

# Miniprojekt 2:

## Talteori med anvendelser

I dette miniprojekt arbejdes der konkret med begreberne og algoritmerne fra Afsnit 4.3, 4.4 og 4.5 i [Rosen]. Husk, at miniprojekterne indgår i pensum. Der er facitliste sidst i dokumentet.

### *Opgave 1:*

Denne opgave regnes i hånden. Givet  $a = 3$ , da søges  $\bar{a}$  således, at  $\bar{a}a \equiv 1 \pmod{7}$ . Find  $\bar{a}$  ved at prøve dig frem (hvorfor behøver du alene teste værdier fra  $\{0, 1, 2, \dots, 6\}$ ?).

### *Opgave 2:*

Denne opgave regnes i hånden. Givet  $a = 5$ , da søges  $\bar{a}$  således, at  $\bar{a}a \equiv 1 \pmod{19}$ . Du skal benytte Euklids algoritme til at bestemme  $\bar{a}$  (se eksemplerne 1 og 2 i afsnit 4.4). Når du har fundet svaret, test da, at det nu også opfylder den ønskede ækvivalens.

### *Opgave 3:*

Denne opgave regnes vha. Maple. Det oplyses, at kommandoen "igcdex(a,b,s,t)" udregner (returnerer) den største fælles divisor mellem a og b. Desuden gemmer den i variablerne "s" og "t" værdier, så  $\gcd(a, b) = sa + tb$  holder. Du kan tilgå s simpelthen ved at lave en kommandolinie "s;" og så trykke return. Givet  $a = 103$  og  $m = 4627$ , find  $\bar{a}$  således at  $\bar{a}a \equiv 1 \pmod{m}$  (Husk, at argumentere for, at  $\bar{a} = s$ ). Test efter, at den fundne værdi opfylder  $\bar{a} \cdot 103 \equiv 1 \pmod{4627}$ .

### *Opgave 4:*

Denne opgave er en fortsættelse af opgave 2 og skal regnes i hånden. Benyt metoden beskrevet i eksempel 3 i afsnit 4.4 til at løse ligningen

$$5x \equiv 2 \pmod{19}.$$

*Opgave 5:*

Denne opgave er en fortsættelse af opgave 3 og skal regnes i Maple. Benyt metoden beskrevet i eksempel 3 i afsnit 4.4 til at løse ligningen

$$103x \equiv 14 \pmod{4627}.$$

GEM DIN WORKSHEET INDEN DU UDFØRER NÆSTE OPGAVE. Som en del af opgaven vil du nemlig formentlig opleve, at Maple crasher.

**Læs afsnit 4.4 i Rosens bog.**

*Opgave 6:*

Indtast i Maple “ $3^{2005} \pmod{11}$ ” og tryk return for at få svaret. Gentag med “ $3^{20005} \pmod{11}$ ”, med “ $3^{200005} \pmod{11}$ ” osv. osv. Bliv ved indtil Maple står af. Eksempelvis kan Maple ikke håndtere “ $3^{2000000000005} \pmod{11}$ ” medmindre du bærer dig smart ad. Er Maple gået ned, så genstart den.

Udregn  $2000000000005 \pmod{10}$ . (Hvorfor 10 ?) Benyt Fermats lille sætning (Th. 3 i afsnit 4.4) og metoden i eksempel 9 i afsnit 4.4 til at udregne  $3^{2000000000005} \pmod{11}$ .

*Opgave 7:*

Denne opgave regnes i hånden. Udregn  $3^{40} \pmod{13}$ . Du skal benytte metoden fra eksempel 9 i afsnit 4.4.

*Opgave 8:*

Vi løser ligningssystemet

$$\begin{cases} x \equiv 1 & (\text{mod } 6) \\ x \equiv 2 & (\text{mod } 7) \\ x \equiv 3 & (\text{mod } 11) \end{cases} \quad (1)$$

Lad  $a_1 = 1$ ,  $a_2 = 2$ ,  $a_3 = 3$ ,  $m_1 = 6$ ,  $m_2 = 7$  og  $m_3 = 11$ .

