \mathbb{L}_{7}^{3}$.

(7) Siden både

$$3 \equiv 3 \pmod 4$$

og

$$7 \equiv 3 \pmod 4,$$

er

$$\mathbb{L}_{7}^{3} = -\mathbb{L}_{3}^{7}.$$

Siden

$$7 \equiv 1 \pmod 3,$$

er

$$\mathbb{L}_{3}^{7} = \mathbb{L}_{3}^{1} = 1.$$

(8) Det følger fra (6) og (7) at $\mathbb{L}_{17}^{7} = -1$.

(9) Det følger fra (3) – (5) og (8) at

$$\mathbb{L}_{43789}^{31} = \mathbb{L}_{17}^{2} \cdot \mathbb{L}_{17}^{7} = 1 \cdot (-1) = -1.$$

(10) Siden

$$43789 \equiv 1 \pmod 4,$$

er $\mathbb{L}_{43789}^{43} = \mathbb{L}_{43}^{43789}$. Siden

$$43789 \equiv 15 \pmod{43},$$

er

$$\mathbb{L}_{43}^{43789} = \mathbb{L}_{43}^{15} = \mathbb{L}_{43}^{3} \cdot \mathbb{L}_{43}^{5}.$$

(11) Siden både

$$3 \equiv 3 \pmod 4$$

og

$$43 \equiv 3 \pmod 4,$$

er

$$\mathbb{L}_{43}^{3} = -\mathbb{L}_{3}^{43}.$$

Siden

$$43 \equiv 1 \pmod 3,$$

er $\mathbb{L}_{3}^{43} = \mathbb{L}_{3}^{1} = 1$. Dermed er $\mathbb{L}_{43}^{3} = -1$.

(12) Siden

$$5 \equiv 1 \pmod 4,$$

er $\mathbb{L}_{43}^{5} = \mathbb{L}_{5}^{43}$. Siden

$$43 \equiv 3 \pmod 5,$$

er $\mathbb{L}_{5}^{43} = \mathbb{L}_{5}^{3}$.

(13) Siden

$$5 \equiv 1 \pmod 4,$$

er $\mathbb{L}_{5}^{3} = \mathbb{L}_{3}^{5}$. Siden

$$5 \equiv 2 \pmod 3,$$

er $\mathbb{L}_{3}^{5} = \mathbb{L}_{3}^{2}$. Siden

$$3 \equiv 3 \pmod 8,$$

er $\mathbb{L}_{3}^{2} = -1$.

(14) Det følger fra (12) og (13) at $\mathbb{L}_{43}^{5} = -1$.

(15) Det følger fra (10), (11), og (14) at

$$\mathbb{L}_{43789}^{43} = \mathbb{L}_{43789}^{3} \cdot \mathbb{L}_{43789}^{5} = (-1) \cdot (-1) = 1.$$

(16) Det følger fra (1), (2), (9), og (15) at

$$\mathbb{L}_{43789}^{42656} = \mathbb{L}_{43789}^{2^5 \cdot 31 \cdot 43} = \mathbb{L}_{43789}^{2^5} \cdot \mathbb{L}_{43789}^{31} \cdot \mathbb{L}_{43789}^{43} = (-1) \cdot (-1) \cdot 1 = 1.$$

Dermed er 42656 er en kvadratisk rest modulo 43789. Vi konkluderer at det finnes to heltall x slik at $0 \leq x < 43789$ og x er en løsning til den kvadratiske kongruensen i oppgaven.

Oppgave 5

Vi gjør følgende observasjoner.

(1) Vi har: $187 = 11 \cdot 17$. Både 11 og 17 er primtall.

(2) Vi har: $(11-1) \cdot (17-1) = 10 \cdot 16 = 160$.

(3) Vi har: $x = -3$ er en løsning til kongruensen

$$53x \equiv 1 \pmod{160},$$

altså $x = 157$ er en løsning til denne kongruensen.

(4) Vi har:

$$25^{157} = \left(25^7\right)^{22} \cdot 25^3 \equiv (-2)^{22} \cdot 25^3 \equiv 81 \cdot 104 = 8424 \equiv 9 \pmod{187}.$$

(5) Når vi oversetter 9 til et symbol, får vi: I.

Oppgave 6

a)

Vi har: 2, 5, 11, 17, 23.

b)

La q være produktet av alle de primtallene som er mindre enn eller like n, og som er kongruent til 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 naturlig tall i slik at $i \leq t$, er ett av følgende er 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 har vi: $3 \mid p_i$. Siden

$$3q - 1 = (p_1 \cdots p_{i-1} p_{i+1} \cdots p_t) \cdot p_i,$$

har vi i tillegg: $p_i \mid 3q - 1$. Derfor har vi: $3 \mid 3q - 1$, altså

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

Imidlertid er

$$3q - 1 \equiv -1 \equiv 2 \pmod 3.$$

Siden det ikke er sant at

$$1 \equiv 2 \pmod 3,$$

kan det ikke være sant at både

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

og

$$3q - 1 \equiv 2 \pmod 3.$$

Siden antakelsen at det finnes et naturlig tall i slik at (1) er sant fører til at begge kongruesene er sanne, konkluderer vi at det ikke finnes et naturlig tall i slik at (1) er sant.

Dermed er enten (2) eller (3) sant for hvert naturlig tall i slik at $i \leq t$. 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 minnes 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

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

Som ovenfor, kan dette ikke være sant. Siden antakelsen at (A) er sant fører til at denne kongruensen er sanne, konkluderer vi at det ikke finnes et naturlig tall i slik at (A) er sant.

Derfor er (B) sant, altså finnes det et naturlig tall i slik at $i \leq t$ og

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

Anta at $p_i \leq n$. Vi gjør følgende observasjoner.

(1) Siden $p_i \equiv 2 \pmod 3$, følger det fra definisjonen til q og antakelsen at $p_i \leq n$ at $p_i \mid q$. Da har vi: $p_i \mid 3q$.

(2) Siden

$$3q - 1 = (p_1 \cdots p_{i-1} p_{i+1} \cdots p_t) \cdot p_i$$

har vi: $p_i \mid 3q - 1$. Da har vi: $p_i \mid -(3q - 1)$, altså $p_i \mid -3q + 1$.

(3) Det følger fra (1) og (2) at $p_i \mid 3q - (3q - 1)$, altså at $p_i \mid 1$.

Siden p_i er et primtall, er $p_i \geq 2$. Det kan ikke være sant at både $p_i \mid 1$ og $p_i \geq 2$. Siden antakelsen at $p_i \leq n$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $p_i \leq n$. Derfor er $p_i > n$.

c)

De primtallene som er mindre enn eller like 14 og som er kongruent til 2 modulo 3 er 2, 5, og 11. En primtallsfaktorisering til $3 \cdot (2 \cdot 5 \cdot 11) - 1$, altså til 329, er

$$7 \cdot 47.$$

Dermed får vi at $p = 47$.