1. Argumenter for, at  $m_1, m_2, m_3$  er parvist indbyrdes primiske.
2. Udregn  $M_1, M_2, M_3$ .
3. Find den multiplikative inverse af  $M_1$  modulo  $m_1$  (i beviset for Th. 2 i afsnit 4.4 benyttes betegnelsen  $y_1$  om dette tal). Du skal altså finde et tal  $y_1$  således at,

$$y_1(M_1 \pmod{m_1}) \equiv 1 \pmod{m_1}$$

holder. Find  $y_1$  ved at prøve dig frem (eller ved at anvende Euklids udvidede algoritme).

4. Find på samme måde den multiplikative inverse  $y_2$  af  $M_2$  modulo  $m_2$ .
5. Find også den multiplikative inverse  $y_3$  af  $M_3$  modulo  $m_3$ .
6. Løs ligningen (1) vha. formlen:

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{m_1 m_2 m_3}.$$

*Opgave 9:*

Vis at Theorem 2 på side 275 har følgende form for  $n = 2$ : (Opgaven er altså specielt at eftervise at udtrykket for  $x$  i beviset for Theorem 2 bliver som vist herunder.)

**Den Kinesiske Rest-Sætning** for  $n = 2$  kongruenser.

Lad  $m_1$  og  $m_2$  være indbyrdes primiske heltal større end 1, og lad  $a_1$  og  $a_2$  være vilkårlige heltal.

Så har systemet

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}$$

en entydig løsning modulo  $m = m_1 m_2$ , nemlig  $x \equiv a_1 t m_2 + a_2 s m_1 \pmod{m}$ , hvor  $\gcd(m_1, m_2) = 1 = s m_1 + t m_2$ , altså  $s$  og  $t$  er fundet ved hjælp af Euklids udvidede algoritme.

*Opgave 10:*

Du løser ligningssystemet

$$\begin{cases} x \equiv 3 & \pmod{5} \\ x \equiv 2 & \pmod{11} \end{cases} \quad (2)$$

og er herefter stolt af dig selv!!!

*Opgave 11:*

Løs vha. metoden fra opgave 8 ovenfor (og eksempel 5 i afsnit 4.4) ligningssystemet:

$$\begin{cases} x \equiv 2 & \pmod{7} \\ x \equiv 4 & \pmod{9} \\ x \equiv 3 & \pmod{13} \end{cases} \quad (3)$$

**Læs afsnit 4.5 i Rosens bog.**

*Opgave 12:*

Lav følgende opgaver Rosen, afsnit 4.5:

- Opgave 1: Which memory locations ...
- Opgave 5: What sequence of pseudorandom ...
- Opgave 11: The first nine digits of the ISBN-10 ...

### Facitliste

- Opg. 1: 5.
- Opg. 2: 4.
- Opg. 3: 584.
- Opg. 4: Det mindste ikke-negative heltal, som er løsning, er 8. Generel løsning er  $\{8 + 19k \mid k \in \mathbb{Z}\}$ .
- Opg. 5: Det mindste ikke-negative heltal, som er løsning, er 3549. Generel løsning er  $\{3548 + 4627k \mid k \in \mathbb{Z}\}$ .
- Opg. 6: 1.
- Opg. 7: 3.
- Opg. 8:
  1.  $\gcd(6, 7) = \gcd(6, 11) = \gcd(7, 11) = 1$ .
  2.  $M_1 = 77, M_2 = 66, M_3 = 42$ .
  3.  $y_1 = 5$
  4.  $y_2 = 5$
  5.  $y_3 = 5$
  6. Det mindste ikke-negative heltal, som er løsning, er 289. Generel løsning er  $\{289 + 462k \mid k \in \mathbb{Z}\}$ .
- Opg. 10: Det mindste ikke-negative heltal, som er løsning, er 13. Generel løsning er  $\{13 + 55k \mid k \in \mathbb{Z}\}$ .
- Opg. 11: Det mindste ikke-negative heltal, som er løsning, er 562. Generel løsning er  $\{562 + 819k \mid k \in \mathbb{Z}\}$ .
- Opg. 12: Se bogens facitliste.